**Aviso de Privacidad**

# Qué necesitamos

Nuestra política de protección de datos personales rige el uso y almacenamiento de sus datos. Nuestra Política de Protección de Datos Personales está disponible para cualquier usuario o parte interesada.

**SUMINISTROS SANITARIOS DE EXTREMADURA (SUMSANEX)** es un responsable de los datos personales que usted (interesado) nos facilita. Recogemos los siguientes tipos de datos de usted:

* Datos de contacto identificables (nombre, dirección, teléfono y/o email de contacto, etc.)
* Datos que aportan información comercial, profesionales y económicos

# Por qué lo necesitamos

Necesitamos sus datos personales para poder proporcionar nuestros servicios y mantener la actividad comercial con Vd.

# Qué hacemos con ello

**Sus datos personales son tratados en P.I EL NEVERO C/ VEINTIUNO Nº 19 BADAJOZ 06006 BADAJOZ localizada en España. El alojamiento y almacenamiento de sus datos se realiza en esa misma dirección**

Ningún tercero tiene acceso a sus datos, a menos que específicamente sea requerido por ley.

# Cuánto tiempo lo guardamos

Bajo la ley española, estamos obligados a conservar sus documentos durante al menos 6 años de acuerdo con la política de retención de datos de carácter mercantil. Después de este período, sus datos personales serán destruidos de forma irreversible. Cualquier dato personal que tengamos para notificaciones comerciales y de actualización de servicio lo guardaremos hasta el momento en que nos avise que ya no desea recibir esta información. Consulte la Política de Retención de Datos para obtener más información sobre nuestro programa de retención de datos personales.

# ¿Cuáles son tus derechos?

Si cree que los datos personales que tenemos sobre usted son incorrectos o están incompletos, puede de solicitar ver esta información, rectificarla o eliminarla. Por favor contacte con nosotros a través de Formulario de Solicitud de Acceso del Interesado. En el caso de que quisiera hacer reclamación de cómo hemos tratado sus datos personales, por favor contacte al Delegado de protección de datos o al Responsable de Seguridad a **administracion@sumsanex.com o** escriba a la dirección **P.I EL NEVERO C/ VEINTIUNO Nº 19 BADAJOZ 06006 BADAJOZ**. Nuestro Responsable de Fichero luego analizará su reclamación y trabajará con usted para solucionar el problema. Si aun así considerara que sus datos personales no han sido tratados apropiadamente de acuerdo con la ley, puede contactar a la Agencia Española de Protección de Datos Personales (www.agpd.es) y presentar una reclamación a ellos.

**AVISO DE PRIVACIDAD DE LOS EMPLEADOS**

# Fundamentos legales del tratamiento

Al ejecutar el contrato de trabajo laboral, SUMINISTROS SANITARIOS EXTREMEÑOS (SUMSANEX), en lo sucesivo “Empresa”, tendrá el derecho de tratar datos personales, incluyendo el número de identificación personal del empleado, proporcionado a la Empresa por el empleado o por un tercero, para permitir a la Empresa cumplir con sus obligaciones legales y contractuales en calidad de contratante o para tomar medidas a solicitud del interesado antes de la celebración de un contrato laboral

Los datos personales pueden además ser utilizados en función de los intereses legítimos perseguidos por la Empresa o por un tercero (como filiales de la Empresa), excepto cuando dichos intereses sean anulados por los intereses o derechos y libertades fundamentales del interesado, los cuales requieren la protección de los datos personales.

# Fines del Tratamiento

Los fines del tratamiento de datos personales incluyen:

Recursos humanos y gestión de personal. Este fin incluye actividades de gestión de recursos humanos llevadas a cabo como parte de la contratación o el cumplimiento de un contrato laboral, e incluye el comienzo, la terminación del empleo, la programación y el registro de tiempo de trabajo, el rendimiento, la indemnización y las prestaciones, y la formación.

Cumplimiento de leyes locales y de los estados miembros de la UE. Este fin se refiere al tratamiento de datos personales según sea necesario para cumplir con una obligación legal a la que está sujeta la Empresa. Su propósito es garantizar el cumplimiento de la ley por parte de la Empresa incluyendo, entre otros, la prevención de delitos y la divulgación de datos personales a instituciones gubernamentales y autoridades de control, incluidas las autoridades tributarias y laborales, en relación con los mismos.

Realización de procesos empresariales y administración interna. Este fin aborda actividades tales como viajes y gastos, administración de activos de la compañía, servicios de TI, seguridad de la información, realización de auditorías e investigaciones internas, consultoría legal o empresarial, y preparación o participación en la resolución de conflictos.

# Transferencias a terceros

Al tratar los datos personales de los empleados para los fines indicados anteriormente, la Empresa puede utilizar los servicios de terceros, tales como: nuestra asesoría laboral (ZETA ASESORES SCL). Por lo tanto, los terceros pueden recibir o tener acceso a los datos personales de los empleados.

Al utilizar los servicios de un tercero, la Empresa se asegurará de que el tercero proporcione las medidas técnicas y organizativas adecuadas para proteger los datos personales según lo exija la ley aplicable.

# Transferencias de datos transfronterizas

Los procesos comerciales de la Empresa de manera creciente van más allá de las fronteras de un país. Esta globalización demanda no sólo la disponibilidad de comunicaciones y sistemas de información en toda la Empresa, sino también el tratamiento y uso de la información de la empresa en todo el mundo. En consecuencia, los datos de los empleados pueden estar sujetos a transferencias de datos transfronterizas, por ejemplo, a países para los cuales no se ha emitido una decisión de adecuación por parte de la Comisión Europea, basadas en cláusulas de protección de datos adoptadas por la Comisión Europea (en adelante “Acuerdos de Transferencias de Datos”) así como en salvaguardias adecuadas reconocidas por el Reglamento de Protección de Datos.

# Retención

Los datos personales de los empleados no serán almacenados más tiempo de lo necesario considerando los fines de las actividades de tratamiento. La retención no excederá los 6 años desde el fin de las relaciones laborales.

# Derechos de los empleados

El empleado tiene derecho a recibir información de la Empresa con respecto al tratamiento de la Empresa de la información personal que concierne al empleado.

El empleado tiene el derecho de solicitar rectificación y/o borrado de los datos personales o restricción del tratamiento que concierne al interesado, o de oponerse al tratamiento, así como el derecho a la portabilidad de datos.

Para ejercer sus derechos, el empleado puede contactar con: Departamento de RRHH

El empleado tiene el derecho de presentar una reclamación a la Autoridad de Control (www.aepd.es). Los empleados también pueden contactar con el Responsable de Fichero o Delegado de Protección de Datos o Departamento de RRHH en administracion@sumsanex.com.

**FORMULARIO DE CONSENTIMIENTO DEL INTERESADO**

Por la presente doy mi consentimiento a que **SUMINISTROS SANITARIOS EXTREMEÑOS (SUMSANEX)** pueda tratar mis datos personales con el fin de mantener relaciones comerciales y a recibir información de tipo comercial u otra, así como comunicaciones de marketing de su organización.

Soy consciente y me informaron de que puedo retirar mi consentimiento en cualquier momento utilizando la “SOLICITUD DE RETIRADA DEL CONSENTIMIENTO DEL INTERESADO,” ya sea enviándolo por correo electrónico a **administracion@sumsanex.com** o correo postal a **P.I EL NEVERO C/ VEINTIUNO Nº 19 BADAJOZ 06006 BADAJOZ**.

Si utiliza esta solicitud en un sitio web, se necesita una acción afirmativa en nombre del interesado, como marcar una casilla de verificación.

En tal caso, la compañía necesita conservar esta acción afirmativa del interesado (manteniendo un registro del consentimiento dado a través de un sitio web).

Firma: Fecha:

Nombre: [**nombre del interesado**]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ACUERDO DE TRATAMIENTO DE DATOS DEL PROVEEDOR**

Este no es un documento independiente. Está destinado a ser un anexo al acuerdo comercial con el proveedor que trata datos en tu nombre

Este acuerdo de protección de datos ("**Acuerdo**"), con fecha de 01 de marzo de 2018 ("**Fecha de vigencia del acuerdo**") forma parte de la relación mercantil de prestación de servicios ("**Acuerdo principal** ") entre:

SUMINISTROS SANITARIOS EXTREMEÑOS (SUMSANEX)(por la presente referido como el "**Responsable**") actuando en nombre propio;

y

ZETA ASESORES SCL/ ZETA ASESORES SCL / Garric Médica, S.L [**Nombre del proveedor que tiene acceso a datos de carácter personal que ha recabado nuestra organización**] **(**por la presente referido como el **“Encargado**"**)** actuando en nombre propio.

Los términos utilizados en este acuerdo tendrán los significados establecidos en este addéndum. Los términos no definidos en este documento tendrán el significado que se les otorga en el acuerdo principal. Excepto como se modifica a continuación, los términos del acuerdo principal permanecerán en pleno vigor y efecto.

Las partes acuerdan por la presente que los términos y condiciones establecidos a continuación se agregarán como un addéndum al acuerdo principal.

# Definiciones

En este Acuerdo, los siguientes términos tendrán los significados que se establecen a continuación y los términos afines se interpretarán en consecuencia:

***"Subencargados autorizados "*** se refiere (a) aquellos subencargados establecidos en el Anexo 3 (Transferencias autorizadas de datos personales del responsable); y (b) cualquier subencargado adicional consentido por escrito por el responsable de acuerdo con la sección de subtratamiento.

***"Subencargado"*** cualquier encargado de datos (incluido cualquier tercero) designado por el responsable para tratar datos personales del responsable en nombre del responsable.

***"Tratar/Tratamiento/Tratado", "responsable de datos", "encargado de datos", "interesado", "datos personales", "categorías especiales de datos personales"*** y cualquier otra definición no incluida en este acuerdo o el principal acuerdo tendrá el mismo significado que en el Reglamento general de protección de datos 2016/679 del Parlamento Europeo y del Consejo ("GDPR").

***"Leyes de Protección de Datos"*** significa el Reglamento General de Protección de Datos de la UE 2016/679 del Parlamento Europeo y del Consejo ("GDPR"), así como cualquier ley local de protección de datos.

***"Borrado"*** significa la eliminación o destrucción de datos personales de manera tal que no puedan ser recuperados o reconstruidos.

***"EEE"***significa Espacio Económico Europeo.

***"Tercer país"*** significa cualquier país fuera de la UE / EEE, excepto cuando ese país esté sujeto a una decisión de adecuación válida por parte de la Comisión Europea sobre la protección de datos personales en terceros países.

***"Datos personales del responsable"*** significa los datos descritos en el Anexo 1 y cualquier otro dato personal tratado por el encargado en nombre del responsable de conformidad o en conexión con el acuerdo principal.

***"Violación de seguridad de datos personales"*** significa una infracción que conduce a la destrucción, pérdida, alteración, divulgación no autorizada o acceso accidental o ilegal de datos personales del responsable transmitidos, almacenados o tratados de otra manera.

***"Servicios"*** se refiere a los servicios que el encargado debe proporcionar al responsable de conformidad con el acuerdo principal.

***"Productos"*** se refiere a los productos que el encargado debe suministrar al responsable de conformidad con el acuerdo principal.

***"Cláusulas contractuales estándar "*** se refiere a las cláusulas contractuales estándar para la transferencia de datos personales a los encargados establecidos en terceros países, según lo aprobado por la Decisión 2010/87 / UE de la Comisión Europea, o cualquier conjunto de cláusulas aprobadas por la Comisión Europea que las modifique, sustituya o reemplace.

# Términos del tratamiento de datos

* 1. En el curso de la prestación de los servicios y/o productos al responsable de conformidad con el acuerdo principal, el responsable puede tratar los datos personales del responsable en nombre del responsable según los términos de este addéndum. El encargado acuerda cumplir con las siguientes disposiciones con respecto a cualquier información personal del responsable.
	2. En la medida en que sea requerida por las leyes de protección de datos que apliquen, el encargado obtendrá y mantendrá todas las licencias, autorizaciones y permisos necesarios para tratar los datos personales, incluidos los datos personales mencionados en el Anexo 1.

El encargado deberá mantener todas las medidas técnicas y organizativas para cumplir con los requisitos establecidos en el addéndum y sus anexos.

# Tratamiento de los datos personales del responsable

* 1. El encargado sólo tratará los datos personales del responsable para los fines del acuerdo principal. El encargado no tratará, transferirá, modificará, corregirá o alterará los datos personales del responsable ni comunicará o permitirá la comunicación de los datos personales del responsable a ningún tercero que no sea de conformidad con las instrucciones documentadas del responsable, a menos que el tratamiento sea requerido por la UE o una ley del Estado Miembro a la cual esté sujeto el encargado. El encargado deberá, en la medida en que lo permita dicha ley, informar al responsable de ese requisito legal antes de tratar los datos personales y cumplir con las instrucciones del controlador para minimizar, en la medida de lo posible, el alcance de la comunicación.
	2. Para los fines establecidos en la sección anterior, el responsable instruye al encargado para transferir los datos personales del responsable a los destinatarios en los Terceros Países enumerados en el Anexo 3 (Transferencias Autorizadas de Datos Personales del Controlador), siempre y cuando el encargado cumpla con la sección Sub-T.

# Responsabilidad y no comunicación

* 1. El encargado deberá tomar medidas razonables para garantizar la fiabilidad de cualquier empleado, agente o contratista que pueda tener acceso a los datos personales del responsable, asegurando en cada caso que el acceso está estrictamente limitado a aquellas personas que requieren acceso a los datos personales del responsable pertinentes.
	2. El encargado debe garantizar que todas las personas físicas que tienen una tarea de tratar datos personales del responsable:
		1. Son informadas de la naturaleza confidencial de los datos personales del responsable y son conscientes de las obligaciones del encargado bajo este addéndum y el acuerdo principal en relación a los datos personales del responsable;
		2. Han llevado a cabo formación/certificaciones apropiadas en relación a las leyes de protección de datos u otras formaciones/certificaciones requeridas por el responsable;
		3. Están sujetas a compromisos de confidencialidad u obligaciones profesionales o estatutarias de confidencialidad; y
		4. Están sujetas a la autenticación de usuario y a los procesos de inicio de sesión cuando acceden a los datos personales del responsable de conformidad con este acuerdo, el acuerdo principal y las leyes de protección de datos aplicables.

# Seguridad de datos personales

* 1. Teniendo en cuenta el estado del arte, los costes de implementación y la naturaleza, alcance, contexto y finalidad del tratamiento, así como el riesgo de variabilidad y severidad de los derechos y libertades de las personas físicas, el encargado deberá implementar los procedimientos técnicos apropiados y medidas organizativas (Anexo 2) para garantizar un nivel de seguridad de los datos personales del responsable apropiado para el riesgo, que incluye, pero no se limita a:

### Seudonimización and encriptado;

### La capacidad de garantizar la confidencialidad, integridad, disponibilidad y flexibilidad constantes de los sistemas y servicios de tratamiento;

### La capacidad de restablecer la disponibilidad y el acceso a los datos personales del responsable de manera oportuna en el caso de un incidente físico o técnico; y

### Un proceso para probar, analizar y evaluar regularmente la efectividad de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento

## A la hora de evaluar el nivel de seguridad adecuado, el encargado tendrá en cuenta los riesgos que presenta el tratamiento, en particular de destrucción accidental o ilegal, pérdida, alteración, comunicación no autorizada o acceso a los datos personales del responsable transmitidos, almacenados o tratados de cualquier otra forma.

# Sub-Tratamiento

## A partir de la fecha de entrada en vigor del addéndum, el responsable autoriza al encargado a contratar a los subencargados establecidos en el Anexo 4 (subencargados autorizados). El responsable no contratará ningún subencargado de datos para trata datos personales del responsable que no sea con el consentimiento previo por escrito del responsable, que el encargado podrá rechazar con absoluta discreción.

## Con respecto al cada subencargado, el encargado deberá:

### Proporcionar todos los detalles del tratamiento que va a ser llevado ca cabo para cada subencargado.

### Llevar a cabo una “due diligence” adecuada a cada subencargado para garantizar que puede proporcionar el nivel de protección de los datos personales del responsable, incluyendo sin limitación, las suficientes garantías para implementar las medidas técnicas y organizativas apropiadas de tal forma que el tratamiento cumplirá con los requisitos del GDPR, este acuerdo, el acuerdo principal y las leyes de protección de datos aplicables.

### Incluye términos en el contrato entre el encargado y cada subencargado que son los mismos que los establecidos en este addéndum. Previa solicitud, el encargado deberá proporcionar una copia de sus acuerdos con los subencargados al responsable para su revisión.

### En la medida en que ese contrato implique la transferencia de datos personales del responsable fuera del EEE, incorpore las cláusulas contractuales estándar o cualquier otro mecanismo según lo indicado por el responsable en el contrato entre el encargado y cada subencargado para garantizar la protección adecuada de los datos personales transferidos del responsable.

### Mantenerse totalmente responsable de cualquier fallo de cada subencargado ante el responsable a la hora de cumplir con sus obligaciones en relación con el tratamiento de cualquier dato personal del responsable.

## A partir de la fecha de entrada en vigor del addéndum, el responsable autoriza al encargado a contratar a los subencargados establecidos en el anexo 3 (transferencias autorizadas de datos personales del responsable).

# Derechos del interesado

## Teniendo en cuenta la naturaleza del tratamiento, el encargado asistirá al responsable implementando las medidas técnicas y organizativas apropiadas, en la medida de lo posible, para el cumplimiento de la obligación del responsable de responder a las solicitudes de ejercicio de los derechos del interesado según lo establecido en la RGPD UE.

## El encargado deberá notificar de inmediato si recibe una solicitud de un interesado al responsable, a la autoridad de control y/u otra autoridad competente bajo cualquier ley de protección de datos aplicable con respecto a los datos personales del responsable.

## El encargado cooperará según lo solicite el responsable para permitir que el responsable cumpla con cualquier ejercicio de los derechos de un interesado bajo las leyes de protección de datos con respecto a los datos personales del encargado y cumpla con cualquier evaluación, consulta, notificación o investigación bajo cualquier ley de protección de datos con respecto a los datos personales del encargado o este acuerdo, que deberá incluir:

### La provisión de todos los datos solicitados por el responsable dentro de un plazo razonable especificado por el responsable en cada caso, incluyendo todos los detalles y copias de la reclamación, comunicación o solicitud y cualquier dato personal del responsable que posea en relación con un interesado.

### Donde corresponda, proporcionar la asistencia que el responsable solicite de forma razonable para que el responsable pueda cumplir con la solicitud pertinente dentro de los plazos establecidos por las leyes de protección de datos.

### Implementar cualquier medida técnica y organizativa adicional que el responsable pueda requerir de manera razonable para permitir que el responsable responda de forma efectiva a las reclamaciones, comunicaciones o solicitudes pertinentes.

# Violación de seguridad de datos personales

## El encargado deberá notificar al responsable sin demora indebida y, en cualquier caso, dentro de las veinticuatro (24) horas a partir del de conocimiento o la sospecha razonable de una violación de seguridad de datos personales. El encargado proporcionará a la responsable información suficiente para permitir que el encargado cumpla con todas las obligaciones de informar una violación de seguridad de datos personales bajo las leyes de protección de datos. Dicha notificación deberá como mínimo:

### Describir de la naturaleza de la infracción de datos personales, las categorías y los números de los interesados de que los se trate, y las categorías y números de registros de los datos personales afectados;

### Comunicar el nombre y los datos de contacto del delegado de protección de datos del encargado, el delegado de privacidad u otro contacto pertinente del cual se pueda obtener más información;

### Describir el riesgo estimado y las consecuencias probables de la violación de seguridad de datos personales; y

### Describir las medidas tomadas o propuestas para abordar la violación de seguridad de los datos personales.

## El encargado deberá cooperar con el responsable y tomar las medidas comerciales razonables que indique el responsable para ayudar en la investigación, mitigación y corrección de cada violación de seguridad de datos personales.

## En caso de una violación de seguridad de datos personales, el encargado no informará a ningún tercero sin antes obtener el consentimiento previo por escrito del responsable, a menos que se requiera notificación por parte de la UE o la legislación del Estado Miembro a la que esté sujeto el encargado, en cuyo caso el encargado deberá, en la medida en que lo permita dicha ley, informar al responsable de ese requisito legal, proporcionar una copia de la notificación propuesta y considerar cualquier comentario realizado por el encargado antes de notificar la violación de seguridad de datos personales.

# Consulta previa y evaluación de impacto de protección de datos

El encargado deberá proporcionar asistencia razonable al responsable con cualquier evaluación de impacto de protección de datos que se requiera bajo el Artículo 35 del RGPD y con cualquier consulta previa a cualquier autoridad de control del responsable que sean requerida bajo el Artículo 36 del RGPD, en cada caso únicamente en relación al tratamiento de datos personales del encargado por parte del encargado en nombre del responsable y considerando la naturaleza del tratamiento y la información que está disponible para el encargado.

#  Borrado o devolución de los datos personales del responsable

## El encargado debe de forma inmediata y, en cualquier caso, dentro de 90 (noventa) días naturales anteriores a: (i) el cese del tratamiento de datos personales del responsable por parte del encargado; o (ii) el término del acuerdo principal, a elección del responsable (tal elección debe ser notificada al encargado por escrito) ya sea:

###  Devolver una copia completa de todos los datos personales del responsable al responsable mediante transferencia segura de archivos en el formato que el responsable notifique al encargado y borrar de manera segura todas las demás copias de los datos personales del responsable tratados por el encargado o cualquier subencargado autorizado; o

### Limpiar cuidadosamente todas las copias de datos personales del responsable tratadas por el encargado o cualquier subencargado autorizado, y en cada caso, proporcionar una certificación por escrito al responsable de que ha cumplido completamente con los requisitos de la sección de eliminación o devolución de los datos personales del responsable.

## El encargado podrá retener los datos personales del responsable en la medida que sea requerida por la Unión Europea o la legislación del Estado Miembro, y sólo en la medida y durante el período requerido por la Unión Europea o la legislación del Estado Miembro, y siempre que el encargado garantice la confidencialidad de los datos personales de dicho responsable y se asegurará de que tales datos personales del responsable sólo se traten según sea necesario para el/los fin(es) especificados en la Unión Europea la legislación del Estado Miembro que exijan su almacenamiento y para ningún otro fin.

#  Derechos de auditoria

El encargado deberá poner a disposición del responsable, previa solicitud, toda la información necesaria para demostrar el cumplimiento con este addéndum y permitir y contribuir a las auditorías, incluidas las inspecciones del responsable u otro auditor autorizado por el responsable de cualquier instalación donde se lleve a cabo el tratamiento de los datos del responsable. El encargado permitirá que el controlador u otro auditor autorizado por el responsable inspeccionen, audite y copie los registros, procesos y sistemas relevantes a fin de que el controlador pueda cerciorarse de que se cumplen las disposiciones de este addéndum. El encargado deberá cooperar plenamente con el responsable con respecto a dicha auditoria y deberá, a solicitud del responsable, proporcionar a la responsable evidencia del cumplimiento de sus obligaciones en virtud de este addéndum. El encargado informará inmediatamente al responsable si, en su opinión, una instrucción de conformidad con esta sección de auditoria (derechos de auditoria) infringe el RGPD u otras disposiciones de protección de datos de la UE o de los Estados miembros.

#  Transferencias internacionales de datos personales del responsable

## El encargado no tratará datos personales del responsable ni permitirá que ningún subencargado autorizado trate los datos personales del responsable en un tercer país, excepto aquellos receptores en terceros países (si los hubiera) enumerados en el Anexo 3 (Transferencias autorizadas de datos personales del responsable), a menos que el encargado lo autorice por escrito con anticipación, a través de una enmienda a este Addéndum.

## Cuando el responsable lo solicite, el encargado deberá formalizar de inmediato (o conseguir que cualquier subencargado pertinente del encargado forme parte) un acuerdo con el responsable, que incluya las cláusulas contractuales estándar (cláusulas establecidas en la Decisión de la Comisión C (2010) 593 de cláusulas contractuales estándar (encargados) y / o la variación que las leyes de protección de datos puedan solicitar, con respecto a cualquier tratamiento de datos personales del responsable en un tercer país, cuyos términos prevalecen sobre aquellos en este addéndum.

#  Códigos de conducta y certificación

A solicitud del responsable, el encargado deberá cumplir con cualquier código de conducta aprobado de conformidad con el Artículo 40 del RGPD y obtener cualquier certificación aprobada por el Artículo 42 del RGDP UE, en la medida en que esté relacionado con el tratamiento de datos personales del responsable.

# Términos generales

## Sujeto a esta sección, las partes acuerdan que este acuerdo y las cláusulas contractuales estándar terminarán automáticamente al finalizar el acuerdo principal o al vencimiento o terminación de todos los contratos de servicios celebrados por el encargado con el responsable, de conformidad con el acuerdo principal, aquello que sea posterior.

## Toda obligación impuesta al encargado en virtud de este addéndum en relación con el tratamiento de datos personales continuará vigente después de la terminación o expiración de este addéndum.

## Este Addéndum, excluyendo las cláusulas contractuales estándar, se regirá por la ley vigente del acuerdo principal mientras la ley aplicable sea la ley de un Estado Miembro de la Unión Europea.

## Cualquier violación de seguridad de este addéndum constituirá una violación de seguridad del acuerdo principal.

##  Con respecto al objeto del presente addéndum, en caso de inconsistencias entre las disposiciones de este addéndum y cualquier otro acuerdo entre las partes, incluido, entre otros, el acuerdo principal, las disposiciones de este addéndum prevalecerán con respecto a las obligaciones de protección de datos de las partes en referencia a los datos personales del interesado de un estado miembro de la Unión Europea.

## Si alguna disposición de este addéndum es inválida o inaplicable, entonces el resto de este addéndum permanecerá válido y en vigor. La disposición inválida o inaplicable deberá (i) modificarse según sea necesario para garantizar su validez y aplicabilidad, preservando al mismo tiempo las intenciones de las partes lo más posible o, si esto no es factible, (ii) interpretarse de manera que la parte no válida o inaplicable nunca hubiera estado contenida en el mismo.

EN VIRTUD DE LO ANTERIOR, este addéndum se celebra y se convierte en una parte vinculante del acuerdo principal con efecto a partir de la fecha de entrada en vigor del addéndum, que se estableció anteriormente.

|  |  |
| --- | --- |
| **SUMINISTROS SANITARIOS EXTREMEÑOS (SUMSANEX) (“Responsable”)** | ZETA ASESORES SCL/ ZETA ASESORES SCL / Garric Médica, S.L **(“Encargado”)** |
| Firma \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Firma\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| SUMINISTROS SANITARIOS EXTREMEÑOS (SUMSANEX) |  |
| Nombre  | Nombre |
| Representante legal | Representante del Encargado o Delegado de Protección de Datos |
| A 3 de marzo de 2018 |  |
|  |  |

**ANEXO 1: DETALLES DE TRATAMIENTO DE LOS DATOS PERSONALES DEL RESPONSABLE**

Este Anexo 1 incluye detalles específicos del tratamiento de datos personales del responsable según lo requerido por el Artículo 28 (3) RGPD.

*Objeto y duración del tratamiento de datos personales del responsable.*

El tema y la duración del tratamiento de los datos personales del responsable se establecen en el acuerdo principal y este anexo.

*La naturaleza y la finalidad del tratamiento de los datos personales del responsable.*

**Realizar la prestación del servicio indicado en el Acuerdo Principal**

*Los tipos de datos personales del responsable que serán tratados*

**Datos identificativos (nombre, dirección, etc.), datos económicos (números de cuenta, importes, etc.), datos profesionales (cargo, empresa)**

*Las categorías de interesados que están relacionados con los datos personales del responsable*

**Personas con las que nuestra organización mantiene relaciones comerciales: clientes, proveedores, trabajadores, etc.**

**ANEXO 2: MEDIDAS TÉCNICAS Y ORGANIZATIVAS**

1. **Medidas de seguridad organizativas**
	1. **Gestión de la seguridad**
2. Política de seguridad y procedimientos: el encargado debe documentar una política de seguridad con respecto al tratamiento de los datos personales.
3. Funciones y responsabilidades：
	1. Las funciones y responsabilidades relacionadas con el tratamiento de datos personales están claramente definidas y asignadas de acuerdo con la política de seguridad.
	2. Durante las reorganizaciones internas o despidos y el cambio de empleo, se define claramente la revocación de los derechos y responsabilidades con los respectivos procedimientos de traspaso.
4. Política de control de acceso: los derechos específicos de control de acceso se asignan a cada función involucrada en el tratamiento de datos personales, siguiendo el principio de “necesidad de saber”.
5. Gestión de recursos / activos: el encargado tiene un registro de los recursos de TI utilizados para el tratamiento de datos personales (hardware, software y red). A una persona específica se le asigna la tarea de mantener y actualizar el registro (por ejemplo, el responsable de TI).
6. Gestión de cambios: el encargado se asegura de que todos los cambios en el sistema de TI sean registrados y supervisados por una persona específica (por ejemplo, un técnico de TI o de seguridad). Se lleva a cabo el seguimiento regular de este proceso
	1. **Respuesta ante incidentes y continuidad de negocio**
7. Gestión de incidentes/violación de seguridad de datos personales:
	1. Se define un plan de respuesta a incidentes con procedimientos detallados para garantizar una respuesta eficaz y ordenada a los incidentes relacionados con los datos personales
	2. El encargado informará sin dilación indebida al responsable de cualquier incidente de seguridad que haya resultado en la pérdida, uso indebido o adquisición no autorizada de datos personales.
8. Continuidad del negocio: el encargado establece los principales procedimientos y controles que se deben seguir para asegurar el nivel requerido de continuidad y disponibilidad del sistema informático que trata los datos personales (en el caso de un incidente / violación de seguridad de datos personales).
	1. **Recursos humanos**
9. Confidencialidad del personal: el encargado se asegura de que todos los empleados comprendan sus responsabilidades y obligaciones relacionadas con el tratamiento de datos personales. Las funciones y las responsabilidades se comunican claramente durante el proceso de pre-empleo y/o inducción.
10. Formación: el encargado garantiza que todos los empleados estén adecuadamente informados sobre los controles de seguridad del sistema de TI que se relacionan con su trabajo diario. Los empleados que participan en el tratamiento de datos personales también están debidamente informados sobre los requisitos de protección de datos pertinentes y las obligaciones legales a través de campañas regulares de concienciación.
11. **Medidas de seguridad técnicas**
	1. **Control de acceso y autenticación**
12. Se implementa un sistema de control de acceso aplicable a todos los usuarios que acceden al sistema de TI. El sistema permite crear, aprobar, revisar y eliminar cuentas de usuario.
13. Se evita el uso de cuentas de usuario comunes. En los casos en que esto sea necesario, se garantiza que todos los usuarios de la cuenta común tengan las mismas funciones y responsabilidades.
14. Al otorgar acceso o asignar funciones de usuario, se debe observar el "principio de necesidad de saber" para limitar el número de usuarios que tienen acceso a datos personales a sólo aquellos que lo soliciten para lograr los propósitos de tratamiento del encargado.
15. Cuando los mecanismos de autenticación se basan en contraseñas, el encargado solicita que la contraseña tenga al menos ocho caracteres de longitud y se ajuste a parámetros de control de contraseñas muy sólidos, como la longitud, la complejidad del carácter y la no repetibilidad.
16. Las credenciales de autenticación (como la identificación de usuario y la contraseña) nunca se transmitirán sin protección a través de la red.
	1. **Registro y seguimiento**: los archivos de registro se activan para cada sistema/aplicación utilizada para el tratamiento de datos personales. Incluyen todos los tipos de acceso a datos (vista, modificación, eliminación).
	2. **Seguridad de los datos en reposo**
17. **Seguridad del servidor/base de datos**
	1. Los servidores de bases de datos y aplicaciones están configurados para ejecutarse utilizando una cuenta separada, con privilegios mínimos de sistema operativo para funcionar correctamente.
	2. Los servidores de bases de datos y aplicaciones sólo tratan los datos personales que realmente se necesitan para lograr sus fines de tratamiento.
18. **Seguridad de la estación de trabajo:**
	1. Los usuarios no pueden desactivar u omitir la configuración de seguridad.
	2. Las aplicaciones antivirus y las firmas de detección se configuran de forma regular.
	3. Los usuarios no tienen privilegios para instalar o desactivar aplicaciones de software no autorizadas.
	4. El sistema tiene tiempos de espera de sesión cuando el usuario no ha estado activo durante un cierto período de tiempo.
	5. Las actualizaciones de seguridad críticas lanzadas por el desarrollador del sistema operativo se instalan regularmente.
	6. **Seguridad de red / comunicación:**
19. Cuando el acceso se realiza a través de Internet, la comunicación se cifra a través de protocolos criptográficos.
20. El tráfico hacia y desde el sistema de TI se sigue y controla a través de cortafuegos y sistemas de detección de intrusos.
	1. **Copias de seguridad:**
21. Los procedimientos de recuperación y restauración de datos están definidos, documentados y claramente vinculados con las funciones y las responsabilidades.
22. Las copias de seguridad reciben un nivel apropiado de protección física y ambiental consistente con los estándares aplicados en los datos de origen.
23. La ejecución de las copias de seguridad se supervisa para garantizar que esté completa
	1. **Dispositivos móviles/portátiles:**
24. Los procedimientos de administración de dispositivos portátiles y móviles se definen y documentan estableciendo reglas claras para su uso adecuado.
25. Los dispositivos móviles que tienen permiso para acceder al sistema de información están pre-registrados y pre-autorizados.
	1. **Seguridad del ciclo de vida de la aplicación:** durante el ciclo de vida del desarrollo, se siguen las mejores prácticas, el estado del arte y las prácticas o estándares de desarrollo seguros reconocidos.
	2. **Borrado/eliminación de datos:**
26. La sobreescritura basada en software se realizará en los medios antes de su eliminación. En los casos en que esto no sea posible (CDs, DVDs, etc.), se realizará una destrucción física.
27. Se lleva a cabo la trituración de papel y medios portátiles utilizados para almacenar datos personales.
	1. **Seguridad física**: el personal no autorizado no puede acceder al perímetro físico de la infraestructura del sistema de TI. Se deben establecer medidas técnicas apropiadas (por ejemplo, sistema de detección de intrusión, torniquete operado con tarjeta chip, sistema de entrada de seguridad de una sola persona, sistema de cierre) o medidas organizativas (por ejemplo, guardia de seguridad) para proteger las áreas de seguridad y sus puntos de acceso personas no autorizadas.

**ANEXO 3: TRANSFERENCIAS AUTORIZADAS DE DATOS PERSONALES DEL RESPONSABLE**

Lista de subencargados aprobados en la fecha de entrada en vigor del addéndum que se incluirá aquí. Por favor incluye (i) nombre legal completo; (ii) actividad de tratamiento; (iii) ubicación del/los centro(s) de servicio.

|  |  |  |  |
| --- | --- | --- | --- |
| No.  | Subencargado autorizado (nombre legal completo) | Actividad de tratamiento | Ubicación del/los centro(s) de servicio. |
| 1. | ……………. |  |  |
|  |  |  |  |