

En _____, a _____ de _____ de _____

REUNIDOS:

De una parte, “Mutualia”, Mutua Colaboradora con la Seguridad Social nº 2 (en adelante, “Mutualia”, “la Mutua” o el “RESPONSABLE del Tratamiento”) con sede operativa y domicilio a efectos de notificaciones en 48009 BILBAO, c/ Henao, nº 26, provista de CIF nº G-95471165, actuando en su nombre y representación **IGNACIO LEKUNBERRI HORMAETXEA**, mayor de edad, con DNI nº 30.565.289-Z y a efectos del presente en el mismo domicilio, como **Director Gerente**, y especialmente facultado en virtud de escritura de poder otorgada a su favor.

De otra parte _____, (en adelante, “Proveedor”, “Empresa”, “Empresa proveedora” o “Adjudicataria”, o “ENCARGADO de Tratamiento”), con domicilio en _____, provista de CIF/NIF núm. _____, representada en este acto por _____, mayor de edad, DNI/Pasaporte/NIE núm. _____ en su calidad de _____ (indicar puesto/cargo de representación)

MANIFIESTAN

- a) Que ambas partes tienen suscrita y vigente una relación contractual según contrato firmado, en virtud de la cual es o puede ser necesario el **tratamiento de datos de carácter personal**; conociendo al respecto las **exigencias de cumplimiento normativo** previstas en el REGLAMENTO (UE) 2016/679 de 27 de abril de 2016 GENERAL DE PROTECCIÓN DE DATOS (en adelante, *RGPD* -) la LEY ORGÁNICA 3/2018 de 5 de diciembre de protección de datos personales y garantía de los derechos digitales (en adelante, *LOPDGDD*) y el REAL DECRETO-LEY 14/2019, de 31 de octubre de medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones; y demás normativa que sea aplicable, complementaria, de desarrollo, o conexas, incluso, en lo que pueda resultar de aplicación, las cláusulas contractuales tipo publicadas por DECISIÓN DE EJECUCIÓN (UE) 2021/915 DE LA COMISIÓN de 4 de junio de 2021 (DOUE de 07.06.2021). Ambas partes están conformes en que la obligación de someterse en todo caso a la normativa nacional y de la Unión Europea en materia de protección de datos tiene el carácter de obligación contractual ESENCIAL.
- b) Si la ejecución del contrato (principal) que une a ambas partes implica el tratamiento (por el PROVEEDOR) por cuenta de Mutualia, de datos de carácter personal de los cuales sea RESPONSABLE Mutualia, el PROVEEDOR tendrá en ese caso la condición jurídica de **ENCARGADO DE TRATAMIENTO**, según regula el art. 28 RGPD y los arts. 28 y 33 LOPDGDD. En este supuesto, el acceso a esos datos no se considerará comunicación de datos, cuando se cumpla lo previsto en los preceptos antes indicados; para lo cual han venido a pactar el presente CONTRATO DE CONFIDENCIALIDAD, SEGURIDAD EN LA INFORMACIÓN Y CUMPLIMIENTO NORMATIVO DE PROTECCIÓN DE DATOS PERSONALES,) conforme a las siguientes:

CLÁUSULAS

1.- PREVIAS

- 1.1. Si la ejecución del contrato (principal) que une a ambas partes implica el tratamiento (por el adjudicatario PROVEEDOR) por cuenta de Mutualia, de datos de carácter personal de los cuales sea RESPONSABLE Mutualia, el PROVEEDOR tendrá en ese caso la condición jurídica de ENCARGADO DE TRATAMIENTO, según regula el art. 28 RGPD y los arts. 28 y 33 LOPDGDD
- 1.2. La finalidad del presente contrato es garantizar que se cumpla el **art. 28, apartados 3 y 4 del RGPD**. El responsable y el encargado del tratamiento identificados en el encabezamiento de este contrato han dado su consentimiento a vincularse por el presente contrato a fin de garantizar tal cumplimiento normativo del art. 28 RGPD
- 1.3. **El presente clausulado se aplica al tratamiento de datos personales que forma parte del contrato principal**. En el ANEXO se especifican las operaciones de tratamiento y las categorías de interesados y de datos personales que el encargado trata por cuenta del responsable. El **plazo** de duración del tratamiento de datos por el ENCARGADO se

corresponderá con la vigencia/ejecución del contrato principal, salvo que en cumplimiento de normativa que sea de aplicación deban prolongarse en plazos más prolongados conforme a lo previsto en la cláusula 2.7.

- 1.4. El presente contrato se entiende **sin perjuicio de todas las obligaciones a las que esté sujeto el RESPONSABLE** en virtud del RGPD.
- 1.5. Las partes se comprometen a no modificar el presente contrato, excepto para añadir o actualizar información en el ANEXO. Sin perjuicio de lo anterior, las partes podrán acordar **añadir en una adenda** otras cláusulas o garantías adicionales, siempre que no contradigan, directa o indirectamente, el presente contrato ni perjudiquen los derechos o libertades fundamentales de las personas interesadas.
- 1.6. Cuando en el presente contrato se utilicen **términos** definidos en el RGPD, se entiende que tienen el mismo significado que en tal Reglamento. El presente contrato deberá leerse e interpretarse con arreglo a las disposiciones de tal Reglamento. No se podrán realizar **interpretaciones** del presente contrato que entren en conflicto con los derechos y obligaciones establecidos en citado Reglamento y/o que perjudiquen los derechos o libertades fundamentales de las personas interesadas. **En caso de contradicción** entre el presente contrato y las disposiciones de acuerdos/contratos conexos entre las partes que estuvieren en vigor en el momento en que se pactare o comenzare a aplicarse el presente contrato, prevalecerá el presente contrato
- 1.7. Las partes deberán poder **demostrar** el cumplimiento del presente contrato. El ENCARGADO resolverá con presteza y de forma adecuada las consultas del RESPONSABLE relacionadas con el tratamiento con arreglo al presente contrato. El ENCARGADO pondrá a disposición del responsable toda la **información** necesaria para demostrar el cumplimiento de las obligaciones contempladas en el presente contrato y que deriven directamente del RGPD o de cualquier otra normativa de Protección de Datos que sea de aplicación.

En relación a lo anterior, a instancia del RESPONSABLE, el ENCARGADO deberá permitir y contribuir a la realización de **auditorías** de las actividades de tratamiento cubiertas por el presente contrato, a intervalos razonables o si existen indicios de incumplimiento. Al decidir si se realiza **un examen o una auditoría**, el RESPONSABLE podrá tener en cuenta las **certificaciones** pertinentes que obren en poder del ENCARGADO. El RESPONSABLE podrá optar por realizar la auditoría por sí mismo o autorizar a un auditor independiente. Las auditorías también podrán consistir en **inspecciones de los locales o instalaciones físicas** del ENCARGADO y, cuando proceda, realizarse con un preaviso razonable.

Las partes pondrán a disposición de las **autoridades de control** competentes, a instancia de estas, la información a que se refiere la presente cláusula y, en particular, los resultados de las auditorías

2. **Obligaciones específicas del ENCARGADO de tratamiento, que este se compromete a cumplir.**

- 2.1. El ENCARGADO tratará los datos personales únicamente siguiendo **instrucciones** del RESPONSABLE (incluidas las contenidas y/o las que se deduzcan del contrato principal y/o de los Pliegos de Condiciones Administrativas Generales y Particulares y/o de Prescripciones Técnicas del expediente de contratación aplicables a la ejecución del contrato). El RESPONSABLE también podrá dar instrucciones ulteriores en cualquier momento del período de tratamiento de los datos personales. Dichas instrucciones deberán estar siempre documentadas. El ENCARGADO informará inmediatamente al RESPONSABLE si las instrucciones dadas por el responsable infringen, a juicio del encargado, el RGPD o las disposiciones aplicables del Derecho de la Unión o de los Estados miembros en materia de protección de datos

Todo lo anterior será de aplicación salvo que el ENCARGADO esté obligado al tratamiento en virtud del Derecho de la Unión o de alguno de los Estados miembros que se le aplique a este. En este último caso, el ENCARGADO informará al RESPONSABLE de esa exigencia legal previa al tratamiento, salvo que tal normativa prohíba tal información por razones importantes de interés público.

- 2.2. El ENCARGADO tratará los datos personales únicamente para los **finés específicos** del tratamiento relacionados con el cumplimiento del contrato principal o siguiendo instrucciones adicionales del responsable. En ningún caso, se

efectuarán tratamientos de datos personales para finalidades incompatibles con el fin para el cual han sido recogidas o con una **finalidad distinta** a la ejecución del objeto del contrato principal. En los supuestos en los que en virtud del Derecho de la Unión Europea o del Estado miembro que le resulte de aplicación a la empresa proveedora, le obligue a un determinado y específico tipo de tratamiento de los datos, incluso en contra de las instrucciones expresas de MUTUALIA, se justificará y se informará de tal eventual situación a MUTUALIA para adaptar las medidas organizativas, jurídicas y de seguridad oportunas

- 2.3. El ENCARGADO aplicará, como mínimo, las **medidas técnicas y organizativas apropiadas** para garantizar un **nivel de seguridad** de los datos personales adecuado al riesgo, que en su caso incluya, entre otros: a) la **seudonimización** 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; c) la capacidad de restaurar la **disponibilidad y el acceso** a los datos personales de forma rápida en caso de incidente físico o técnico; d) un proceso de **verificación, evaluación y valoración regulares** de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular (**protección contra violaciones de la seguridad**) como consecuencia de la **destrucción, pérdida o alteración accidental o ilícita** de datos personales transmitidos, conservados o tratados de otra forma, o la **comunicación o acceso no autorizados** a dichos datos.

A la hora de determinar un nivel adecuado de seguridad, se tendrá debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, y los riesgos que entraña el tratamiento para las personas interesadas. No obstante lo anterior, **en cualquier caso**, se indican a continuación las **medidas mínimas de seguridad** que, al menos, debe cumplir el ENCARGADO:

- **Autorización de personal usuario:** Exigencia de autorización de acceso a datos personales validada por responsable. Segregación de roles según confidencialidad del dato. Medidas tecnológicas que limitan accesibilidad a la información en base a los permisos. Listado de usuarios con acceso a la información. Actualización del listado.
- **Identificación y autenticación:** Exigencia de credenciales de acceso que identifiquen a los usuarios de manera inequívoca y personalizada mediante usuario y contraseña de acceso robusta a los sistemas de información, con actualización periódica manual de contraseña. Registro especial de accesos a categorías especiales de datos (si es el caso)
- **Soportes:** Se deberá disponer de una relación actualizada de personas autorizadas a tratar soportes con datos personales. Medidas de seguridad en caso de traslados de soportes fuera de las instalaciones para evitar sustracción, pérdida o acceso indebido durante el transporte (como el cifrado y/o etiquetado externo únicamente comprensible a nivel interno de la organización a fin de impedir el acceso no autorizado). Restricción de uso de soportes de memoria extraíbles (pendrives, DVDs y similares)
- **Copias de respaldo:** Implantar y aplicar procedimientos de copias de respaldo de los datos personales a fin de impedir la pérdida y/o destrucción de información.
- **Telecomunicaciones y envío de datos:** En caso de envío de datos especialmente protegidos (ejemplo: datos de salud) a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará **cifrando** dichos datos o utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.
- **Medidas de control de acceso a instalaciones y dependencias.** Los **servidores**, en su caso, protegido por dispositivos de apertura y designación de persona responsable
- Protección con **contraseña** el acceso a información personal contenida en **dispositivos portátiles**.
- **Antivirus** actualizado y con escaneos periódicos. **Sistema operativo** permanentemente actualizado
- **Acceso desde el exterior de la red** a los Sistemas de Información protegido con identificación de usuario y comunicaciones cifradas. Si existe un **WIFI** de empresa, tiene medidas de seguridad
- **Formación y concienciación** periódica a las personas empleadas sobre la confidencialidad de los datos y la seguridad. Las personas empleadas que acceden a datos personales (especialmente las que desempeñen funciones sensibles) firman **compromisos escritos de confidencialidad**

- **Gestión de soportes o documentos en papel:** En caso de que el ENCARGADO de tratamiento deba conservar, archivar, custodiar y/o trasladar documentos y **soportes en formato papel con datos personales** deberá aplicar las siguientes medidas de seguridad:
 - o Los medios/dispositivos de almacenamiento de documentos tienen mecanismos de apertura tipo llaves o tarjetas electrónicas, o cualquier otra medida que impidan el acceso de personas no autorizadas.
 - o Política (implantada) de "*mesas limpias*"
 - o Los soportes o documentos en proceso de revisión o tramitación deberán ser custodiados por personal a cargo de la misma e impedir en todo momento que pueda ser accedidos por persona no autorizada.
 - o Durante el traslado físico de la documentación deberán adoptarse medidas para impedir el acceso no autorizado o manipulación de la información (contenedores opacos y medios de transporte protegidos e inaccesibles por cualquier tercero - con llave o sistema equivalente -).
 - o Para destruir datos en papel se utilizarán las destructoras de tal modo que resulte imposible reconstruir los datos a un estado anterior que permita identificar datos personales.

Si el tratamiento afecta a **datos personales sensibles** (que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, o datos relativos a condenas e infracciones penales), el ENCARGADO aplicará restricciones específicas y/o garantías adicionales, que en su caso procedan.

En relación a todas las obligaciones contenidas en este punto 2.3., **se entenderá que el ENCARGADO cumple con un nivel adecuado de medidas técnicas y organizativas de seguridad si dispone de una certificación** (emitida por entidad auditora externa) de Seguridad de la Información tipo **ISO 27001 o equivalente** y/o del cumplimiento en su organización del **Esquema Nacional de Seguridad (ENS)**, siempre que el servicio objeto de contrato esté dentro del alcance de dicha certificación. En este caso, el RESPONSABLE podrá verificar la constancia documental de tales certificaciones, las cuales deberán estar vigentes a lo largo de la duración del contrato.

- 2.4. El ENCARGADO y su personal deberá mantener la más absoluta **confidencialidad** sobre los datos personales a los que tenga acceso para la ejecución del contrato, así como sobre los que resulten de su tratamiento, cualquiera que sea el soporte en el que se hubieren obtenido. Esta obligación se extiende a toda persona que pudiera intervenir en cualquier fase del tratamiento por cuenta del adjudicatario, siendo deber del adjudicatario instruir a las personas que de él dependan de este **deber de confidencialidad**, y del mantenimiento de dicho deber aún después de la terminación de la prestación del Servicio o de su desvinculación de la empresa.

El ENCARGADO solo concederá **acceso a los datos** personales tratados a las personas trabajadoras y/o miembros de su organización/personal en la medida en que sea estrictamente necesario para la ejecución, la gestión y el seguimiento del contrato (principal). El encargado garantizará que las personas autorizadas para tratar los datos personales recibidos se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

Incluso en el caso de tratamientos de datos especialmente sensibles; y/o en el caso de acceso/tratamiento (in situ o en remoto) de datos con privilegios de administrador y/o de mantenimiento/desarrollo tecnológico en los Sistemas de Información de Mutualia, esta podrá requerir directamente a las personas empleadas/colaboradoras del ENCARGADO la firma de específicos compromisos escritos de confidencialidad en los modelos propios, como requisito previo para el acceso a los datos por tal personal.

- 2.5. El ENCARGADO y su personal **no podrá comunicar ni difundir los datos personales a terceros, salvo** en los supuestos en los que en virtud del Derecho de la Unión Europea o del Estado miembro que le resulte de aplicación al ENCARGADO, le obligue y/o ampare jurídicamente a realizar tal comunicación.
- 2.6. El ENCARGADO deberá comunicar a Mutualia los datos de contacto de su **Delegado de Protección de Datos** (en caso de que lo tenga designado por serle legalmente obligatorio o decidido voluntariamente), lo cual se cumplimentará en el ANEXO al presente documento.

- 2.7. **Una vez finalizada la prestación contractual**, el ENCARGADO **suprimirá**, a petición del responsable, todos los datos personales tratados por cuenta del responsable y acreditará al responsable que lo ha hecho, **o devolverá** todos los datos personales al responsable y **suprimirá las copias** existentes; todo lo anterior **salvo** que por norma de Derecho de la UE o del Estado miembro que le sea de aplicación al ENCARGADO, este deba conservarlos. En este último caso, los datos personales se conservarán bloqueados por el tiempo mínimo necesario, procediendo a su supresión de forma segura y definitiva al final de dicho plazo cuando proceda legalmente su destrucción. Hasta que se destruyan o devuelvan los datos, el encargado seguirá garantizando el cumplimiento con el presente documento de cláusulas.
- 2.8. Los datos personales objeto de tratamiento se encontrarán disponibles por el ENCARGADO para su **acceso por parte de las autoridades judiciales y administrativas competentes** cuando así lo disponga el Derecho de la Unión Europea o del Estado miembro que le resulte de aplicación, o por mandato administrativo/judicial.
- 2.9. En aquellos supuestos en los que, por razón de cumplimiento del presente contrato, sea necesaria la utilización de medidas de **identificación electrónica**, éstas serán las determinadas por la autoridad competente y conforme a la normativa vigente. Para el cumplimiento de las obligaciones dimanantes de este contrato o del principal, **no** será posible utilizar **tecnologías de registros distribuidos** mientras estas no estén legalmente autorizadas/reguladas.
- 2.10. El ENCARGADO **notificará** con presteza al RESPONSABLE (en todo caso antes tres (3) días hábiles siguientes al de su recepción) de las **solicitudes y/o ejercicio de derechos que reciba de las personas interesadas**. No responderá a dicha solicitud por sí mismo, a menos que el responsable le haya autorizado a hacerlo. El ENCARGADO **ayudará** al RESPONSABLE a cumplir sus obligaciones al responder a las solicitudes de ejercicio de derechos de las personas interesadas teniendo en cuenta la naturaleza del tratamiento. En el cumplimiento de tales obligaciones, el ENCARGADO cumplirá las **instrucciones** del responsable.
- 2.11. El ENCARGADO también **ayudará al RESPONSABLE** a garantizar el cumplimiento de las obligaciones siguientes (teniendo en cuenta la naturaleza del tratamiento y la información de que disponga el ENCARGADO):
- a) la obligación de realizar una **evaluación del impacto** de las operaciones de tratamiento en la protección de datos personales cuando sea probable que un tipo de tratamiento suponga un alto riesgo para los derechos y libertades de las personas físicas
 - b) la obligación de **consultar a las autoridades de control competentes** antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo;
 - c) la obligación de **garantizar que los datos personales sean exactos y estén actualizados**, informando sin demora al responsable si el ENCARGADO descubre que los datos personales que está tratando son inexactos o han quedado obsoletos;
 - d) las obligaciones contempladas en el **artículo 32 del RGPD**.
- 2.12. En caso de **violación de la seguridad de los datos personales**, el ENCARGADO **colaborará con el RESPONSABLE** y le ayudará a cumplir las obligaciones que le atribuyen los artículos 33 y 34 del RGPD, en su caso, teniendo en cuenta la naturaleza del tratamiento y la información de que disponga el ENCARGADO.
- En caso de **violación de la seguridad de los datos personales** en relación con los **datos tratados por el RESPONSABLE**, el ENCARGADO **ayudará** al responsable en lo siguiente.
- a) Notificar, si así procede conforme al RGPD, la violación de la seguridad de los datos personales a las autoridades de control competentes sin dilación indebida una vez tenga constancia de ella, si así procede conforme a la normativa de Protección de Datos de aplicación.
 - b) Recabar la información siguiente, que, de conformidad con el artículo 33, apartado 3, del RGPD, deberá figurar en la notificación del responsable, que debe incluir como mínimo:
 - 1) la naturaleza 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;
 - 2) las consecuencias probables de la violación de la seguridad de los datos personales;
 - 3) las medidas adoptadas o propuestas por el responsable del tratamiento 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. Cuando y en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.

4) Cumplir, cuando así proceda conforme al artículo 34 del RGPD, la obligación de comunicar sin dilación indebida al interesado la violación de la seguridad de los datos personales cuando sea probable que la violación de la seguridad entrañe un alto riesgo para los derechos y libertades de las personas físicas.

En caso de **violación de la seguridad de datos personales tratados por el ENCARGADO**, este lo **notificará al RESPONSABLE sin dilación indebida (antes de 24 horas desde su constancia)** una vez que el encargado tenga constancia de ella. Dicha notificación deberá incluir como mínimo:

- a) una descripción de la naturaleza de la violación de la seguridad (inclusive, cuando sea posible, las categorías y el número aproximado de interesados y de registros de datos afectados);
- b) los datos de un punto de contacto en el que pueda obtenerse más información sobre la violación de la seguridad de los datos personales;
- c) sus consecuencias probables y las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad, incluyendo las medidas adoptadas para mitigar los posibles efectos negativos.

Cuando (en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial) se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.

2.13 El ENCARGADO llevará un **registro de las actividades de tratamiento** efectuadas por cuenta de MUTUALIA.

2.14 El ENCARGADO solo podrá **subcontratar** a un **SUBENCARGADO** las operaciones de tratamiento que realice por cuenta del responsable en virtud del presente contrato con la **autorización previa específica por escrito** del RESPONSABLE. El ENCARGADO presentará la solicitud de autorización específica al menos diez (10) días hábiles antes de la contratación del SUBENCARGADO de que se trate, junto con la información necesaria para que el responsable pueda resolver la solicitud. Así mismo, el ENCARGADO informará al RESPONSABLE de cualquier cambio previsto en la incorporación o sustitución de otros subcontratistas, dando así al RESPONSABLE la oportunidad de otorgar el consentimiento previsto en esta cláusula. En cualquiera de los casos citados, la no respuesta expresa por el RESPONSABLE a la solicitud por el ENCARGADO equivale a no autorizar la subcontratación o a los cambios en esta.

Cuando el ENCARGADO contrate a un SUBENCARGADO para llevar a cabo actividades de tratamiento específicas (por cuenta del RESPONSABLE), lo hará por medio de un contrato que imponga al SUBENCARGADO, en esencia, las mismas obligaciones en materia de protección de datos que las impuestas al encargado en virtud del presente contrato. El ENCARGADO se asegurará de que el SUBENCARGADO cumpla las obligaciones a las que esté sujeto en virtud del presente contrato y del RGPD y demás normativa de Protección de Datos que en su caso sea de aplicación. Esta obligación se podrá cumplimentar también, previo acuerdo de las tres partes (responsable, encargado y sub encargado) mediante la fórmula de ADHESIÓN a lo dispuesto en este contrato.

El ENCARGADO proporcionará al RESPONSABLE, a instancia de este, una copia del contrato con el SUBENCARGADO y de cualquier modificación posterior del mismo. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como datos personales, el ENCARGADO podrá expurgar el texto del contrato antes de compartir la copia.

El ENCARGADO seguirá siendo plenamente responsable ante el RESPONSABLE del cumplimiento de las obligaciones que imponga al SUBENCARGADO su contrato con el encargado. El ENCARGADO notificará al responsable los incumplimientos por parte del SUBENCARGADO de las obligaciones que le atribuya dicho contrato.

Especialmente, el ENCARGADO (empresa adjudicataria) deberá manifestar si tienen previsto subcontratar los recursos y/o servicios necesarios para la recogida, almacenamiento, tratamiento y gestión de la información con datos personales, o cualquier servicio asociado a los mismos (primordialmente, si hay previsión de subcontratación de tales servicios en **sistemas "cloud" o "en la nube"**), debiendo asegurarse en tal caso de las condiciones de solvencia profesional o técnica de las empresas subcontratistas a los que se vaya a encomendar tal servicio y verificar que estos cumplen con lo dispuesto en este contrato y que les resulte de aplicación, advirtiéndose que esta obligación tiene el carácter de obligación contractual ESENCIAL. La empresa adjudicataria firmante de este contrato

deberá para ello informar dónde van a estar ubicados los servidores y desde dónde se van a prestar los servicios asociados a los mismos, debiendo comunicar cualquier cambio que se produzca, a lo largo de la vida del contrato. Toda la información anterior se cumplimentará en el ANEXO de este documento.

- 2.13. En caso de ser necesario y producirse **accesos remotos** por el ENCARGADO de Tratamiento a los sistemas de información de MUTUALIA, el ENCARGADO se obliga a no aprovechar el acceso o tratamiento que pudiera tener a datos de carácter personal por razón del servicio que presta para usarlos, tratarlos o cederlos con infracción de la legislación vigente en esta materia, ni para fines distintos de aquellos que sean precisos para propiciar el desarrollo y cumplimiento del servicio prestado, siguiendo estrictamente las instrucciones del RESPONSABLE de Tratamiento.
- 2.14. Las **transferencias de datos a un tercer país o a una organización internacional** por parte del encargado solo podrán realizarse siguiendo instrucciones documentadas del RESPONSABLE o en virtud de una exigencia expresa del Derecho de la Unión o del Estado miembro al que esté sujeto el encargado; se llevarán a cabo de conformidad con el capítulo V del RGPD.

El RESPONSABLE se aviene a que, cuando el ENCARGADO recurra a un **SUBENCARGADO** de conformidad con lo previsto en este contrato para llevar a cabo actividades de tratamiento específicas (por cuenta del RESPONSABLE) y dichas actividades conlleven una transferencia de datos personales en el sentido del capítulo V del RGPD, el ENCARGADO y el SUBENCARGADO puedan garantizar el cumplimiento normativo de tal capítulo V utilizando **cláusulas contractuales tipo** adoptadas por la Comisión Europea, con arreglo al artículo 46, apartado 2, del RGPD, siempre que se cumplan las condiciones para la utilización de dichas cláusulas contractuales tipo

No obstante todo lo anterior, en el caso que la ejecución del contrato principal exija de su tratamiento, los sistemas de información y comunicaciones para la recogida, almacenamiento, procesamiento y gestión de **datos de usuarios del Sistema Nacional de Salud**, así como los correspondientes tratamientos de sus datos personales, deberán ubicarse y prestarse **dentro del territorio de la Unión Europea**. Estos datos no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales; advertiéndose de que esta obligación tiene el carácter de **obligación contractual esencial**.

TERCERA. - Disposiciones finales comunes a las cláusulas PRIMERA y SEGUNDA:

- 3.1 Sin perjuicio de lo dispuesto en el RGPD, **en caso de que el ENCARGADO del tratamiento incumpla las obligaciones que le atribuye el presente contrato, el RESPONSABLE podrá ordenar al ENCARGADO que suspenda el tratamiento** de datos personales hasta que este vuelva a dar cumplimiento al presente pliego de cláusulas, o resolver el contrato (principal). El ENCARGADO informará con presteza (antes de 48 horas) al RESPONSABLE en caso de que no pueda dar cumplimiento al presente contrato por cualquier motivo
- 3.2 **El RESPONSABLE estará facultado para resolver el contrato (principal) en lo que se refiera al tratamiento de datos personales** en virtud del presente contrato cuando:
- 1) el tratamiento de datos personales por parte del encargado haya sido suspendido por el responsable con arreglo al apartado anterior y no se vuelva a dar cumplimiento al presente contrato en un plazo razonable y, en cualquier caso, en un plazo de un (1) mes a contar desde la suspensión;
 - 2) el ENCARGADO incumpla de manera sustancial o persistente el presente contrato y/o las obligaciones que le atribuye el RGPD
 - 3) el ENCARGADO incumpla una resolución vinculante de un órgano jurisdiccional competente o de las autoridades de control competentes en relación con las obligaciones que les atribuye el presente contrato y/o el RGPD
- 3.3. **El ENCARGADO estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales** en virtud del presente contrato si, tras haber informado al RESPONSABLE de que sus instrucciones infringen los requisitos jurídicos exigidos conforme a lo previsto en la cláusula 2.1 de este contrato, el RESPONSABLE insiste en que se sigan dichas instrucciones.
- 3.4. **Tras la resolución del contrato**, el ENCARGADO suprimirá, a petición del RESPONSABLE, todos los datos personales tratados por cuenta del responsable y acreditará al responsable que lo ha hecho, o **devolverá todos los datos**

personales al RESPONSABLE y suprimirá las copias existentes, a menos que el Derecho de la Unión o de los Estados miembros exija el almacenamiento de los datos personales. Hasta que se destruyan o devuelvan los datos, el encargado seguirá garantizando el cumplimiento con el presente pliego de cláusulas

- 3.5. **Las obligaciones y prestaciones que se contienen en este documento no son onerosas/retribuidas** ni generan derechos u obligaciones económicos distintas de las contempladas en el contrato y/o pliegos/documentos con valor contractual del objeto del servicio cuya ejecución requiere el tratamiento de datos.
- 3.6. Lo previsto en el presente documento y demás documentos contractuales tendrán la misma **duración** que la prestación del servicio, prorrogándose en su caso por períodos iguales a éste. No obstante, a la finalización del contrato, el **deber de secreto** continuará vigente, sin límite de tiempo, para todas las personas involucradas en la ejecución del contrato.
- 3.7. **Mutualia se reserva el derecho a ejercitar todas las acciones y medidas legales** (civiles, laborales, administrativas y/o penales) que le amparen para su propia defensa y/o para exigir/repetir las responsabilidades oportunas que procedan en caso de incumplimiento de sus obligaciones por parte del ENCARGADO de tratamiento.

ANEXO

Descripción del servicio y naturaleza, finalidad, objeto del tratamiento de datos (describir brevemente)	

Datos de contacto del Delegado de Protección de Datos (DPD)	
	Datos de contacto del Delegado de Protección de Datos de MUTUALIA: dpd@mutualia.es . Datos de contacto del Delegado de Protección de Datos del ENCARGADO:@..... (Si no se cumplimenta este dato se entiende que el ENCARGADO no tiene obligación de tener DPD, ni lo ha designado voluntariamente)
Categorías de personas interesadas cuyos datos se tratan (marcar con una X los que procedan)	
	<input type="checkbox"/> PERSONAS TRABAJADORAS Y/O PACIENTES (trabajadores protegidos por Mutualia: cuenta ajena o autónomos) <input type="checkbox"/> PERSONAS DE MUTUALIA (de su plantilla y/o representantes de sus órganos de gobierno/participación) <input type="checkbox"/> PERSONAS DE OTRAS EMPRESAS/ORGANIZACIONES/ENTIDADES (de su plantilla y/o representantes) <input type="checkbox"/> PERSONAS VISITANTES (en controles de accesos a instalaciones) <input type="checkbox"/> PERSONAS CANDIDATAS (en procesos de selección/contratación de personas, ejemp: CV) <input type="checkbox"/> PERSONAS DOCENTES O DISCENTES (en acciones formativas) <input type="checkbox"/> OTRAS PERSONAS (reseñar).....
Categorías de datos tratados (marcar con una X los que procedan)	
	<input type="checkbox"/> DATOS DE IDENTIFICACIÓN (Ejemp: nombre, apellidos, nº DNI/Pasaporte/S.S./Tarjeta sanitaria/Tarjeta de residente/Permiso conducción, dirección IP, firma manuscrita y/o electrónica ...) <input type="checkbox"/> DATOS DE CONTACTO (Ejemp: dirección postal/electrónica, nº teléfono...) <input type="checkbox"/> CARACTERISTICAS PERSONALES (Ejemp: sexo; estado civil; nacionalidad, edad; fecha y lugar de nacimiento; lengua materna; altura; peso; características antropométricas; marcas físicas...) <input type="checkbox"/> CIRCUNSTANCIAS FAMILIARES/SOCIALES (Ejemp: nº, nombre y edad de los hijos; permisos, licencias y autorizaciones; filiación; pertenencia a clubes/asociaciones; ayudas y subvenciones; permiso de residencia...) <input type="checkbox"/> DATOS DE IMAGEN/VOZ/AUDIO (Ejemp: cuando se tomen o graben imágenes, videos, ...) <input type="checkbox"/> DATOS ECONOMICOS, TRIBUTARIOS, FINANCIEROS Y DE SEGUROS (Ejemp: nominas/recibos salariales/finiquitos, impuestos, productos financieros, pólizas de seguro, ingresos; rentas; inversiones; créditos; préstamos; avales; deducciones/retenciones tributarias; datos bancarios; datos de actividad económica y solvencia; bienes patrimoniales; planes de pensión y jubilación...) <input type="checkbox"/> LABORALES (Ejemp: empleo/puesto/cargo; categoría o grupo profesional; empresa; datos no económicos de nómina; datos de contacto corporativos; permiso de trabajo, Curriculum vitae...) <input type="checkbox"/> ACADEMICOS/PROFESIONALES (Ejemp: titulaciones; formación; experiencia profesional; expediente académico; alta en colegios profesionales, creaciones artísticas, literarias, científicas o técnicas, titularidad de licencias comerciales, marcas, patentes...) <input type="checkbox"/> ADMINISTRATIVOS/JUDICIALES (Ejemp: Procedimientos administrativos; Reclamaciones y recursos; Sanciones; Registros; Solicitudes; Procedimientos judiciales ...) <input type="checkbox"/> DATOS DE CONDENAS E INFRACCIONES PENALES (Ejemp: antecedentes penales, certificado antecedentes delitos de naturaleza sexual, autos y sentencias penales ...) <input type="checkbox"/> GEOLOCALIZACION <input type="checkbox"/> VIDEOVIGILANCIA <input type="checkbox"/> DATOS DE SALUD <input type="checkbox"/> DATOS BIOMETRICOS <input type="checkbox"/> DATOS GENETICOS <input type="checkbox"/> OPINIONES POLITICAS/CONVICIONES RELIGIOSAS/FILOSOFICAS <input type="checkbox"/> AFILIACION SINDICAL <input type="checkbox"/> DATOS RELATIVOS A LA VIDA SEXUAL/ORIENTACIÓN SEXUAL <input type="checkbox"/> PATRONES/PERFILES DE COMPORTAMIENTO <input type="checkbox"/> OTROS (reseñar).....
Declaración sobre Naturaleza del tratamiento (marcar con una X los que procedan)	

<p>Indicar cuales de los siguientes tipos de tratamientos de datos personales está previsto realizar en la ejecución del contrato principal - (marcar una X en lo que proceda)</p> <ul style="list-style-type: none"><input type="checkbox"/> RECOGIDA/REGISTRO/CONSERVACION de los datos<input type="checkbox"/> ORGANIZACIÓN/ESTRUCTURACIÓN de los datos<input type="checkbox"/> CONSULTA/UTILIZACION de los datos<input type="checkbox"/> MODIFICACIÓN/ADAPTACIÓN de los datos<input type="checkbox"/> CONSULTA de los datos<input type="checkbox"/> COMUNICACIÓN POR TRANSMISIÓN/INTERCONEXION/OTRAS FORMAS DE ACCESO de los datos<input type="checkbox"/> EXTRACCIÓN de los datos<input type="checkbox"/> COTEJO de los datos<input type="checkbox"/> LIMITACION de los datos<input type="checkbox"/> SUPRESION de los datos<input type="checkbox"/> OTROS TRATAMIENTOS de los datos
--

Declaración sobre subcontratación de servicios de tratamiento de datos <i>en la nube (cloud computing)</i>
<p>Indicar si está prevista la subcontratación por el ENCARGADO de servicios <i>en la nube (cloud computing)</i> - para el tratamiento de los datos objeto del contrato principal - (marcar una X en lo que proceda)</p> <ul style="list-style-type: none"><input type="checkbox"/> SÍ<input type="checkbox"/> NO <p>(<u>En caso de respuesta afirmativa a la anterior</u>) Indicar dónde van a estar ubicados los servidores desde los cuales se van a prestar los servicios <i>en la nube (cloud computing)</i> (marcar una X y rellenar en lo que proceda)</p> <ul style="list-style-type: none"><input type="checkbox"/> DENTRO del Espacio Económico Europeo (Unión Europea + Noruega + Islandia+ Liechtenstein)<input type="checkbox"/> FUERA del Espacio Económico Europeo (indicar en ese caso el país:)

En prueba de su conformidad, **una vez cumplimentados todos los apartados del ANEXO**, ambas partes firman el presente documento, en lugar y fecha reseñados en el encabezamiento (ut supra).

MUTUALIA

EMPRESA