Acuerdo de Tratamiento de Datos

(“Acuerdo”)

(de conformidad con el anexo de la Decisión de Ejecución de la Comisión Europea sobre cláusulas contractuales tipo entre responsables y encargados en virtud del artículo 28 (7) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, C(2021) 3701, 4 de junio de 2021)

entre

_____

_____

_____

en adelante, el “Responsable” (Controller)

y

NO ISOLATION GMBH
THIERSCHSTRASSE 20, 80538
Munchen, Germany

en adelante, el “Encargado” (Processor)

Cada uno, una “Parte” y conjuntamente, las “Partes”.

SECCIÓN I

Cláusula 1

Objeto y alcance

(a) El objeto de este Acuerdo es garantizar el cumplimiento del artículo 28, apartados (3) y (4), del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

(b) Estas Cláusulas se aplican al tratamiento de datos personales tal como se especifica en el Anexo II.

(c) Los Anexos I a IV forman parte integrante de las Cláusulas.

(d) Estas Cláusulas se entienden sin perjuicio de las obligaciones a las que esté sujeto el Responsable en virtud del Reglamento (UE) 2016/679 y/o del Reglamento (UE) 2018/1725.

(e) Estas Cláusulas, por sí mismas, no garantizan el cumplimiento de las obligaciones relacionadas con las transferencias internacionales de conformidad con el Capítulo V del Reglamento (UE) 2016/679 y/o del Reglamento (UE) 2018/1725.

Cláusula 2

Invariabilidad de las Cláusulas

(a) Las Partes se comprometen a no modificar las Cláusulas, salvo para añadir información a los Anexos o actualizar la información contenida en los mismos.

(b) Esto no impide que las Partes incluyan las cláusulas contractuales tipo establecidas en estas Cláusulas en un contrato más amplio, ni que añadan otras cláusulas o salvaguardas adicionales, siempre que no contradigan directa o indirectamente las Cláusulas ni menoscaben los derechos o libertades fundamentales de los interesados.

Cláusula 3

Interpretación

(a) Cuando estas Cláusulas utilicen términos definidos en el Reglamento (UE) 2016/679 o en el Reglamento (UE) 2018/1725, dichos términos tendrán el mismo significado que en el correspondiente Reglamento.

(b) Estas Cláusulas se leerán e interpretarán a la luz de las disposiciones del Reglamento (UE) 2016/679 o del Reglamento (UE) 2018/1725, según corresponda.

(c) Estas Cláusulas no se interpretarán de forma contraria a los derechos y obligaciones previstos en el Reglamento (UE) 2016/679 / Reglamento (UE) 2018/1725, ni de forma que perjudique los derechos o libertades fundamentales de los interesados.

Cláusula 4

Jerarquía

En caso de contradicción entre estas Cláusulas y las disposiciones de acuerdos relacionados entre las Partes existentes en el momento en que se acuerden estas Cláusulas o que se celebren posteriormente, prevalecerán estas Cláusulas.

Cláusula 5

Cláusula de adhesión

(a) Cualquier entidad que no sea Parte en estas Cláusulas podrá, con el acuerdo escrito de todas las Partes, adherirse a ellas en cualquier momento como Responsable o Encargado completando los Anexos pertinentes y notificando por escrito su adhesión a las demás Partes.

(b) Una vez completados y firmados los Anexos mencionados en el apartado (a), la entidad adherida será tratada como Parte de estas Cláusulas y tendrá los derechos y obligaciones de un Responsable o un Encargado, según corresponda.

(c) La entidad adherida no tendrá derechos u obligaciones derivados de estas Cláusulas respecto del período anterior a convertirse en Parte.

SECCIÓN II – OBLIGACIONES DE LAS PARTES

Cláusula 6

Descripción del/de los tratamiento(s)

Los detalles de las operaciones de tratamiento, en particular las categorías de datos personales y las finalidades del tratamiento para las cuales se tratan los datos personales en nombre del Responsable, se especifican en el Anexo II.

Cláusula 7

Obligaciones de las Partes

7.1. Instrucciones

(a) El Encargado tratará los datos personales únicamente siguiendo instrucciones documentadas del Responsable, salvo que esté obligado a ello en virtud del Derecho de la Unión o de un Estado miembro al que esté sujeto el Encargado. En tal caso, el Encargado informará al Responsable de dicha exigencia legal antes de tratar los datos, salvo que dicho Derecho lo prohíba por razones importantes de interés público. El Responsable podrá impartir instrucciones adicionales durante toda la duración del tratamiento de los datos personales. Estas instrucciones deberán documentarse siempre.

(b) El Encargado informará inmediatamente al Responsable si, a su juicio, una instrucción infringe el Reglamento (UE) 2016/679 / Reglamento (UE) 2018/1725 u otras disposiciones de la Unión o de los Estados miembros en materia de protección de datos.

7.2. Limitación de la finalidad

El Encargado tratará los datos personales únicamente para la(s) finalidad(es) específica(s) del tratamiento establecida(s) en el Anexo II, salvo que reciba instrucciones adicionales del Responsable.

7.3. Duración del tratamiento de datos personales

El tratamiento por parte del Encargado se realizará únicamente durante el tiempo especificado en el Anexo II.

7.4. Seguridad del tratamiento

(a) El Encargado aplicará, como mínimo, las medidas técnicas y organizativas especificadas en el Anexo III para garantizar la seguridad de los datos personales. Esto incluye proteger los datos frente a violaciones de seguridad que provoquen, de forma accidental o ilícita, destrucción, pérdida, alteración, divulgación no autorizada o acceso no autorizado a los datos (violación de seguridad de los datos personales). Al evaluar el nivel adecuado de seguridad, las Partes tendrán en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y las finalidades del tratamiento, así como los riesgos para los interesados.

(b) El Encargado concederá acceso a los datos personales objeto de tratamiento a los miembros de su personal únicamente en la medida estrictamente necesaria para la ejecución, gestión y supervisión del contrato. El Encargado garantizará que las personas autorizadas para tratar los datos personales se comprometan a respetar la confidencialidad o estén sujetas a una obligación legal adecuada de confidencialidad.

7.5. Datos sensibles

Si el tratamiento implica datos personales que revelen el origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, o afiliación sindical, datos genéticos o biométricos para identificar de manera unívoca a una persona física, datos relativos a la salud o a la vida sexual u orientación sexual, o datos relativos a condenas e infracciones penales ("datos sensibles"), el Encargado aplicará restricciones específicas y/o salvaguardas adicionales.

7.6. Documentación y cumplimiento

(a) Las Partes deberán poder demostrar el cumplimiento de estas Cláusulas.

(b) El Encargado atenderá de forma rápida y adecuada las consultas del Responsable sobre el tratamiento de datos de conformidad con estas Cláusulas.

(c) El Encargado pondrá a disposición del Responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en estas Cláusulas y permitirá y contribuirá a auditorías, incluidas inspecciones, realizadas por el Responsable o por un auditor designado por el Responsable.

(d) El Responsable podrá decidir realizar la auditoría por sí mismo o encargarla a un auditor independiente. Las auditorías podrán incluir inspecciones en los locales o instalaciones físicas del Encargado y, cuando proceda, se llevarán a cabo con un preaviso razonable.

(e) Las Partes pondrán a disposición de la autoridad de control competente, a solicitud, la información contemplada en esta cláusula, incluida la documentación de auditorías.

7.7. Uso de subencargados

(a) El Encargado cuenta con la autorización general del Responsable para la contratación de subencargados a partir de una lista acordada. El Encargado informará específicamente y por escrito al Responsable de cualquier cambio previsto en dicha lista, mediante la adición o sustitución de subencargados, con al menos 14 días de antelación, de modo que el Responsable disponga de tiempo suficiente para formular objeciones a dichos cambios antes de la contratación del/de los subencargado(s) en cuestión. El Encargado facilitará al Responsable la información necesaria para que este pueda ejercer su derecho de oposición.

(b) Cuando el Encargado recurra a un subencargado para llevar a cabo actividades específicas de tratamiento (por cuenta del Responsable), lo hará mediante un contrato que imponga al subencargado, en esencia, las mismas obligaciones en materia de protección de datos que las impuestas al Encargado del Tratamiento de conformidad con las presentes Cláusulas. El Encargado garantizará que el subencargado cumple las obligaciones a las que está sujeto el Encargado en virtud

de estas Cláusulas y del Reglamento (UE) 2016/679 y/o del Reglamento (UE) 2018/1725.

(c) A solicitud del Responsable, el Encargado facilitará al Responsable una copia de dicho contrato con el subencargado y de cualquier modificación posterior. En la medida necesaria para proteger secretos comerciales u otra información confidencial, incluidos datos personales, el Encargado podrá suprimir información del contrato antes de compartir la copia.

(d) El Encargado seguirá siendo plenamente responsable ante el Responsable del cumplimiento de las obligaciones del subencargado de conformidad con su contrato con el Encargado. El Encargado notificará al Responsable cualquier incumplimiento del subencargado de sus obligaciones contractuales.

(e) El Encargado acordará con el subencargado una cláusula de tercero beneficiario según la cual —en caso de que el Encargado haya desaparecido de facto, haya dejado de existir jurídicamente o haya devenido insolvente— el Responsable tendrá derecho a resolver el contrato con el subencargado e instruir al subencargado para que suprima o devuelva los datos personales.

7.8. Transferencias internacionales

(a) Cualquier transferencia de datos a un tercer país u organización internacional por parte del Encargado se realizará únicamente sobre la base de instrucciones documentadas del Responsable o para cumplir una obligación específica en virtud del Derecho de la Unión o de los Estados miembros a la que esté sujeto el Encargado y se efectuará de conformidad con el Capítulo V del Reglamento (UE) 2016/679 o del Reglamento (UE) 2018/1725, según corresponda.

(b) El Responsable acepta que, cuando el Encargado recurra a un subencargado de conformidad con la cláusula 7.7 para llevar a cabo actividades específicas de tratamiento (por cuenta del Responsable) y dichas actividades de tratamiento impliquen una transferencia de datos personales en el sentido del Capítulo V del Reglamento (UE) 2016/679, el Encargado y el subencargado podrán garantizar el cumplimiento del Capítulo V del Reglamento (UE) 2016/679 mediante el uso de las cláusulas contractuales tipo adoptadas por la Comisión de conformidad con el artículo 46.2 del Reglamento (UE) 2016/679, siempre que se cumplan las condiciones para el uso de dichas cláusulas contractuales tipo.

(c) Con el fin de aumentar la estabilidad y la seguridad de su infraestructura, el Encargado podrá utilizar servicios de una empresa (y, en su caso, de su empresa matriz) situada en Estados Unidos. Esto puede dar lugar a la transferencia de datos personales a Estados Unidos. Dicha transferencia se basa en la decisión de adecuación de la Comisión Europea (artículo 45.1 del RGPD), dado que el proveedor del servicio está registrado en el Marco de Privacidad de Datos UE-EE. UU. (EU-US Data Privacy Framework, DPF). Incluso en el caso de que se introduzcan cambios en dicha decisión o de que esta sea revocada, la transferencia quedará asegurada y legitimada mediante medidas contractuales, técnicas y organizativas conforme a los artículos 44 y siguientes del RGPD, tal como se describe en el apartado 7.8(b).

Cláusula 8

Asistencia al Responsable

(a) El Encargado notificará sin demora indebida al Responsable cualquier solicitud que reciba del interesado. No responderá por sí mismo a dicha solicitud, salvo que el Responsable le haya autorizado a hacerlo.

(b) El Encargado asistirá al Responsable en el cumplimiento de sus obligaciones de responder a las solicitudes de los interesados para el ejercicio de sus derechos, teniendo en cuenta la naturaleza del tratamiento. En el cumplimiento de sus obligaciones de conformidad con los apartados (a) y (b), el Encargado cumplirá las instrucciones del Responsable.

(c) Además de la obligación del Encargado de asistir al Responsable conforme al apartado 8(b), el Encargado asistirá asimismo al Responsable en el cumplimiento de las siguientes obligaciones, teniendo en cuenta la naturaleza del tratamiento de los datos y la información disponible para el Encargado:

    (i) la obligación de llevar a cabo una evaluación de impacto relativa a la protección de datos cuando un tipo de tratamiento sea probable que entrañe un alto riesgo para los derechos y libertades de las personas físicas;

    (ii) la obligación de consultar a la(s) autoridad(es) de control competente(s) con carácter previo al tratamiento cuando una evaluación de impacto relativa a la protección de datos indique que el tratamiento entrañaría un alto riesgo en ausencia de medidas adoptadas por el Responsable para mitigar dicho riesgo;

    (iii) la obligación de garantizar que los datos personales sean exactos y estén actualizados, informando sin demora al Responsable si el Encargado tiene conocimiento de que los datos personales que está tratando son inexactos o han quedado desactualizados;

    (iv) las obligaciones establecidas en el artículo 32 del Reglamento (UE) 2016/679.

(d) Las Partes establecerán en el Anexo III las medidas técnicas y organizativas apropiadas mediante las cuales el Encargado deberá asistir al Responsable en la aplicación de la presente Cláusula, así como el alcance y la extensión de la asistencia requerida.

Cláusula 9

Notificación de violaciones de la seguridad de los datos personales

En caso de una violación de la seguridad de los datos personales, el Encargado cooperará con el Responsable y le asistirá para que este pueda cumplir sus obligaciones en virtud de los artículos 33 y 34 del Reglamento (UE) 2016/679 o de los artículos 34 y 35 del Reglamento (UE) 2018/1725, según corresponda, teniendo en cuenta la naturaleza del tratamiento y la información disponible para el Encargado.

9.1 Violación de la seguridad de los datos personales relativa a datos tratados por el Responsable

En caso de una violación de la seguridad de los datos personales relativa a datos tratados por el Responsable, el Encargado asistirá al Responsable:

(a) en la notificación de la violación de la seguridad de los datos personales a la(s) autoridad(es) de control competente(s), sin dilación indebida después de que el Responsable tenga conocimiento de la misma, cuando proceda (salvo que sea improbable que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y libertades de las personas físicas);

(b) en la obtención de la siguiente información, que, de conformidad con el artículo 33.3 del Reglamento (UE) 2016/679, deberá incluirse en la notificación del Responsable y deberá contener, como mínimo:

(i) la naturaleza de los datos personales, incluyendo, cuando sea posible, las categorías y el número aproximado de interesados afectados, así como las categorías y el número aproximado de registros de datos personales afectados;

(ii) las posibles consecuencias de la violación de la seguridad de los datos personales;

(iii) las medidas adoptadas o propuestas por el Responsable para hacer frente a la violación de la seguridad de los datos personales, incluidas, cuando proceda, las medidas destinadas a mitigar sus posibles efectos adversos.

Cuando, y en la medida en que, no sea posible facilitar toda esta información al mismo tiempo, la notificación inicial contendrá la información entonces disponible y se facilitará información adicional sin dilación indebida a medida que vaya estando disponible.

(c) en el cumplimiento, de conformidad con el artículo 34 del Reglamento (UE) 2016/679, de la obligación de comunicar sin dilación indebida la violación de la seguridad de los datos personales al interesado, cuando sea probable que dicha violación entrañe un alto riesgo para los derechos y libertades de las personas físicas.

9.2 Violación de la seguridad de los datos personales relativa a datos tratados por el Encargado

En caso de una violación de la seguridad de los datos personales relativa a datos tratados por el Encargado, el Encargado notificará al Responsable sin dilación indebida desde que tenga conocimiento de dicha violación. Dicha notificación contendrá, como mínimo:

(a) una descripción de la naturaleza de la violación, incluyendo, cuando sea posible, las categorías y el número aproximado de interesados afectados, así como las categorías y el número aproximado de registros de datos personales 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) las posibles consecuencias de la violación y las medidas adoptadas o propuestas para hacer frente a la misma, incluidas aquellas destinadas a mitigar sus posibles efectos adversos.

Cuando, y en la medida en que, no sea posible facilitar toda esta información al mismo tiempo, la notificación inicial contendrá la información entonces disponible y se facilitará información adicional sin dilación indebida a medida que vaya estando disponible.

Las Partes establecerán en el Anexo III todos los demás elementos que el Encargado deba facilitar al Responsable al asistirle en el cumplimiento de las obligaciones del Responsable conforme a los artículos 33 y 34 del Reglamento (UE) 2016/679.

SECCIÓN III – DISPOSICIONES FINALES

Cláusula 10

Incumplimiento de las Cláusulas y resolución

(a) Sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679 y/o en el Reglamento (UE) 2018/1725, en caso de que el Encargado incumpla sus obligaciones en virtud de estas Cláusulas, el Responsable podrá instruir al Encargado para que suspenda el tratamiento de datos personales hasta que este cumpla con estas Cláusulas o hasta que el contrato se resuelva. El Encargado informará inmediatamente al Responsable si no puede cumplir estas Cláusulas, por cualquier motivo.

(b) El Responsable tendrá derecho a resolver el contrato en la medida en que se refiera al tratamiento de datos personales de conformidad con estas Cláusulas, si:

(i) el tratamiento de datos personales por el Encargado ha sido suspendido por el Responsable conforme al apartado (a) y el cumplimiento de estas Cláusulas no se restablece dentro de un plazo razonable y, en todo caso, en el plazo de un mes desde la suspensión;

(ii) el Encargado incumple de forma sustancial o persistente estas Cláusulas o sus obligaciones en virtud del Reglamento (UE) 2016/679 y/o del Reglamento (UE) 2018/1725;

(iii) el Encargado no cumple una decisión vinculante de un órgano jurisdiccional competente o de la autoridad de control competente respecto de sus obligaciones en virtud de estas Cláusulas o del Reglamento (UE) 2016/679 y/o del Reglamento (UE) 2018/1725.

(c) El Encargado tendrá derecho a resolver el contrato en la medida en que se refiera al tratamiento de datos personales conforme a estas Cláusulas cuando, tras haber informado al Responsable de que sus instrucciones infringen requisitos legales aplicables conforme a la cláusula 7.1 (b), el Responsable insista en seguir dichas instrucciones.

(d) Tras la resolución del contrato, el Encargado suprimirá o devolverá, a elección del Responsable, todos los datos personales tratados en nombre del Responsable, y suprimirá las copias existentes, salvo que el Derecho de la Unión o de los Estados miembros exija conservar los datos personales.

ANEXO I - Lista de las Partes

Responsable del tratamiento (Controller):

Nombre: _____

Dirección: _____

Nombre, cargo y datos de contacto de la persona de contacto: _____

Firma y fecha: _____

Encargado del tratamiento (Processor):

Nombre: NO ISOLATION GMBH

Dirección: THIERSCHSTRASSE 20, 80538, Munchen, Germany

Representado por director general Morten Jørgensen

Phone: +47 90 54 45 69

E-Mail: jorgensen@noisolation.com

Firma y fecha: _____

ANEXO II: Descripción del/los tratamiento(s)

La solución AV1 está diseñada para apoyar la inclusión de personas que no pueden asistir a la escuela durante períodos prolongados. La solución consta del robot de telepresencia AV1 («AV1») y de la aplicación AV1 instalada en el dispositivo del usuario final. El Responsable del Tratamiento también puede gestionar sus dispositivos AV1 y consultar datos estadísticos de uso a través del portal web AV1 Admin. Dado que todas las referencias realizadas a una unidad AV1 se hacen mediante un seudónimo y el Encargado del Tratamiento no dispone de medios razonables para la reidentificación, ningún dato de uso puede vincularse a una persona identificable por parte del Encargado.

AV1 permite la transmisión en directo, en tiempo real, de datos de audio y vídeo desde el aula hasta el dispositivo del usuario final (como un teléfono móvil o una tableta). El audio se transmite desde la aplicación del estudiante al AV1. AV1 permite al alumnado seguir de forma remota las actividades del aula desde su domicilio, al tiempo que permite que compañeros y profesorado vean y respondan a las señales y a la participación del estudiante. Todas las transmisiones se realizan en directo y no se almacenan grabaciones de audio ni de vídeo.

Los detalles relativos al tipo y alcance del tratamiento de datos personales se basan en las obligaciones contractuales establecidas en el Contrato Principal de Prestación de Servicios suscrito entre las Partes.

Con carácter general, el tratamiento de categorías especiales de datos personales en el sentido del artículo 9 del Reglamento (UE) 2016/679 (en lo sucesivo, el «RGPD») no forma parte de los acuerdos contractuales principales.

En la medida en que, en casos individuales, se traten categorías especiales de datos (por ejemplo, en el contexto de la puesta a disposición de contenidos de vídeo y audio), se adoptarán medidas técnicas y organizativas apropiadas para garantizar que, en particular, se tengan debidamente en cuenta los principios de minimización de datos y de confidencialidad.

La duración del tratamiento (cláusula 8.3) se basa en la duración del correspondiente Contrato Principal de Prestación de Servicios entre las Partes.

La naturaleza del tratamiento es la siguiente: recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión y supresión de datos.

Módulo de Servicio 1: «Entrega de AV1 y AV1 Admin» (Infraestructura)

La finalidad del tratamiento en el marco de este módulo de servicio es prestar los servicios acordados, en particular para:

- Administrar y gestionar los servicios correspondientes, incluida la incorporación (onboarding) de clientes.
- Crear y gestionar cuentas de clientes y autenticar a los clientes usuarios.
- Gestionar el inventario de AV1 (por ejemplo, generación de palabras clave para nuevos usuarios; creación de una lista de activos AV1).
- Proporcionar al cliente estadísticas sobre el uso de AV1.
- Realizar el seguimiento de cuándo se activa AV1 y del uso de la aplicación AV1 una vez activada.
- Implementar medidas de seguridad y gestionar la resolución de incidencias.

Categorías de datos personales tratados en este módulo:

- Datos de contacto (tratamiento, nombre, correo electrónico, lugar de trabajo, función, etc.).
- Datos de acceso (dirección de correo electrónico, credenciales).
- Datos de tráfico y uso de TI (dirección IP —no persistente—, fecha y hora de acceso, etc.).
- Otra información que el Responsable del Tratamiento pueda introducir en los campos de texto libre del portal AV1 Admin.
- Identificador de asignación del robot.
- Estadísticas de uso*.
- Motivos de asignación de AV1*.

* Las estadísticas de uso y los motivos de asignación se tratan por cuenta del Responsable del Tratamiento como parte de la solución AV1, tal y como se establece en el Contrato Principal de Prestación de Servicios. Asimismo, se agregan con el fin de analizar el uso y mejorar los servicios del Encargado del Tratamiento. Puede encontrarse más información en la política de privacidad de No Isolation.

Categorías de interesados:

- «Usuario del cliente» (miembro del personal de la organización educativa autorizado a utilizar el servicio).
- «Usuario final» (persona que utiliza la aplicación AV1).

Nota aclaratoria

Adicionalmente, salvo que la funcionalidad haya sido desactivada mediante instrucciones expresas del Responsable del Tratamiento, podrán tratarse también los siguientes datos seudonimizados —anonimizados desde la perspectiva del Encargado del Tratamiento—:

- Motivo de uso de AV1 (especificado de forma categorizada):
    - Enfermedad somática o lesión, Trastornos de salud mental (SEMH), Intervención temprana para prevenir el rechazo escolar, Necesidades educativas especiales (NEE), Apoyo conductual y exclusión temporal, Situaciones de desplazamiento, transitorias o de vivienda inestable, Discapacidad, Estudiantes de alta capacidad con aprendizaje remoto, Programas educativos alternativos, Otros motivos
- Género del usuario
    - Estos datos son proporcionados al Encargado del Tratamiento por el Responsable del Tratamiento a través de la infraestructura técnica en una forma anonimizada para el Encargado, y se utilizan con el fin de proporcionar al Responsable evaluaciones estadísticas sobre el uso de los avatares AV1. No es posible que el Encargado del Tratamiento extraiga conclusiones sobre personas físicas ni establezca un vínculo con individuos identificables. En este sentido, no tiene lugar un tratamiento por cuenta del Responsable respecto de dichos datos.

El Responsable del Tratamiento es el único responsable de verificar la licitud del tratamiento para la anonimización (antes de la transmisión de los datos mencionados).

Categorías de interesados en este módulo:

Los datos personales se recogen de: el «usuario del cliente» (es decir, miembro del personal de la organización educativa autorizado a utilizar el servicio), y el «usuario final» (es decir, estudiantes que utilizan la aplicación AV1 o sus progenitores).

Módulo de Servicio 2: «AV1 y la aplicación AV1» (Transmisión en directo)

La finalidad del tratamiento en el marco de este módulo de servicio es posibilitar la prestación y el uso de transmisiones en directo (livestreaming) entre un dispositivo móvil (por ejemplo, un iPad) y AV1, concretamente para proporcionar al usuario final los medios técnicos necesarios para participar en actividades educativas y otras actividades escolares desde una ubicación diferente.

Categorías de datos personales tratados en este módulo:

- Datos de audio y vídeo (cifrados) (no persistentes).
- Metadatos (duración y calidad de la transmisión de vídeo, fecha y hora, información sobre la red inalámbrica, intensidad de la señal, información de la red móvil).
- Direcciones IP (no persistentes).

Categorías de interesados:

- Usuario del cliente.
- Usuario final.
- *Otros estudiantes, profesorado o empleados del cliente presentes en el aula u otras personas físicas en el contexto de una actividad escolar.

* Los datos de audio y vídeo se transmiten como parte de la transmisión en directo al usuario final. Estos datos no se almacenan en ningún momento y, por tanto, no son persistentes. La transmisión en directo está cifrada de extremo a extremo, y nadie excepto el usuario final puede acceder a ella, incluido el propio Encargado del Tratamiento.

Módulo de Servicio 3: «Soporte Técnico»

La finalidad del tratamiento en el marco de este módulo de servicio es prestar servicios de soporte técnico tanto a los usuarios del cliente como a los usuarios finales (incluida la investigación de solicitudes de soporte y la resolución de incidencias técnicas).

Tipos de datos personales tratados en este módulo:

- Datos de contacto (por ejemplo, nombre, dirección de correo electrónico, número de teléfono).
- Datos de contenido incluidos en las comunicaciones escritas entre el Responsable del Tratamiento y el Encargado del Tratamiento, que en casos concretos pueden contener datos personales.
- Metadatos (duración y calidad de la transmisión de vídeo, fecha y hora, información sobre la red inalámbrica, intensidad de la señal, información de la red móvil).

Categorías de interesados:

- Usuarios del cliente.
- Usuarios finales.
- Empleados tanto del Responsable del Tratamiento como del Encargado del Tratamiento.
- «Usuario del cliente»: miembro del personal de la organización educativa autorizado a utilizar el servicio.

ANEXO III: MEDIDAS TÉCNICAS Y ORGANIZATIVAS, INCLUIDAS LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LA SEGURIDAD DE LOS DATOS

Cumplimiento de los requisitos de seguridad del tratamiento de datos conforme al artículo 32 del RGPD. Medidas para proteger la confidencialidad, integridad y disponibilidad.	
Seudonimización, anonimización y cifrado de los datos personales	☒ Seudonimización El usuario final recibe un identificador de usuario seudonimizado a través del Responsable del Tratamiento. El Encargado del Tratamiento no tiene conocimiento de la identidad del usuario. ☒ Cifrado ☒ Datos en tránsito ☒ Datos en reposo El cifrado se realiza mediante TLS 1.2 y AES de 256 bits. ☒ Anonimización Todos los metadatos se anonimizan cuando ya no existe una suscripción activa para AV1.
Confidencialidad de los sistemas y servicios de tratamiento	☒ Control de acceso físico (control físico) Todas las instalaciones están equipadas con sistemas de alarma antirrobo y videovigilancia en las entradas y salidas, gestionados y mantenidos por los arrendadores. Existen medidas para evitar que personas no autorizadas accedan a los lugares donde se encuentran los sistemas. El personal de No Isolation recibe formación sobre los procedimientos para el cierre y apertura seguros de las instalaciones. El personal de No Isolation debe utilizar tarjetas de acceso individuales protegidas por PIN o llaves físicas tradicionales (según la ubicación) para acceder a las instalaciones. El personal autorizado figura en el inventario de equipamiento gestionado por la persona responsable de la oficina en Noruega y delegado a los directores en Alemania y el Reino Unido. Los visitantes deben estar acompañados en todo momento por personal de No Isolation. ☒ Control de acceso a sistemas y datos (control organizativo / técnico)

	Solo las personas autorizadas tienen acceso a los sistemas en los que se almacenan datos personales y metadatos. El acceso se concede conforme al principio de necesidad de conocer y se supervisa y registra. Los sistemas internos de gestión de No Isolation y los sistemas de gestión propiedad de los clientes utilizan controles de acceso basados en roles, restringiendo la capacidad de modificar o eliminar datos a organizaciones de clientes específicas y grupos de usuarios autorizados. El acceso a los sistemas y a las cuentas basadas en la nube se realiza mediante un identificador de usuario asignado y autenticación de doble factor. El acceso a la infraestructura de No Isolation está sujeto a normas y reglas de seguridad que solo permiten tráfico procedente de fuentes autorizadas. El acceso a los recursos de la infraestructura se limita a los administradores de No Isolation (personal de operaciones) que necesitan dicho acceso para realizar tareas de mantenimiento de los sistemas.
Integridad de los sistemas y servicios de tratamiento	Registro de eventos (por ejemplo, durante autenticación o acciones CRUD: crear, leer, actualizar, eliminar datos): ☒ Control de entrada (Verificación de cuándo y por quién se han introducido, modificado o eliminado datos personales) Los sistemas solo exponen el conjunto mínimo de puntos finales necesarios para prestar los servicios. Los puntos finales expuestos solo admiten HTTPS y todos los clientes deben autenticarse contra el sistema antes de poder utilizarlos. Existen medidas para verificar quién ha introducido, modificado o eliminado datos personales en los sistemas. Las bases de datos y los sistemas de almacenamiento de datos se mantienen mediante la aplicación continua de medidas de mantenimiento, recomendaciones y buenas prácticas de los proveedores; todos los procedimientos mediante los cuales se introducen, almacenan y tratan datos personales están diseñados con salvaguardas de integridad y seguridad integradas. Todos estos procedimientos se prueban exhaustivamente y se someten a revisión por pares antes de su implementación. ☒ Control de transmisión y comunicación *(Verificación de a qué entidades se han transmitido datos personales)* Toda transmisión de datos por Internet relacionada con AV1 está cifrada al menos conforme al estándar TLS 1.2 y cubre las transmisiones necesarias para la prestación de

	los servicios. Todas las señales están cifradas con claves robustas y utilizan el protocolo HTTPS. Las bases de datos y servidores disponen de discos, copias de seguridad y comunicaciones cifradas. Todo el tráfico multimedia (es decir, transmisión de audio y vídeo) utiliza SRTP (con DTLS para el intercambio de claves) o DTLS. Las comunicaciones se cifran de extremo a extremo mediante estas claves, tanto si se realizan directamente entre AV1 y las aplicaciones como si se realizan a través de un servidor de retransmisión. Los metadatos (incluidas direcciones IP, identificadores de extremo y claves de cifrado) necesarios para establecer las conexiones se envían cifrados mediante TLS entre AV1 y los servidores de No Isolation. Se utiliza el estándar WebRTC para establecer la transmisión de audio y vídeo, y las señales WebRTC (es decir, metadatos) se transmiten cifradas mediante TLS a través de los servidores de No Isolation.
Disponibilidad de los sistemas y servicios de tratamiento y capacidad de restauración	☒ Recuperabilidad (recuperación / copias de seguridad) No Isolation utiliza servicios en la nube para garantizar que los datos y servicios estén disponibles cuando sea necesario. El proveedor realiza copias de seguridad de los sistemas críticos cada 24 horas. Las copias de seguridad se almacenan en la nube para permitir la restauración rápida de los sistemas, si fuera necesario, en una ubicación diferente (por ejemplo, en caso de daños como incendios o fallos eléctricos). No Isolation mantiene un plan de continuidad del negocio (“BC Plan”) que incluye procedimientos para proteger frente a interrupciones causadas por eventos imprevistos e incorpora canales de notificación, contactos de emergencia, formación de equipos de respuesta y planes de contingencia para sistemas críticos. El BC Plan se prueba anualmente, y los resultados y mejoras se gestionan como parte del Sistema de Gestión de Seguridad de la Información de No Isolation. La información de software y configuración relativa a los sistemas y a los servicios de aplicaciones desarrollados y gestionados internamente se gestiona en un repositorio de código fuente seguro. No Isolation puede restaurar o volver a desplegar rápidamente los servicios de aplicaciones si fuera necesario, incluida la posibilidad de trasladar los servicios a otra ubicación si se requiere. ☒ Control de fiabilidad (notificación de fallos, errores y amenazas)

	Los sistemas en red están protegidos frente a accesos no autorizados mediante cortafuegos, servicios de protección de endpoints y herramientas de supervisión y gestión. La infraestructura de No Isolation registra información sobre el comportamiento del sistema, el tráfico recibido, la autenticación del sistema y otras solicitudes de aplicaciones. Los sistemas internos alertan al personal correspondiente ante actividades maliciosas, no intencionadas o atípicas. El personal de No Isolation, incluidos los equipos de seguridad, operaciones y soporte, está formado para responder a incidentes de seguridad identificados. Se mantienen registros de los incidentes de seguridad identificados. Los incidentes sospechosos y confirmados se investigan y se documentan las medidas de resolución adecuadas. En el caso de incidentes de seguridad confirmados, se realiza una revisión posterior al incidente y se adoptan las acciones apropiadas para minimizar el riesgo de daños o divulgación no autorizada. El proveedor supervisa continuamente sus sistemas con notificaciones directas al personal operativo en caso de fallo de cualquier sistema. Se despliegan aplicaciones de monitorización configuradas para supervisar la capacidad del sistema y alertar al personal de operaciones cuando se alcanzan umbrales predefinidos. ☒ Disponibilidad (redundancias de sistemas e infraestructuras) Las rutinas de continuidad del negocio, recuperación ante desastres y respuesta a incidentes son proporcionadas por el proveedor de infraestructura en la nube de No Isolation y por los proveedores SaaS (que emplean esfuerzos comercialmente razonables para garantizar la disponibilidad, energía redundante, red y servicios de climatización). Las políticas ISO 27001 —por ejemplo, gestión de vulnerabilidades, copias de seguridad, gestión de riesgos y gestión de parches— reflejan un enfoque gestionado de los objetivos de seguridad de la información. La infraestructura es proporcionada por AWS, con entornos separados para diseño/pruebas (staging) y producción. La disponibilidad se supervisa de forma continua.

Tratamiento de datos personales únicamente conforme a instrucciones documentadas del Responsable	☒ Control de encargos (los datos personales se tratan únicamente conforme a las instrucciones del cliente) No Isolation mantiene contratos con su personal (incluidos empleados, consultores y trabajadores contratados) que incluyen obligaciones de confidencialidad. El deber de confidencialidad continúa tras la finalización de la relación laboral y mientras la información siga siendo confidencial. El acceso para diagnóstico remoto solo se concede con la aprobación del Cliente. Las sesiones de diagnóstico remoto se registran y, en función del nivel de acceso requerido, el personal de soporte debe presentar una clave física de autenticación de hardware para iniciar la sesión de diagnóstico remoto. De conformidad con este Acuerdo, No Isolation está obligada a tratar los datos únicamente conforme a instrucciones documentadas. El personal recibe la información y formación necesarias al respecto. Se especifica qué personas pueden emitir y recibir instrucciones relativas al tratamiento. ☒ Separación de datos (los datos personales recogidos para finalidades distintas se tratan de forma separada) Se aplica una separación lógica adicional dentro del software de No Isolation mediante identificadores fijos y únicos de cliente y dispositivo, así como tokens temporales seguros basados en sesión generados tras conexiones autenticadas con éxito.
Proceso para probar, evaluar y valorar periódicamente la eficacia de las medidas técnicas y organizativas	☒ Responsable de Seguridad de la Información (ISO) designado ☒ Sistema de Gestión de Seguridad de la Información (SGSI / ISMS)
Pruebas del cumplimiento de la seguridad del tratamiento de datos mediante certificaciones o medidas organizativas reconocidas	*Certificaciones relevantes* ☒ ISO 27001 – Sistema de Gestión de Seguridad de la Información La información relativa a los controles es verificable de forma creíble mediante conceptos y directrices documentados en el ámbito de la certificación ISO 27001.

ANEXO IV – LISTA DE SUBENCARGADOS DEL TRATAMIENTO

El Responsable del Tratamiento ha autorizado el uso de los siguientes Subencargados del Tratamiento de conformidad con la Cláusula 8.7(a):

1. Amazon Web Services EMEA SARL
   38, Avenue John F. Kenned
   1855 Luxemburg
   Luxemburgo

Objeto del encargo:
Servicios de infraestructura en la nube.

Tratamiento en: UE
Ubicación del centro de datos: Frankfurt am Main, Alemania

El Subencargado del Tratamiento se ha obligado contractualmente a alojar los datos exclusivamente en Frankfurt. No se prevén transferencias de datos, salvo cuando sea estrictamente necesario para fines de soporte o para el cumplimiento de la legislación nacional de los Estados Unidos.

Como garantías adecuadas en el sentido de los artículos 44 y siguientes del RGPD, se ha formalizado un acuerdo de tratamiento de datos utilizando las Cláusulas Contractuales Tipo (SCC) de la Comisión Europea (vigentes desde junio de 2021). Como medidas complementarias, se han seleccionado configuraciones respetuosas con la protección de datos (minimización de datos) y se han implementado medidas técnicas adecuadas, como la seudonimización.

2. No Isolation AS
   Pilestredet 2
   0166 Osl
   Noruega

Objeto del encargo:
Prestación de servicios de atención al cliente (CRM).

Tratamiento en: EEE (Noruega)

3. No Isolation GmbH
   Innere Wiener Straße 1
   81667 Múnic
   Alemania

Objeto del encargo:
Prestación de servicios de atención al cliente (CRM).

Tratamiento en: UE (Alemania)