CONTRATO DE ENCARGO DE TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL (De acuerdo a lo estipulado en el Reglamento General de Protección de Datos)

En Sevilla a 27 de febrero de 2019.

REUNIDOS

De una parte, **D. ÁNGEL ORTIZ SÁNCHEZ** mayor de edad y con N.I.F. 45.593.302-B en nombre y representación de **SOCIEDAD ANDALUZA PARA EL DESARROLLO DE LAS TELECOMUNICACIONES, S.A.** (en adelante el **RESPONSABLE DEL TRATAMIENTO**), con domicilio sito en Avda. Camino de los Descubrimientos, 17. PCT Cartuja, 41092 – Sevilla; y con C.I.F. A-41857988.

De otra parte, **D. JOSE MARÍA CABALLERO GÓMEZ**, mayor de edad, con D.N.I. nº 25571860T, en calidad de apoderado de **MAPFRE VIDA S.A. DE SEGUROS Y REASEGUROS SOBRE LA VIDA HUMANA**, (en adelante **ENCARGADO DEL TRATAMIENTO**) con domicilio social en Carretera de Pozuelo nº 50, 28222 Majadahonda (Madrid) y CIF n.º A28229599, mediante escritura otorgada ante el Notario de Madrid, D. José María de Prada Guaita, el día 24 de octubre de 2012, con número de protocolo 2412.

Ambas partes, reconociéndose mutuamente capacidad legal suficiente para contratar y obligarse mediante este documento, y manifestando tener sus respectivos poderes en vigor,

MANIFIESTAN

El objetivo de las normas y procedimientos de actuación descritos en este contrato es garantizar la seguridad, confidencialidad, disponibilidad e integridad de la información titularidad del Responsable del Tratamiento, con el fin de evitar su alteración, pérdida y tratamiento o acceso no autorizado.

Dicha cláusula de seguridad obliga al Encargado del Tratamiento y a todo su personal que trate datos de carácter personal titularidad del Responsable del Tratamiento al cumplimiento y aplicación del Reglamento General de Protección de Datos (en adelante, RGPD), o de aquella legislación que pudiera complementarlo y/o sustituirlo, para que los datos dispongan del nivel de seguridad necesario.

En orden a lo anterior, ambas partes contemplas las siguientes,

CLÁUSULAS

Primera. - Ámbito de aplicación geográfico del presente contrato.

Las obligaciones contenidas en el presente contrato, así como aquellas que deriven de la normativa vigente se aplicarán a las actividades de un establecimiento del Encargado del

Tratamiento en el territorio de la Unión Europea, con independencia de que el tratamiento de datos personales tenga lugar en la Unión o no.

También se aplicará al tratamiento de datos personales de interesados que residan en la Unión realizado por un encargado no establecido en la Unión, si las actividades de tratamiento están relacionadas con ofrecer bienes y servicios a interesados en la Unión o cuando se realice un control del comportamiento.

Segunda. - Definiciones

El Responsable del Tratamiento es la persona física o jurídica, autoridad u organismo que ostenta la titularidad sobre los datos personales puestos a disposición. El Responsable del Tratamiento será quien decida en todo momento la finalidad y tratamiento de datos personales de su titularidad. No perderá esta condición en ningún momento y actuará con una obligación de especial diligencia en la elección y supervisión del Encargado del Tratamiento.

El Encargado del Tratamiento es la persona física o jurídica, autoridad pública u organismo que presta un servicio al Responsable que conlleva el tratamiento de datos personales por cuenta de éste.

El Encargado del Tratamiento ha sido elegido de acuerdo a criterios de diligencia y eficacia por parte del Responsable. El Encargado del Tratamiento debe ofrecer en todo momento garantías suficientes respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas y en concreto la adecuada protección de los derechos de las personas afectadas.

Tercera. - Objeto del Contrato y Finalidades del Tratamiento

El tratamiento de datos personales que realizará el Encargado del Tratamiento en cumplimiento del presente contrato consistirá en **SERVICIO DE PÓLIZA DE SEGUROS DE VIDA (Expte 19-00017)**.

Los datos de los trabajadores de SANDETEL a tratar por el adjudicatario son, potencialmente, los siguientes:

- Nombre y apellidos
- Sexo
- Fecha de nacimiento
- Fecha de defunción
- Datos de salud
- Retribuciones brutas de los trabajadores

Cuarta. – Duración del presente contrato

El presente contrato de Encargo de Tratamiento tiene una duración de 9 meses, así como una posible prórroga, y estará vinculado a los servicios prestados por el Encargado del Tratamiento. La prórroga en el presente contrato deberá ser comunicada expresamente por el Responsable del Tratamiento.

Quinta. - Obligaciones del Encargado del Tratamiento

Con la firma del presente contrato, el Encargado del Tratamiento y todo su personal se obliga a:

- Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.
- Tratar los datos de acuerdo con las instrucciones del Responsable del Tratamiento.
- Si el Encargado del Tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.
- Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:
  - El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.
  - Las categorías de tratamientos efectuados por cuenta de cada responsable.
  - En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.
  - Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

    a) La seudoanimización y el cifrado de datos personales.
    b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

- No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del Responsable del Tratamiento, en los supuestos legalmente admisibles. El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable 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.
- Implantar las medidas de seguridad comunicadas por el Responsable del Tratamiento indicadas en el Anexo, en función al análisis de riesgos que realice.

  En todo caso, deberá implantar mecanismos para:

  a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
  b) Restaurar la disponibilidad y el acceso a los datos personales en el menor tiempo posible, en caso de incidente físico o técnico.
  c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
  d) Seudonimizar y cifrar los datos personales, en su caso.

- El Encargado del Tratamiento deberá designar un delegado de protección de datos (DPD) y comunicar su identidad y datos de contacto al responsable.

Sexta. - Verificación de las medidas de seguridad

El Responsable del Tratamiento, en cumplimiento de su capacidad de control, podrá realizar por su cuenta revisiones que verifiquen el cumplimiento de las políticas y medidas de seguridad exigidas en este acuerdo, para comprobar la correcta implantación de las medidas de seguridad en el tratamiento de los datos personales del Responsable del Tratamiento.

Las revisiones podrán ser en los sistemas de información e instalaciones de tratamiento de datos del Encargado del tratamiento o bien a través de la recopilación de información que corrobore el cumplimiento por parte del Encargado del tratamiento de lo establecido en este acuerdo.

En cualquier caso, el Encargado del tratamiento se obliga a tener a disposición del Responsable del Tratamiento, de sus Auditores Externos o del regulador u otra parte interesada, la documentación (en soporte físico o electrónico) que acredite el cumplimiento de sus obligaciones conforme a lo establecido en el presente acuerdo.

Asimismo, el Encargado del tratamiento deberá acreditar que ha realizado los correspondientes análisis de riesgos y, si procede, las evaluaciones de impacto sobre la protección de datos pertinentes.

El Encargado del tratamiento se obliga a realizar auditorías y afrontar su coste, siempre que exista una regulación vigente que así lo exija, dentro de los servicios que presta al Responsable del Tratamiento.

El Responsable del Tratamiento se reserva el derecho de realizar auditorías afrontando su coste, y a solicitar evidencias sobre el cumplimiento de lo establecido en el presente acuerdo por el Encargado del tratamiento, de cara a cumplir aspectos regulatorios, legales y/o contractuales. En este caso, el Responsable del Tratamiento notificará al Encargado del tratamiento su voluntad de realizar dichas auditorías, con al menos quince días de antelación a la fecha en la que desee llevarlas a cabo, adaptando su realización a los protocolos y procedimientos de intervención del Encargado del tratamiento.

A este respecto, el Encargado del tratamiento se reserva el derecho de acordar con el Responsable del Tratamiento la fecha y el horario concreto dentro de un periodo máximo de quince días en el que el Responsable del Tratamiento podrá llevar a cabo dichas auditorías.

Adicionalmente, el Responsable de Tratamiento podrá realizar auditorías al objeto de evaluar el grado de calidad de la prestación del servicio objeto de este contrato y particularmente el nivel de cumplimiento por el Encargado del tratamiento de las mejores prácticas de seguridad. Como por ejemplo pruebas de hacking y pentesting cuando se presten servicios que impliquen la utilización de información propiedad del Responsable del Tratamiento o proporcionada por clientes del Responsable del Tratamiento.

A estos efectos, el Encargado de tratamiento se obliga (i) a colaborar en todo lo que fuere necesario para la realización de la Auditoría descrita, y (ii) a adoptar las medidas que fueren

necesarias para corregir de forma inmediata las debilidades que fueran detectadas por la Auditoría, particularmente en materia de Seguridad.

En los procesos de auditoría, el Encargado del tratamiento deberá facilitar el acceso a la información adecuada para responder a las necesidades de estas partes interesadas. Las evidencias y otra documentación generada para el proceso de auditoría deberán almacenarse en un repositorio del Responsable del Tratamiento que ambas partes acuerden.

En caso de que el Responsable del Tratamiento encontrase incumplimientos de seguridad incompatibles con lo establecido en el presente acuerdo según el análisis de riesgos realizado por éste, dependiendo de la gravedad de los mismos, podrá requerir al Encargado de tratamiento la resolución inmediata de los problemas detectados mediante la elaboración de un plan de corrección que deberá hacerse efectivo en un plazo determinado, que no podrá exceder de 3 meses.

Las personas que desempeñan funciones profesionales para el Encargado del tratamiento deben ser conscientes de la importancia de la información del Responsable del Tratamiento, tratar la misma de forma segura y estar formados y cualificados en todas y cada una de las fases de proceso de la información, para todas y cada una de las funciones que desempeñen. Estos deberán observar toda la diligencia posible y medidas adecuadas para proteger el proceso de la información en cumplimiento de su deber de buena fe a la que están obligados contractualmente.

Séptima. - Destino de los datos

Una vez finalice el presente contrato o en el caso de que no existan prórrogas establecidas, el Encargado del Tratamiento, según la opción que le comunique el Responsable del Tratamiento, deberá destruir o devolver los datos de carácter personal al mismo y, si procede, los soportes donde consten, una vez cumplida la prestación. La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el Encargado. No obstante, el Encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

Octava. - Derechos del Encargado del Tratamiento

El Encargado del Tratamiento podrá adoptar todas las decisiones organizativas y operacionales que estime necesarias para la mejor prestación del servicio que tenga encomendado, siempre que se cumpla con las finalidades indicadas. En ningún momento podrá variar las finalidades indicadas por el Responsable ni utilizar los datos personales para sus propias finalidades.

Novena. - Subcontratación de los servicios o tratamientos

La subcontratación de los servicios o los tratamientos de datos personales encomendados al Encargo del Tratamiento no está autorizada.

En caso de que sea necesaria la subcontratación de los servicios o tratamientos de datos encomendados al Encargado del Tratamiento, ésta deberá ser comunicada al Responsable del Tratamiento en el plazo de 10 días, indicando la identidad y datos de contacto del subcontratista, así como los tratamientos o servicios subcontratados. La subcontratación deberá ser autorizada expresamente y por escrito por parte del Responsable del Tratamiento. Si pasado el plazo de 5 días no ha habido respuesta por parte del Responsable del Tratamiento acerca de la subcontratación, se entenderá que queda autorizada.

En todo caso, el subencargado del tratamiento estará sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y en la misma forma que el Encargado del Tratamiento en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas.

En caso de incumplimiento por el subencargado, el Encargado inicial seguirá siendo plenamente responsable ante el Responsable del Tratamiento en lo referente al cumplimiento de las obligaciones del subencargado.

Décima. - Compromiso de Confidencialidad

El Encargado del Tratamiento está obligado al más absoluto secreto y deber de confidencialidad sobre los datos personales a los que tenga acceso con motivo de la prestación del servicio y en ejecución del presente contrato. En este sentido, deberá disponer de todas las medidas técnicas y organizativas necesarias para garantizar la más absoluta confidencialidad.

Este compromiso de confidencialidad alcanzará a todo el personal del Encargado del Tratamiento que esté autorizado para tener acceso a los datos personales objeto del presente contrato, con independencia de otras obligaciones de secreto a las que esté obligado por su pertenencia al Encargado del Tratamiento o por su régimen estatutario.

En caso de detectarse cualquier tipo de actuación indebida por cualquier persona que desempeñe funciones profesionales para el Encargado del tratamiento (acceso a información que no corresponde a sus funciones, uso indebido de usuarios y contraseñas, un usuario con más autorizaciones de las necesarias o cualquier otra), será responsabilidad y obligación expresa del Encargado del tratamiento la comunicación inmediata al Responsable del Tratamiento junto con informe detallado de los hechos.

El Responsable del Tratamiento podrá exigir al Encargado del Tratamiento que acredite de forma documental la firma del compromiso de confidencialidad por parte del personal con acceso a los datos personales objeto de este contrato.

El compromiso de confidencialidad alcanzará incluso una vez que se extingan las obligaciones previstas en este contrato. La violación del compromiso de confidencialidad facultará al Responsable del Tratamiento para emprender las acciones necesarias, incluso por vía judicial.

Undécima. - Adhesión a Códigos de Conducta, Certificados del Encargado del Tratamiento

El Encargado del Tratamiento declara de forma responsable estar al día en cuanto a sus obligaciones en materia de protección de datos. En este sentido, a la firma del presente contrato aporta certificación suficiente de estar al corriente de las obligaciones exigidas por la normativa vigente en materia de protección de datos personales.

Duodécima. - Transferencias Internacionales

La comunicación de datos personales a un país que no forme parte de la Unión Europea se regulara según lo dispuesto por el RGPD. En cualquier caso, cuando sea necesario realizar transferencias internacionales de datos, el Encargado del Tratamiento lo pondrá en conocimiento del responsable.

La transferencia de datos personales titularidad del Responsable del Tratamiento a países que no garantizan el mismo nivel de seguridad proporcionado por el RGPD, deberá ser autorizado expresamente por el Responsable del Tratamiento, y en todo caso, el Encargado del Tratamiento deberá proporcionar las garantías suficientes para los derechos de los interesados.

En el supuesto de que la prestación del servicio implique necesariamente una transferencia internacional de datos a un tercer país que no tenga el nivel de seguridad requerido, el Encargado del Tratamiento deberá garantizar el cumplimiento de las medidas de seguridad necesarias mediante la firma de las cláusulas tipo elaboradas por la Comisión Europea o mediante la autorización de la autoridad de control correspondiente.

Decimotercera. - Publicidad del contrato

Cuando el Responsable del Tratamiento estime que la naturaleza de los datos personales objeto del tratamiento requieran de la publicidad del presente contrato, informará a los afectados sobre la identidad del Encargado del Tratamiento y de los objetivos del presente contrato.

Decimocuarta. - Derecho de Información

Los datos personales de las personas firmantes del presente contrato quedarán bajo responsabilidad de cada parte con la única finalidad de gestionar y administrar la relación contractual y las posibles responsabilidades derivadas del mismo.

El Responsable del Tratamiento será quien aplique el derecho de información sobre el tratamiento de datos personales a los afectados de acuerdo a lo recogido en el RGPD.

El Responsable del Tratamiento garantiza que los datos personales puestos a disposición del Encargado del Tratamiento para la ejecución de sus servicios son legítimos y que ha obtenido el consentimiento de los afectados de acuerdo a la normativa vigente.

En el caso de que, por razones del servicio, sea el Encargado del Tratamiento quien recabe los datos personales por cuenta del Responsable del Tratamiento, deberá ser previsto de forma expresa junto con el alcance y contenido del derecho de información.

Decimoquinta. - Derechos de los Interesados

Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, ante el Encargado del Tratamiento, éste debe comunicarlo por el correo electrónico dpd.sandetel@juntadeandalucia.es . La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

Decimosexta. - Notificaciones de violaciones de seguridad

El Encargado del Tratamiento notificará al Responsable del Tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas, y a través del correo electrónico dpd.sandetel@juntadeandalucia.es , las violaciones de seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

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

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

c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, la información se facilitará de manera gradual sin dilación indebida.

El Responsable del Tratamiento será el responsable de realizar las notificaciones de las violaciones de seguridad a las Autoridades de Protección de Datos que procedan, así como realizará las comunicaciones de las violaciones de seguridad a los afectados, cuando así se establezca por la normativa.

Decimoséptima. - Incumplimiento del presente contrato

En caso de verificarse, mediante una auditoría reglamentaria, realizada por una empresa subcontratada a tal efecto o, de cualquier otra forma, el incumplimiento por parte del Encargado del Tratamiento de cualquiera de las obligaciones estipuladas en el presente contrato, se considerará incumplimiento contractual grave y facultará al Responsable del Tratamiento para resolver el contrato y exigir del Encargado de Tratamiento la indemnización por daños y perjuicios que corresponda, entendiendo explícitamente incluidos en estos daños y perjuicios cualquier multa y/o sanción que pudiera imponer las Autoridades de Protección de Datos, como consecuencia de un eventual incumplimiento de la presente cláusula

En testimonio de conformidad con el contenido del presente, que los comparecientes aceptan en el respectivo interés y carácter con que actúan, firman el presente Contrato por duplicado, en lugar y fecha citados en el encabezamiento del mismo.

Firma: El Responsable del Tratamiento	Firma: El Encargado del Tratamiento
	MAPFRE | VIDA Ronda de los Tejares s/n. 41010 SEVILLA
D. ÁNGEL ORTIZ SÁNCHEZ	**D. JOSE MARÍA CABALLERO GÓMEZ,**

ANEXO DE MEDIDAS TÉCNICAS

El Encargado del tratamiento estará sujeto a unas medidas de seguridad que serán adecuadas para la protección de los datos personales y demás información que deberá llevarse a cabo por el Encargado del tratamiento y de acuerdo con el resultado de la evaluación de riesgos realizada por El Responsable del Tratamiento habida cuenta del estado de la tecnología, los costes de aplicación, la naturaleza de los datos almacenados, el alcance y los fines del tratamiento y los riesgos a que estén expuestos. El Anexo recoge las medidas de seguridad que el Responsable del Tratamiento establece como resultado del análisis de riesgos y la evaluación del impacto sobre la protección de los datos personales de las operaciones de tratamiento a realizar por el Encargado de tratamiento. Estas medidas de seguridad tendrán como vigencia la duración del presente contrato

El presente Anexo incluye una descripción de las medidas de seguridad físicas, técnicas y organizativas mínimas que el Encargado del tratamiento está obligado a implementar para evitar la alteración, pérdida, tratamiento o acceso no autorizado a los datos personales objeto de tratamiento, garantizando la seguridad de los mismos, de conformidad con lo dispuesto en la normativa en materia de protección de datos.

El Responsable del Tratamiento se reserva el derecho a verificar la correcta definición, funcionamiento y aplicación de dichas medidas de seguridad y el Encargado del tratamiento se compromete a facilitar las evidencias que El Responsable del Tratamiento considere necesarias. El Encargado del tratamiento deberá facilitar al Responsable del Tratamiento, las evidencias necesarias que pongan de manifiesto su cumplimiento con lo establecido en la normativa aplicable en materia de protección de datos personales así como cualquier otra información de la que disponga Como mínimo (siempre que estuviera a su disposición), la siguiente información:

- Los fines y los medios del tratamiento previsto.
- Las medidas de seguridad implementadas.
- La evaluación de impacto, en caso de que el Encargado del tratamiento haya llevado a cabo una.

En concreto, las medidas de seguridad mínimas, que el Encargado del tratamiento está obligado a implementar son las siguientes:

Verificación de las medidas de seguridad

El Responsable del Tratamiento, en cumplimiento de su capacidad de control, podrá realizar por su cuenta revisiones que verifiquen el cumplimiento de las políticas y medidas de seguridad exigidas en este acuerdo para la protección de los datos personales responsabilidad del Responsable del Tratamiento. Las revisiones podrán ser en los sistemas de información e instalaciones de tratamiento de datos del Encargado del tratamiento o bien a través de la recopilación de información que corrobore el cumplimiento por parte del Encargado del tratamiento de lo establecido en este acuerdo.

En cualquier caso, el Encargado del tratamiento se obliga a tener a disposición del Responsable del Tratamiento, de sus Auditores Externos o del regulador u otra parte interesada, la documentación (en soporte físico o electrónico) que acredite el cumplimiento de sus obligaciones conforme a lo establecido en el presente acuerdo.

Asimismo, el Encargado del tratamiento deberá acreditar que ha realizado los correspondientes análisis de riesgos y, si procede, las evaluaciones de impacto sobre la protección de datos pertinentes.

El Encargado del tratamiento se obliga a realizar auditorías y afrontar su coste siempre que exista una regulación vigente que así lo exija dentro de los servicios que presta al Responsable del Tratamiento.

El Responsable del Tratamiento se reserva el derecho de realizar auditorías afrontando su coste, y a solicitar evidencias sobre el cumplimiento de lo establecido en el presente acuerdo por el Encargado del tratamiento, de cara a cumplir aspectos regulatorios, legales y/o contractuales. En este caso, El Responsable del Tratamiento notificará al Encargado del tratamiento su voluntad de realizar dichas auditorías, con al menos quince días de antelación a la fecha en la que desee llevarlas a cabo, adaptando su realización a los protocolos y procedimientos de intervención del Encargado del tratamiento.

Adicionalmente, El Responsable del Tratamiento podrá realizar auditorías al objeto de evaluar el grado de calidad de la prestación del servicio objeto de este contrato y particularmente el nivel de cumplimiento por el Encargado del tratamiento de las mejores prácticas de seguridad (conocidos como hacking y pentesting) cuando se presten servicios que impliquen la utilización de información propiedad del Responsable del Tratamiento o proporcionada por clientes del Responsable del Tratamiento. A estos efectos, el Encargado de tratamiento se obliga (i) a colaborar en todo lo que fuere necesario para la realización de la Auditoría descrita, y (ii) a adoptar las medidas que fueren necesarias para corregir de forma inmediata las debilidades que fueran detectadas por la Auditoría, particularmente en materia de Seguridad.

En los procesos de auditoría, el Encargado del tratamiento deberá facilitar el acceso a la información adecuada para responder a las necesidades de estas partes interesadas. Las evidencias y otra documentación generada para el proceso de auditoría deberán almacenarse en un repositorio del Responsable del Tratamiento que ambas partes acuerden. A fin de facilitar o incluso evitar la revisión por parte del Responsable del Tratamiento, el Encargado del tratamiento podrá aportar las oportunas certificaciones cuyos ámbitos de aplicación incluyan los servicios y personal ofrecidos por este al Responsable del Tratamiento. Si el Encargado del tratamiento decidiera aportar las mencionadas certificaciones, deberá asimismo aportar la documentación pertinente, certificación, ámbito de aplicación, así como presentar los informes de las auditorías a las que de acuerdo a la certificación se encuentra sometida. En caso de que El Responsable del Tratamiento encontrase incumplimientos de seguridad incompatibles con lo establecido en el presente acuerdo según el análisis de riesgos realizado por éste, dependiendo de la gravedad de los mismos, podrá requerir al Encargado de tratamiento la resolución inmediata de los problemas detectados mediante la elaboración de un plan de corrección que deberá hacerse efectivo en un plazo determinado acordado por ambas partes.

Notificaciones de violaciones de seguridad

El Encargado del Tratamiento notificará al Responsable del Tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas, las violaciones de seguridad de los

datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

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

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

c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, la información se facilitará de manera gradual sin dilación indebida.

El Responsable del Tratamiento será el responsable de realizar las notificaciones de las violaciones de seguridad a las Autoridades de Protección de Datos que procedan, así como realizará las comunicaciones de las violaciones de seguridad a los afectados, cuando así se establezca por la normativa.

El Responsable del Tratamiento, realizará un seguimiento periódico del estado de la resolución del incidente, comprometiéndose el Encargado del tratamiento a colaborar con los informes que le sean solicitados.

Medidas de seguridad aplicables a los tratamientos

1) Funciones y obligaciones del personal

- Las funciones y las obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal responsabilidad del Responsable del tratamiento y a los sistemas de información estarán claramente definidas y documentadas por el Encargado de tratamiento.
- El Encargado de tratamiento deberá adoptar las medidas necesarias para que el personal con acceso a datos personales responsabilidad del Responsable del tratamiento conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

2) Registro de incidencias

- El Encargado de tratamiento deberá disponer de un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal responsabilidad del Responsable del tratamiento que contendrá un registro en el que se haga constar:

- el tipo de incidencia
- el momento en que se ha producido, o en su caso, detectado
- la persona que realiza la notificación
- a quién se le comunica
- los efectos que se hubieran derivado de la misma
- las medidas correctoras aplicadas

- El Encargado del tratamiento deberá resolver las vulnerabilidades críticas (según las escalas y métricas determinadas por CVSS) en el plazo de 1 mes desde que hayan sido detectadas y en caso de no ser críticas en el plazo máximo acordado entre ambas partes para su resolución.

3) Control de acceso

- Los usuarios deberán tener acceso únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- El Encargado del tratamiento deberá elaborar una relación actualizada de los usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos, así como establecer los mecanismos necesarios para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
- Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios que debe establecer el Encargado del tratamiento.
- Proceso formal para el control y gestión de las autorizaciones respecto a los sistemas de información y siguientes dispositivos:
  - Se mantendrá un control en la entrada y utilización de instalaciones, tanto habituales como alternativas.
  - Se mantendrá un control en la entrada de equipos en producción, en particular, equipos que involucren criptografía.
  - Se mantendrá un control en la entrada de aplicaciones en producción.
  - Se mantendrá un control en el establecimiento de enlaces de comunicaciones con otros sistemas.
  - Se mantendrá un control en la utilización de medios de comunicación (tanto habituales como alternativos).
  - Se mantendrá un control en la utilización de soportes de información.
  - Se mantendrá un control en la utilización de equipos móviles.
- Para el acceso a los datos se deberá establecer un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

4) Gestión de soportes y documentos

- Los soportes y documentos que contengan datos de carácter personal del Responsable del tratamiento deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado. Criterios de archivo. Se debe garantizar la correcta conservación, localización y consulta de los documentos y posibilitar el ejercicio de derechos.

- La salida de soportes y documentos que contengan datos de carácter personal responsabilidad del Responsable del tratamiento, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales en donde estén ubicados los ficheros, deberá ser autorizada por la persona que designe el Encargado de tratamiento o encontrarse debidamente autorizada en el documento de seguridad. Dichos soportes deberán estar cifrados.

- En el traslado de la documentación que contenga datos de carácter personal responsabilidad del Responsable del tratamiento, el Encargado del tratamiento deberá adoptar las medidas necesarias para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte. Se deberá mantener un registro de entrada y salidas de soportes o documentos que identifique quién accede y la fecha de los mismos.

- Siempre que se vaya a desechar cualquier documento o soporte que contenga datos de carácter personal responsabilidad del Responsable del tratamiento, el Encargado del tratamiento deberá proceder a su destrucción o borrado, mediante la adopción de las medidas necesarias para evitar el acceso a la información contenida en el mismo o su recuperación posterior.

- Los soportes que contengan datos de carácter personal especialmente sensibles se deberán identificar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

- Los dispositivos de almacenamiento que contengan datos de carácter personal especialmente sensibles se deberán disponer de mecanismos que obstaculicen su apertura, o en su defecto, medidas que impidan el acceso de personas no autorizadas.

- Se debe custodiar la documentación cuando no se encuentre en archivada en los dispositivos de almacenamiento.

- Se exigirá que los puestos de trabajo permanezcan despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.

5) Identificación y autenticación

- El Encargado del tratamiento debe establecer una segregación interna de funciones adecuada, con la finalidad de gestionar el riesgo de acceso por parte de usuarios no autorizados. El Encargado del tratamiento establecerá las medidas suficientes y necesarias para asegurar que los derechos de acceso (roles y perfiles) asignados internamente por el Encargado del tratamiento para prestar el servicio, lo son de acuerdo a las necesidades funcionales del proyecto y a la seguridad para el Responsable del Tratamiento.

- El Encargado del tratamiento deberá garantizar la trazabilidad de las acciones realizadas en los sistemas que almacenan información del Responsable del Tratamiento pudiendo identificarse en todo momento la persona concreta que las realizó. No se permitirá la existencia de usuarios genéricos salvo aquellos requeridos

por las tecnologías empleadas y en este caso, su uso debe estar inventariado y controlado. Debe ser aprobado y validado por el Responsable del Tratamiento.

- Si el mecanismo de autenticación se basa en la existencia de contraseñas deberá existir un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. Las contraseñas se cambiarán con la periodicidad que indique el Responsable del tratamiento, que en ningún caso será superior a un año, y mientras estén vigentes se almacenarán de forma ininteligible.

6) Copias de respaldo y recuperación

- El Encargado de tratamiento deberá encargarse de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos responsabilidad del Responsable del tratamiento y deberá realizar copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

- Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. En el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

- El Encargado del tratamiento deberá verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos de carácter personal responsabilidad del Responsable del tratamiento.

- Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal del Responsable del tratamiento no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad. Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

7) Verificación

- El Encargado de tratamiento deberá someterse a un proceso de verificación, evaluación y valoración de la eficacia de las medidas técnicas periódicamente o tras cada cambio importante en la organización.

8) Seguridad en los accesos a datos a través de redes de comunicaciones

- Las medidas de seguridad exigibles a los accesos a través de redes de comunicaciones deben garantizar un nivel de seguridad equivalente a los accesos en modo local anteriormente mencionados.

- El Encargado de tratamiento deberá garantizar que las comunicaciones se realizan mediante protocolos de comunicación seguros (SSH, S-FTP, Editran, SSL, IPSec VPN, etc.). La transmisión de datos a través de redes públicas o de redes inalámbricas debe ser cifrada por algoritmos acreditados por el CCN.

- El Encargado de tratamiento deberá establecer mecanismos de defensa perimetral a la red (Cortafuegos, Proxy, DMZ, IPS/IDS, etc.).
- El Encargado del tratamiento deberá garantizar el adecuado aislamiento entre los diferentes clientes.
- Ambas partes se comprometen a reducir al mínimo necesario las conexiones entre ambas empresas.
- El Encargado del tratamiento deberá tomar las medidas preventivas necesarias para evitar que un incidente potencial en cualquier elemento de su red sea propagado al Responsable del Tratamiento.
- El Responsable del Tratamiento podrá realizar auditorías técnicas para validar la adecuada segmentación de dichas redes así como el nivel de seguridad de los elementos conectados.

8) Registros de accesos

- Para todo tratamiento de dato sensible el prestador de servicios todas las actividades de los usuarios en el sistema de información. Deberá indicar quién realiza la actividad, cuándo la realiza y sobre qué información, sea cual sea el usuario.
- El registro de acceso se mantendrá un mínimo de los dos últimos años de forma ininterrumpida.
- El Encargado de tratamiento revisará mensualmente los registros de accesos y emitirá un informe con las incidencias surgidas durante la revisión, que podrá ser solicitado por el Responsable del Tratamiento.

9) Planes de contingencia y continuidad

- Planes de contingencia para los servicios que van a prestarse al Responsable del Tratamiento El plan de contingencia deberá haber sido probado o disponer de un plan de pruebas y como tal el Encargado de tratamiento deberá facilitar evidencias, resultado y/o la realización de las pruebas si así lo requiere el Responsable del Tratamiento.
- Plan de continuidad del Encargado de tratamiento. El plan de continuidad deberá haber sido probado y como tal el Encargado de tratamiento deberá facilitar evidencias y resultado de su última prueba si así lo requiere el Responsable del Tratamiento.

10) Cifrado

- Se protegerá la Información que contenga datos sensibles (datos especialmente protegidos: datos de ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual, datos genéticos, biométricos, las infracciones y condenas penales, aunque no las administrativas) almacenados en el disco mediante cifrado, de manera que un tercero no autorizado no pueda leerla.

11) Para encargados de tratamiento que desarrollen software

- El desarrollo de software se realizará sobre la base de las mejores prácticas de la industria, debiendo velar en todo el ciclo de desarrollo del software (diseño, desarrollo y prueba) por la seguridad de la información.

- El desarrollo de las aplicaciones web (tanto internas como externas siempre que incluyan acceso administrativo web a la aplicación) se basarán en directrices de codificación segura tales como la Guía OWASP (Open Web Application Security Project / Proyecto abierto de seguridad de aplicaciones web), por lo que el Encargado de tratamiento deberá enfocar la seguridad de aplicaciones informáticas desarrolladas considerando ésta todas sus dimensiones: personas, procesos y tecnologías.

Responsable del Tratamiento_____ Fdo._____	_____ Fdo._____

MAPFRE | VIDA
Ronda de los Tejares s/n.
41010 SEVILLA