Acuerdo adicional al tratamiento de datos por encargo del cliente responsable del tratamiento

entre

_____

(«**cliente responsable del tratamiento**»)

y

Brainlab Sales GmbH, Olof-Palme-Straße 9, 81829 Múnich, Alemania
(«**proveedor encargado del tratamiento**», y en conjunto, las «**partes**»)

Preámbulo

Este acuerdo resultará de aplicación a las actividades del proveedor encargado del tratamiento relacionadas con la instalación de hardware y software, mantenimiento, reparación, formación, acceso remoto, localización de averías y los demás servicios de asistencia para los productos del proveedor que le sirvan de apoyo al cliente responsable del tratamiento de datos para la prestación de servicios sanitarios y a través de los cuales los miembros del personal del proveedor o terceros encargados por este pudiesen entrar en contacto con datos personales del cliente responsable del tratamiento. El acuerdo sobre el que se basa la realización de estas actividades o prestación de servicios se denominará, en lo sucesivo, contrato principal.

Este acuerdo adicional se concluye de conformidad con el contrato principal y tendrá la misma duración que este último.

1. Definiciones

En este contrato se estipulan las siguientes definiciones, que tendrán el siguiente significado:

«Tercer país con nivel de protección de datos adecuado» es cualquier país fuera del EEE que ha sido reconocido como país con un nivel de protección de datos adecuado, o bien por la Comisión Europea en base a su legislación nacional interna, o bien en base a las obligaciones internacionales contraídas por el mismo.

«RGPD» es el reglamento (EU) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea de 27 de abril de 2016 de protección de personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos);

«**Instrucción**» es la orden ejecutiva escrita del cliente responsable del trato de datos personales que acata a un tratamiento de datos determinado de protección de datos (por ejemplo, anonimización, bloqueo, cancelación, edición) del encargado del tratamiento.

Los conceptos «**datos personales**», «**responsable**», **«encargados del tratamiento»** «**tratamiento/tratar**», «**interesado**», «**medidas técnicas y organizativas**», «**autoridad de control**» o «**tratamiento por encargo de persona responsable**» se interpretarán según lo dispuesto en el RGPD.

2. Objeto y responsabilidad

El proveedor encargado del tratamiento de datos de datos personales, tratará los datos personales por encargo del cliente responsable del tratamiento. Objeto del encargo son las actividades descritas en el contrato principal y sus anexos, en particular en la descripción sobre los servicios a prestar. La responsabilidad por la observancia de las leyes de protección de datos en el marco de este acuerdo adicional, en particular por del cumplimiento de la legalidad de la transmisión de datos al proveedor, así como del cumplimiento de la legalidad del tratamiento de datos por el proveedor, recaerá única y exclusivamente sobre sobre el cliente responsable del tratamiento.

3. Descripción del contenido del encargo

3.1 La finalidad, tipo y alcance de la recogida, tratamiento y/o utilización de datos personales dentro del marco del encargo están descritas en el contrato principal, al que se hace remisión a este respecto.

3.2 El tipo de categoría de los datos personales recogidos y/o utilizados, así como las categorías de los interesados por el tratamiento de datos personales dentro del marco de este encargo, están descritas en el Anexo 1 y/o en el contrato principal, al que se hace remisión a este respecto.

4. Derecho de impartir instrucciones del cliente responsable del tratamiento

4.1 En el marco de la especificación acordada en este acuerdo, el cliente responsable del tratamiento se reserva el derecho de impartir instrucciones sobre el modo, alcance y proceso del tratamiento de datos, que podrá concretar a través de instrucciones individuales. Las modificaciones realizadas sobre el objeto de tratamiento y el proceso deberán ser aprobadas y documentadas de modo conjunto por las partes.

4.2 El proveedor encargado del tratamiento informará al cliente responsable del tratamiento cuando considere que una instrucción vulnera los requisitos legales de protección de datos. El proveedor estará facultado para omitir el cumplimiento de la correspondiente instrucción siempre que y mientras el cliente responsable del tratamiento no la haya confirmado o cambiado.

5. Obligaciones del proveedor

5.1 El proveedor encargado del tratamiento recogerá, tratará o utilizará datos, en tanto que no sea permitido de otro modo por la ley (por ejemplo, por el consentimiento de la persona afectada), principalmente tan solo por encargo y en base a las instrucciones del cliente responsable del tratamiento, pero en particular no para sus propios fines. El proveedor corregirá, suprimirá, rectificará, o bloqueará los datos personales tratados por encargo del cliente responsable del tratamiento tan solo siguiendo las instrucciones de este último. En la medida que un interesado se dirigiese directamente al proveedor para que se llevase a cabo la rectificación o supresión de sus datos, el proveedor remitirá esta solicitud al cliente responsable del tratamiento.

5.2 El proveedor permanecerá facultado, en casos concretos de datos obtenidos en el marco del servicio de asistencia, para utilizarlos de modo que a los respectivos miembros del personal del proveedor no les sea posible obtener conclusiones sobre la persona del interesado (por ejemplo, de un paciente, de un médico o un miembro del personal del hospital). La utilización tendrá lugar a efectos, o bien (i) del cumplimiento de obligaciones legales (por ejemplo, obligaciones de observación del producto y de información), o bien (ii) de la observación de intereses legítimos del proveedor y del cliente responsable del tratamiento, en particular con la finalidad de mejora de la calidad y funcionalidad de los productos del proveedor a través de la utilización de datos seleccionados para el servicio

de asistencia (por ejemplo, imágenes de TC o MRI sin identificador), por ejemplo, con objeto de realizar pruebas de nuevas versiones del producto. No se aplicarán el resto de las restricciones contenidas en este acuerdo para el tratamiento de datos personales por encargo.

5.3 El tratamiento se realizará tan solo siguiendo las instrucciones del cliente responsable del tratamiento, salvo que el proveedor estuviese obligado al tratamiento en virtud del derecho de la Unión Europea o del Estado miembro que se le aplique; en tal caso, antes de que el tratamiento tenga lugar, el proveedor informará al cliente responsable del tratamiento sobre esa exigencia legal, salvo que tal Derecho lo prohíba por razones importantes de interés público (véase artículo 28, párrafo 3, letra a del RGPD).

5.4 En la medida que no estuviese prohibido por el derecho vigente o por una solicitud de una autoridad administrativa, el proveedor deberá informar inmediatamente al cliente responsable del tratamiento sobre todas las solicitudes emitidas por organismos oficiales, autoridades competentes para la protección de datos o las autoridades competentes para la persecución penal relativas al acceso o confiscación de los datos personales del cliente responsable del tratamiento.

5.5 Con anterioridad a la concesión de acceso a datos personales, el proveedor obligará a las personas encargadas del tratamiento de los mismos a la observancia del secreto de datos y confidencialidad y las pondrá en conocimiento de las disposiciones relativas a las obligaciones de protección de datos vigentes aplicables al proveedor. Esto incluye también, de ser así necesario, la obligación de los interesados de observar, dado el caso, un secreto profesional (derivado) existente (por ejemplo, en el caso tratamiento de datos de hospitales o de médicos con consultorio) o un secreto de las comunicaciones, siempre y cuando y en la medida que las prestaciones correspondientes estuviesen pactadas en el contrato principal. En la medida que resultasen necesarias deontológica y profesionalmente, el cliente responsable del tratamiento aplicará todas las medidas necesarias e informará e instruirá correspondientemente al proveedor.

5.6 En la medida que esto estuviera requerido por la ley, el proveedor nombrará a un responsable de protección de datos y, durante la duración del contrato principal, pondrá a disposición del cliente responsable del tratamiento los datos de contacto de este último.

5.7 El proveedor informará al cliente responsable del tratamiento sobre infracciones, realizadas por el mismo o por una persona empleada en su empresa, a instrucciones o a disposiciones relativas a la protección de datos personales del cliente responsable del tratamiento.

En el caso de que se perdiesen datos personales, se transmitiesen ilícitamente o se revelasen de otro modo a terceros de modo ilícito de conformidad con lo dispuesto en los artículos 33 y 34 del RGPD, se deberá informar inmediatamente al cliente responsable del tratamiento. De común acuerdo con el cliente responsable del tratamiento, el proveedor adoptará las medidas apropiadas para proteger los datos y reducir las posibles consecuencias desventajosas de los interesados.

Además, el proveedor informará inmediatamente al cliente responsable del tratamiento sobre las perturbaciones en el funcionamiento normal y sobre la sospecha de violaciones de la protección de datos o cualquier otra irregularidad en el tratamiento de los datos personales.

El proveedor es consciente de que el cliente responsable del tratamiento está obligado a documentar las violaciones de la seguridad de datos personales y, de ser necesario, de informar sobre las mismas a las autoridades de control o a los interesados, respectivamente. En la medida en que, y en el caso de que ocurriesen tales violaciones, el proveedor asistirá adecuadamente al cliente responsable del tratamiento en la observancia de sus obligaciones de conformidad con lo dispuesto en el artículo 28, párrafo 3, letra f del RPGD, de modo que el cliente responsable del tratamiento las pueda cumplir dentro de plazo. El proveedor le comunicará la violación de la seguridad de datos al cliente responsable del tratamiento haciendo indicación, como mínimo, de los siguientes términos, en tanto se le hayan presentado las informaciones correspondientes:

a) una descripción del tipo de violación de la seguridad de datos personales, haciendo indicación en la medida de lo posible de las categorías y el número aproximado de interesados, de las categorías y del número aproximado de grupos de datos personales afectados;

b) el nombre y datos de contacto de los responsables de protección de datos o de las eventuales oficinas de atención al cliente responsable del tratamiento para la obtención de más informaciones;

c) una descripción de las probables consecuencias de la violación de la seguridad de datos personales;

d) una descripción de las medidas adoptadas o propuestas por el cliente responsable del tratamiento con el fin de mitigar los efectos de la violación de la seguridad de datos personales y, en su caso, de las medidas adoptadas para reducir el impacto de los posibles efectos desventajosos.

5.8 El proveedor informará inmediatamente al cliente responsable del tratamiento sobre todas las actividades de control y medidas que fuesen adoptadas por la autoridad de control con respecto al tratamiento de datos personales del cliente responsable del mismo.

5.9 En el caso de que el cliente responsable del tratamiento estuviese obligado a aportar información sobre la recogida, tratamiento o utilización de datos de conformidad con las disposiciones legales de protección de datos vigentes, el proveedor deberá poner a disposición del primero todas las informaciones correspondientes.

5.10 El proveedor velará por la observancia de las obligaciones arriba mencionadas durante la realización del tratamiento de datos encargado.

5.11 De conformidad con lo dispuesto en el artículo 30, párrafo 2 del RPGD, el proveedor gestionará un archivo escrito de todas las categorías de actividades de tratamiento encargadas por del cliente responsable del tratamiento.

5.12 De conformidad con lo dispuesto en el artículo 28, párrafo 3, letra f del RPGD, el proveedor asistirá, en su caso, en la elaboración de una evaluación de impacto relativa a la protección de datos de conformidad con lo dispuesto en el artículo 35 del RPGD, así como asistirá, donde fuese pertinente, en la realización de consulta a la autoridad de control de conformidad con lo dispuesto en el artículo 36 del RPGD. A petición del cliente responsable del tratamiento, el proveedor deberá poner a disposición del mismo todos los documentos e información necesarios. Los costes adicionales que surgiesen de estas prestaciones deberán ser abonados al proveedor.

5.13 El proveedor adoptará medidas oportunas respecto a la utilización abusiva de datos, pérdida y recuperación de datos (por ejemplo, a través de la elaboración de copias de seguridad según las referencias estándar de la industria), en la medida que esto esté previsto en el contrato principal.

6. Seguridad del tratamiento de datos

6.1 En el marco de su competencia, el proveedor encargado del tratamiento llevará a cabo su organización interna en atención a todos los requisitos vigentes en materia de protección y seguridad de datos. De conformidad con los requisitos de las leyes vigentes, el proveedor adoptará, gestionará y llevará el control de medidas técnicas y organizativas, con el objetivo de garantizar la seguridad adecuada de los datos del cliente responsable del tratamiento frente a la utilización abusiva y pérdida de los mismos.

6.2 El proveedor adoptará todas las medidas técnicas y organizativas apropiadas que cumplan con los requisitos del artículo 32 del RPGD con el fin de garantizar un nivel de seguridad adecuado al riesgo y asistir al cliente responsable del tratamiento en el cumplimiento de las obligaciones contempladas en el artículo 32 del RPGD (artículo 28, párrafo 3, letras c, f del RPGD)

6.3 En este contexto, el proveedor tendrá en cuenta el estado de la técnica, los costes de implementación y el tipo, el alcance, las circunstancias y la finalidad del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas. Para ello se incluyen la adopción de medidas apropiadas, como por ejemplo los controles de entradas, de usuarios, de acceso, de transmisión, de introducción de datos, de encargos, de disponibilidad, así como la clasificación según la finalidad, del mismo modo que

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.

6.4 El Anexo 2 contiene una descripción y especificación de las medidas técnicas y organizativas necesarias, que el proveedor adoptará en el marco de este acuerdo. Estas podrán ser complementadas a través de documentos adicionales.

6.5 Las medidas técnicas y organizativas están sujetas al progreso y desarrollo tecnológico. El proveedor podrá adoptar medidas alternativas apropiadas. Estas no deberán, sin embargo, estar por debajo del nivel de seguridad de las medidas establecidas. Las modificaciones esenciales deberán ser documentadas.

6.6 En la medida que esto sea posible y razonablemente exigible, el proveedor asistirá al cliente responsable del tratamiento a través de la adopción de medidas técnicas y organizativas oportunas de conformidad con lo dispuesto en el artículo 28, párrafo 3, letra e del RPGD, para que este pueda cumplir con sus obligaciones frente a los interesados de conformidad con lo dispuesto en el capítulo 3 del RPGD, por ejemplo en cuanto a la información y el derecho de ser informado de los interesados, la rectificación y supresión de datos, limitación del tratamiento o del derecho de transmisión de datos y el derecho de oposición. Los costes adicionales que surgiesen de estas prestaciones deberán ser abonados al proveedor.

7 Acceso remoto y de soporte técnico

7.1 La realización del acceso remoto y de soporte técnico se regirá, adicionalmente, por lo dispuesto en las siguientes disposiciones, siempre y cuando y en la medida que las actividades de tratamiento afectasen a determinadas categorías de datos personales o el cliente responsable del tratamiento estuviese sometido a un secreto profesional.

7.2 Siempre y cuando y en la medida que no se pueda excluir un acceso a los datos personales, el acceso remoto tan solo podrá llevarse a cabo con el consentimiento del miembro del personal competente del cliente responsable del tratamiento.

7.3 Los miembros del personal del proveedor encargado del tratamiento utilizarán procesos adecuados de identificación y cifrado.

7.4 Los accesos remotos serán objeto de documentación y registro. El cliente responsable del tratamiento estará facultado para controlar los trabajos de verificación y mantenimiento antes, durante y después de su implementación. Para ello deberá observar las disposiciones contempladas en el capítulo 9. En el caso de accesos remotos, el cliente responsable del tratamiento estará facultado –en la medida que esto sea técnicamente posible y ejecutable en atención al tipo de las prestaciones realizadas–, para hacer un seguimiento de los mismos a través de un monitor de control y para interrumpirlo en cualquier momento.

7.5 El acceso remoto a los sistemas relevantes tan solo tendrá lugar según el principio de necesidad imperiosa (*need-to-know*).

7.6 Las actividades de análisis de averías que presupongan un acceso a datos personales, requerirán el consentimiento previo del miembro competente del personal del cliente responsable del tratamiento. Si se realizasen copias para estos fines, el proveedor las modificará de tal modo tras la eliminación de la avería que ya no le fuese posible realizar ninguna referencia personal más, o las cancelará, salvo que, por otros motivos, fuese necesaria la conservación (sin modificaciones) de los correspondientes datos (por ejemplo, como prueba de los trabajos realizados y de la realización con regularidad de los mismos). Los datos personales tan solo podrán ser utilizados para poder llevar a cabo análisis de averías y no podrán, además, ser copiados en medios de almacenamiento (PDA, memorias portátiles o dispositivos parecidos) sin un cifrado adecuado. Ello se entenderá sin perjuicio de lo dispuesto en el número 5.2.

7.7 En casos concretos existe la posibilidad, de ser necesario para la prestación de los servicios previstos en el contrato (sobre todo para llevar a cabo una reparación), de que las actividades de análisis de averías se realicen sin la obtención de un consentimiento previo. El cliente responsable del tratamiento otorga, mediante el presente acuerdo, su consentimiento general para la realización de las correspondientes actuaciones.

7.8 Tanto los accesos remotos como todas las actividades necesarias relacionadas con ellos, como, en particular, la supresión, la transmisión de datos o los análisis de averías, se realizarán en base a las medidas técnicas y organizativas adoptadas para la seguridad de los datos personales.

8. Derechos y obligaciones del cliente responsable del tratamiento

8.1 En lo que respecta a los datos sometidos al tratamiento, el cliente responsable y el proveedor encargado del mismo serán responsables del cumplimiento de las leyes de protección de datos pertinentes en cada caso para cada uno de ellos.

8.2 Tras la terminación del encargo, el cliente responsable del tratamiento especificará las medidas a adoptar para la devolución de los soportes de datos cedidos y/o la supresión de los datos guardados. En la medida que no se llevasen a cabo tales especificaciones, se deberán suprimir o entregar los datos al cliente responsable del tratamiento. En la medida que tuviese lugar la supresión de los datos sobre la base de una especificación particular, el proveedor deberá confirmar esta al cliente responsable del tratamiento, haciendo indicación de la fecha. La devolución o supresión de los datos guardados tan solo será posible, siempre y cuando no existiesen obligaciones legales o regulatorias, a las que estuviese sometido el proveedor encargado del tratamiento, de conservarlos. Ello se entenderá sin perjuicio de lo dispuesto en el número 5.2.

9. Derechos de control

9.1 A solicitud del cliente responsable del tratamiento, el proveedor encargado del tratamiento pondrá a su disposición pruebas justificantes de la implementación de medidas técnicas y organizativas y de las demás obligaciones de conformidad con lo dispuesto en el artículo 28 del RPGD.

9.2 Previa consulta con el proveedor, el cliente responsable del tratamiento podrá realizar un control de pedidos o encargar inspectores para que lleven a cabo esta tarea antes de que comience el tratamiento de datos y, de modo razonablemente exigible, durante la completa duración del encargo. El proveedor podrá cumplir con esas exigencias en cualquier momento antes y durante la duración del tratamiento a través de correspondientes informaciones proporcionadas por si mismo, certificaciones actuales, informes o extractos de entidades independientes (por ejemplo, por medio de inspectores externos, de auditorías internas, de un responsable de protección de datos, de un departamento de seguridad informática, de inspectores de protección de datos o de calidad) o por medio de la certificación adecuada en el marco de una auditoría de seguridad informática o de protección de datos.

9.3 En tanto que el cliente responsable del tratamiento presentase dudas fundadas al proveedor sobre las informaciones o valoraciones proporcionadas por este último, el cliente responsable del tratamiento estará facultado a llevar a cabo a su coste una inspección adecuada en los establecimientos comerciales del proveedor, con el fin de la observancia de las medidas técnico-organizativas y de las demás obligaciones de conformidad con lo dispuesto en el artículo 28 del RPGD. La inspección correspondiente deberá anunciarse como mínimo dos semanas con antelación y ser ejecutada tan solo durante los horarios laborales regulares, sin poder interferir en el funcionamiento interno de la empresa. El cliente responsable del tratamiento deberá resarcir todos los costes adicionales que le pudieran surgir al proveedor como consecuencia de la correspondiente inspección.

9.4 A solicitud escrita del cliente responsable del tratamiento, el proveedor deberá poner a su disposición dentro de un plazo adecuado todas las informaciones necesarias para la inspección.

10. Subcontratistas

10.1 El proveedor encargado del tratamiento estará autorizado a encargar subcontratistas u otras empresas para el cumplimiento de sus obligaciones contractuales.

10.2 En la conclusión de acuerdos con subcontratistas y antes de que se le conceda el acceso al subcontratista de los datos personales del cliente responsable del tratamiento durante la realización del mismo, el proveedor garantiza que al subcontratista se le impondrán fundamentalmente como mínimo las mismas obligaciones asumidas por el proveedor de conformidad con lo dispuesto en este acuerdo. Si el subcontratista prestara uno de los servicios acordados fuera de la UE/EEE y en un tercer país con un nivel de protección adecuado, el proveedor velará por el cumplimiento de las disposiciones de protección de datos de la UE.

10.3 A solicitud del cliente responsable del tratamiento, el proveedor pondrá a su disposición una lista de las actividades de tratamiento de datos realizadas por los subcontratistas participantes. El proveedor informará al cliente responsable del tratamiento sobre todas las modificaciones previstas en relación con la inclusión o sustitución de otros subcontratistas, y le concederá la posibilidad de oponerse a esas modificaciones, pudiendo este último presentar objeciones fundadas contra las mismas. En el caso de que el cliente responsable del tratamiento no aprobase un nuevo subcontratista, tanto este como el proveedor, o ambas partes, podrán denunciar por escrito y sin plazo, o sea sin la observancia de un plazo de preaviso o cualesquiera obligaciones de compensación por daños o gastos, los servicios afectados por el tratamiento correspondiente en los que el subcontratista debiere estar implicado.

10.4 El cliente responsable del tratamiento estará facultado a inspeccionar a los subcontratistas del proveedor en atención a lo dispuesto en el punto 9 y tras previo acuerdo con el proveedor, encargando el cliente responsable del tratamiento al proveedor, en este caso, a que realice la inspección en su nombre y mostrando su conformidad con que tal inspección tan solo se realice por el proveedor mediante la presentación de certificaciones, informes o extractos actuales de entidades independientes (por ejemplo, por medio de inspectores externos, de auditorías internas, de responsables de protección de datos, de un departamento de seguridad informática, de inspectores de protección de datos o de calidad) o mediante certificación adecuada en el marco de una auditoría de seguridad informática o de protección de datos. A este fin, el cliente responsable del tratamiento deberá concluir, en su caso, uno o varios acuerdos de confidencialidad con el subcontratista y/o proveedor antes de transmitir los documentos e informaciones correspondientes del subcontratista.

10.5 Los requisitos recogidos en este punto 10 no serán de aplicación, cuando el proveedor asignase servicios complementarios a terceros; entre estos servicios complementarios se encuentran servicios de correos, de envío y de instalaciones.

11. Transmisión de datos fuera de la EEE

11.1 Por norma general, el tratamiento tendrá lugar en un Estado miembro de la Unión Europea, en un país de del Espacio Económico Europeo o en un tercer país con un nivel de protección adecuado (incluidos los Estados Unidos de América, en la medida que existiese la certificación de escudo de privacidad UE-EE.UU. (*Privacy-Shield*) correspondiente). Estarán permitidos los tratamientos en otro país ("**tercer país**"), siempre y cuando se observasen los requisitos de transmisión de datos personales de conformidad con lo dispuesto en los artículos 44 y siguientes del RPGD.

11.2 En el caso y en la medida que (i) el cliente responsable del tratamiento y el proveedor encargado del tratamiento se encontrasen dentro del Espacio Económico Europeo ("**EEE**"), mientras el subcontratista del proveedor estuviere en un tercer país, y (ii) el proveedor adoptase acuerdos con subcontratistas sobre la base de las cláusulas contractuales estándar de la UE para proveedores encargados del tratamiento ("**SCC**"), el cliente responsable del tratamiento autoriza al proveedor mediante el presente acuerdo a concluir tales acuerdos de subcontratación de tratamiento de datos con subcontratistas, en la medida que esto le fuere posible al proveedor, también en nombre y por encargo del cliente responsable del tratamiento. De así requerirlo el cliente responsable del tratamiento, el proveedor deberá informar a este, así como a las partes contractuales de los mismos, sobre la existencia y el estado de los contratos de cláusulas contractuales estándar, que se hayan concluido bajo las circunstancias mencionadas. En este caso, será el proveedor el que decida a su propia discreción si deberán ser concluidos los correspondientes contratos.

12. Responsabilidad

12.1 El cliente responsable del tratamiento exonera al proveedor encargado del tratamiento del cumplimiento de cualesquiera pretensiones de terceros o de responsabilidad por daños u obligaciones que pudiesen resultar (i) del incumplimiento de obligaciones del cliente responsable del tratamiento resultantes de este acuerdo y/o de otras infracciones contra leyes de protección de datos vigentes, y/o (ii) infracciones del proveedor contra la legislación relativa a la protección de datos vigentes, en la medida que estas hubiesen estado en relación con la ejecución de las especificaciones pactadas en este acuerdo o con otras eventuales instrucciones del cliente responsable del tratamiento. Esto no resultará de aplicación en la medida que el cliente responsable del tratamiento no fuese responsable de las circunstancias que fundamentan la responsabilidad. Lo dispuesto en el artículo 85 (5) del RPGD permanecerá inalterado.

12.2 En la medida que el contrato principal prevea una limitación o una exclusión de responsabilidad u obligación de dispensa para el proveedor, resultarán de aplicación estas limitaciones o exclusiones también para las pretensiones que se puedan hacer valer frente el proveedor en relación con este acuerdo.

12.3 Las disposiciones sobre responsabilidad y dispensa reguladas en el contrato principal permanecerán, en lo demás, inalteradas.

13. Confidencialidad

Las partes se comprometen a tratar confidencialmente todos los conocimientos y secretos comerciales y profesionales obtenidos en el marco de la relación contractual. Esto también resultará de aplicación tras la finalización del encargo particular y/o la relación comercial.

14. Obligaciones de información, cláusula de requerimiento de la forma escrita, elección de la ley aplicable

14.1 Para el caso de que se hubiesen puesto en peligro en el negocio del proveedor encargado del tratamiento datos personales del cliente responsable del tratamiento a causa de un embargo o confiscación, de un proceso de insolvencia o liquidación o como consecuencia de otros sucesos o medidas adoptadas por terceros, el proveedor deberá de informar al respecto al cliente responsable del tratamiento. El proveedor informará a todas partes resultantes en este contexto, que la soberanía y propiedad sobre los datos residen, única y exclusivamente, en el cliente responsable del tratamiento.

14.2 Las modificaciones y complementos de este acuerdo adicional requerirán la forma escrita y una advertencia expresa de que se trata de una modificación o un complemento, respectivamente. La modificación de este requisito de forma requerirá a su vez la forma escrita.

14.3 El derecho aplicable a este acuerdo adicional y a todos los posibles litigios relativos a su celebración e implementación será exclusivamente el de la República Federal Alemana, quedando excluido el Convenio de las Naciones Unidas sobre la compraventa internacional de mercancías de 11/04/1980. El fuero competente para todos los litigios surgidos entre las partes en relación con este acuerdo adicional es el del Tribunal Regional de Múnich I.

Para el proveedor encargado del tratamiento:	**Para el cliente responsable del tratamiento:**
[*nombre*] [*puesto*] [*lugar, fecha*]	[*nombre]* [*puesto*] [*lugar, fecha*]
_____	_____

<u>Anexo 1</u>: Tipos de categorías de datos y categorías de interesados en el marco de la recogida, el tratamiento y/o utilización de datos personales

1. Tipos de datos personales recogidos y/o utilizados

- Datos personales principales (por ejemplo, nombre y apellidos, fecha de nacimiento, sexo, código de identificación del paciente)
- Datos de contacto (por ejemplo, número de teléfono, dirección de correo electrónico)
- Datos principales del contrato (por ejemplo, relación contractual, interés en productos o contratos)
- Historial del cliente
- Datos de facturación y pago (por ejemplo, el número de la cuenta bancaria)
- Datos de planificación y administrativos (por ejemplo, información sobre la infraestructura del cliente)
- Datos de evaluación (de terceros, por ejemplo, agencias de evaluación, o de registros públicos)
- Informaciones médicas e imágenes del paciente

2. Categorías de personas sujetas al tratamiento de los datos personales

- Clientes
- Clientes potenciales
- Suscriptores
- Pacientes del cliente

<u>Anexo 2</u>: Seguridad del tratamiento de datos

Este anexo describe las medidas técnicas y organizativas y procesos que deberá adoptar el proveedor encargado del tratamiento para poder proteger la seguridad de datos personales creados, recogidos, recibidos u obtenidos de otro modo, y para garantizar la continua confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de tratamiento.

Medidas técnicas y organizativas

I. Confidencialidad, artículo. 32, párrafo. 1 letra. b) del RPGD

1. Controles de entrada a las instalaciones

Medidas apropiadas para impedir a personas no autorizadas la entrada a instalaciones de tratamiento de datos con las que se tratan o utilizan datos personales.

- ☒ Definición de círculo limitado de personas con acceso
- ☒ Cerraduras de seguridad
- ☒ Sistema de cierre manual (por ejemplo, habitación con llave, armario) - aplicable específicamente para home office
- ☒ Sistema de cierre con tarjetas inteligentes/transmisor-receptor
- ☒ Vigilancia por videocámara de los accesos

2. Controles de acceso

Medidas adecuadas para evitar que personas no autorizadas puedan utilizar los sistemas de tratamiento de datos.

- ☒ Concesión funcional o temporalmente limitada de autorizaciones de uso
- ☒ Directiva de contraseñas de acceso, incluyendo la longitud de la contraseña, la concesión y el cambio de la misma
- ☒ Autenticación con nombre / contraseña de usuario
- ☒ Utilización de detectores de intrusiones (*Intrustion-Detection*) y sistemas de detección de intrusiones.
- ☒ Utilización de programas de antivirus
- ☒ Utilización de cortafuegos como dispositivo de hardware (*hardware-firewall*)
- ☒ Utilización de filtros de spam para correos electrónicos
- ☒ Elaboración de perfiles de usuario
- ☒ Clasificación de perfiles de usuario a sistemas informáticos
- ☒ Utilización de la tecnología VPN
- ☒ Utilización de software central de administración de teléfonos inteligentes (por ejemplo, para la supresión externa de datos)
- ☒ Utilización de programas cortafuegos (*software- firewall*)
- ☒ Cifrado del disco duro y del ordenador portátil
- ☒ Sistema adicional de acceso para las diferentes aplicaciones

3. Controles de acceso limitados

Medidas que garantizan que las personas facultadas para el uso de los sistemas de tratamientos de datos únicamente puedan acceder a los datos para los que tienen facultado el acceso, y que datos personales no puedan ser leídos, copiados, modificados y extraídos sin autorización durante el tratamiento, la utilización, y tras su almacenamiento.

- ☒ Determinación de las autorizaciones de acceso
- ☒ Concesión restrictiva de autorizaciones para administradores
- ☒ Supresión física de portadores de datos antes de su reutilización
- ☒ Registro de transmisiones de datos
- ☒ Destrucción segura de portadores de datos
- ☒ Administración de derechos a través de un administrador de sistema
- ☒ Requisito de identificación a través del uso de contraseñas de acceso
- ☒ Almacenamiento seguro de portadores de datos
- ☒ Registro de accesos a diferentes aplicaciones
- ☒ Procesos determinados para la concesión de autorizaciones, controles y retirada de autorizaciones

4. Controles de separación

Medidas que garantizan que datos recogidos para diferentes fines puedan ser tratados de forma separada

- ☒ Almacenamiento físicamente separado en sistemas anexos o en portadores de datos
- ☒ Elaboración de un sistema de autorizaciones
- ☒ Separación lógica de clientes (desde el punto de vista del software)
- ☒ Separación del sistema productivo y de ensayo

II. Seudonimización y cifrado, artículo. 32, párrafo 1 letra. A del RPGD

Medidas para la seudonimización y cifrado de datos personales (en la medida que ya no bajo punto I)

- ☒ Utilización de técnicas de seudonimización y anonimización, entre otras en el ámbito de investigación y desarrollo (*R&D*)
- ☒ Existencia de normativa para el cifrado de datos
- ☒ Cifrado estandarizado de datos especialmente sensibles (*at rest*) en servicios individuales

III. Integridad, artículo. 32, párrafo. 1 letra. b) del RPGD

1. Controles de reenvío

Medidas que garantizan que datos personales, durante la transmisión electrónica o durante su transporte o su almacenamiento en portadores de datos, no puedan ser leídos, copiados, modificados y extraídos sin autorización, y que se pueda verificar y determinar en que sitios está prevista una transmisión de datos personales por medio de instalaciones de transmisión de datos.

- ☒ Instalaciones de líneas alquiladas o túneles VPN, respectivamente.
- ☒ Capacitación de miembros del personal en la protección de datos
- ☒ Documentación sobre los receptores de datos
- ☒ Clara regulación en una directiva sobre la forma de reaccionar en caso de pérdida de un soporte de datos
- ☒ Cifrado del disco duro y del ordenador portátil

2. Controles de entradas de datos

Medidas que garantizan que se pueda verificar y determinar a posteriori si y de quien ha habido entradas, modificaciones y eliminaciones de datos personales en sistemas de tratamiento de datos.

- ☒ Concesión de derechos de entrada, modificación y supresión de datos sobre la base de un sistema de autorizaciones
- ☒ Registro de entradas, modificaciones y supresión de datos, en la medida que lo permitan los sistemas

IV. Disponibilidad y resiliencia, artículo 32, párrafo 1 letra b) y c) del RPGD

1. Controles de disponibilidad

Medidas que garantizan que los datos personales estén protegidos contra la destrucción fortuita o pérdida de datos personales, incluidas medidas de recuperación en el caso de incidentes físicos o técnicos.

- ☒ Sistema de alimentación ininterrumpida (SAI)
- ☒ Control de climatización en las salas de servidores
- ☒ Detectores de fuego y humo
- ☒ Sistema de copia de seguridad y recuperación de datos
- ☒ Existencia de un plan de emergencia
- ☒ Empleo de cortafuegos (firewalls) y escáneres de virus
- ☒ Gestión de parches
- ☒ Sistemas adecuados de extinción de fuegos en las salas de los servidores
- ☒ Ensayos de recuperación de datos
- ☒ Almacenamiento de la seguridad de datos en un sitio seguro y externalizado

V. Procedimientos para la verificación y valoración regulares, artículo 32, párrafo 1, letra d) del RPGD

1. Gestión de protección de datos

Otras medidas, sobre todo organizativas, para la protección de datos personales.

☒ Descripción de los requisitos vigentes de protección de datos contenidos en las directivas vinculantes e instrucciones de manejo

☒ Obtención de información actual sobre la seguridad informática y vulnerabilidad del sistema informático

☒ Verificaciones regulares de las mediadas adoptadas para la protección de datos y de la normativa existente

☒ En su caso, involucración del responsable de protección de datos en relevantes nuevos procesos de tratamiento de datos

2. Gestión de incidencias y respuesta (*incident response management*)

Otras medidas para gestionar incidentes en protección de datos

☒ Normativa de comportamiento en caso de incidentes en la protección de datos y seguridad informática

☒ Procesos de gestión de continuidad de la actividad empresarial (*business continuity management*)

☒ Proceso de aviso de incidentes

3. Ajustes por defecto respetuosos con la protección de datos, artículo 25, párrafo 2 del RPGD

Medidas que garantizan que los ajustes por defecto se correspondan con los intereses de los interesados (privacy by default).

☒ Implementación de ajustes por defecto respetuosos con la protección de datos

☒ Empleo de seudonimización y anonimización de datos personales, por ejemplo, en el ámbito de I&D (*R&D*)

☒ Limitación de la recogida de datos

4. Controles de encargos

Medidas que garantizan que los datos personales elaborados por encargo tan solo se puedan elaborar sobre la base de las correspondientes instrucciones del cliente responsable del tratamiento

☒ Selección diligente del proveedor encargado del tratamiento de datos (en particular, en lo que se refiere a la seguridad de datos)

☒ Control previo del encargado del tratamiento, en particular, verificación previa de la documentación sobre las medidas de seguridad adoptadas por el encargado de tratamiento

☒ Instrucciones documentadas al proveedor encargado del tratamiento (por ejemplo, mediante un contrato de tratamiento por encargo)

☒ Obligación del encargado del tratamiento de obligar a los miembros de su personal a observar la confidencialidad de los datos

☒ En su caso nombramiento de un responsable de protección de datos por el proveedor encargado del tratamiento

☒ Pactados derechos eficaces de control frente al proveedor encargado del tratamiento

☒ Capacitación de los miembros del personal

☒ Registro de las actividades de tratamiento de datos por encargo