ACUERDO DE TRATAMIENTO DE DATOS (DPA) PARA SERVICIOS VDO FLEET (ANEXO C)

Este DPA establece las obligaciones legales de las PARTES en relación con la protección de datos resultante del tratamiento de datos personales relativa al respectivo contrato de SERVICIOS VDO FLEET con el Cliente. El presente DPA se basa en las cláusulas contractuales estándar establecidas por la Comisión Europea en la Decisión de Implementación (UE) 2021/915.

El Cliente como "Responsable" y Continental Trading GmbH como "Encargado" acuerdan lo que sigue:

SECCIÓN I

CLÁUSULA 1
Objeto y alcance

a) El objeto de las presentes Cláusulas Contractuales Estándar (las Cláusulas) es asegurar el cumplimiento del Artículo 28(3) y (4) del Reglamento (EU) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 sobre la protección de las personas físicas en relación con el tratamiento de datos personales y sobre la libre circulación de tales datos, que deroga la Directiva 95/46/EC (Reglamento General de Protección de Datos).

b) El/los responsable/s y el/los Encargado/s, como se ha indicado, han acordado las presentes Cláusulas con el fin de asegurar el cumplimiento de lo previsto en el Artículo 28(3) and (4) del Reglamento (UE) 2016/679 y/o el Artículo 29 (3) y (4) del Reglamento (UE) 2018/1725.

c) Estas Cláusulas se aplican al tratamiento de datos personales como se especifica en el Anexo I.

d) Los Anexos I a III son parte integral de las Cláusulas.

e) Las Cláusulas son sin perjuicio de las obligaciones a las que está sujeto el responsable en virtud del Reglamento (UE) 2016/679 y/o el Reglamento (UE) 2018/1725.

f) Estas Cláusulas por sí solas no garantizan el cumplimiento de las obligaciones en relación con la transferencia internacional de datos según el Capítulo V del Reglamento (UE) 2016/679 y/o el Reglamento (EU) 2018/1725.

CLÁUSULA 2
No modificación de las Cláusulas

a) Las Partes se comprometen a no modificar las Cláusulas excepto para añadir información a los Anexos o para actualizar la información contenida en ellos.

b) Eso no evita que las Partes incluyan las cláusulas contractuales estándar contenidas en el presente en un contrato más Amplio, ni que añadan otras cláusulas o salvaguardias adicionales, siempre y cuando ello no suponga contradecir de forma directa o indirecta las Cláusulas o sea en detrimento de los derechos y libertades fundamentales de los Interesados.

CLÁUSULA 3
Interpretación

a) Donde estas Cláusulas usan los términos definidos en el Reglamento (UE) 2016/679 o en el Reglamento (UE) 2018/1725 respectivamente, esos términos tendrán el mismo significado que en el Reglamento correspondiente.

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

c) Estas Cláusulas no se interpretarán de forma que sea contraria a los derechos y obligaciones establecidos en el Reglamento (UE) 2016/679 / Reglamento (UE) 2018/1725 o de forma que perjudiquen los derechos fundamentales o libertades de los Interesados.

CLÁUSULA 4
Jerarquía / Orden de prelación

En caso de contradicción entre estas Cláusulas y las previsiones o acuerdos relacionados entre las Partes existentes a la fecha en que estas Cláusulas se acuerden o entren en vigor, las Cláusulas prevalecerán

CLÁUSULA 5
Cláusula de adhesión

a) Una entidad que no sea parte de esta Cláusulas puede, con el acuerdo de todas las Partes, adherirse a estas Cláusulas como Encargado o Responsable, completando los Anexos y firmando el presente DPA.

b) Una vez los Anexos en (a) se han completado y firmado, la entidad que se adhiere será tratada como una Parte de estas Cláusulas y tendrá los derechos y obligaciones de un Encargado o de un responsable, de conformidad con lo firmado.

c) La Parte que se adhiere no tendrá ni derechos ni obligaciones que resulten de estas Cláusulas en el periodo anterior a haberse convertido 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 la finalidad del tratamiento por el que los datos son tratados en nombre del responsable se especifican en el Anexo I.

CLÁUSULA 7
Obligaciones de las Partes

7.1. Instrucciones

a) El Encargado del tratamiento sólo tratará los datos personales siguiendo instrucciones escritas del responsable del tratamiento, salvo exigencia de la legislación de la Unión o del Estados miembros al que esté sometido el Encargado. En este caso, el Encargado del tratamiento informará al responsable del tratamiento de dicho requisito legal antes del tratamiento, a menos que la ley lo prohíba por motivos importantes de interés público. El responsable del tratamiento también podrá dar instrucciones posteriores mientras dure el tratamiento de los datos personales. Estas instrucciones deberán estar siempre documentadas.

b) El Encargado informará inmediatamente al responsable si, en opinión del Encargado, las instrucciones dadas por el Responsable infringen el Reglamento (UE) 2016/679 / Reglamento (UE) 2018/1725 o las normas en materia de protección de datos de la Unión o del Estado Miembro.

7.2. Limitación del Objeto del Tratamiento

El Encargado tratará los datos solo para los fines específicos del tratamiento, como se dice en el Anexo I, a menos que reciba ulteriores instrucciones del responsable.

7.3. Duración del Tratamiento de datos personales

El Tratamiento por parte del Encargado tendrá lugar solamente por el periodo de tiempo establecido en el Anexo I.

7.4. Seguridad del tratamiento

a) El Encargado del tratamiento aplicará, como mínimo, las medidas técnicas y organizativas especificadas en el Anexo II para garantizar la seguridad de los datos personales. Esto incluye la protección de los datos contra una violación de la seguridad que provoque su destrucción accidental o ilícita, su pérdida, su alteración, su divulgación no autorizada o el acceso a los mismos (violación de los datos personales). Al evaluar el nivel adecuado de seguridad, las Partes tendrán debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos que entraña para los interesados.

b) El Encargado del Tratamiento concederá acceso a los datos personales objeto de tratamiento a los miembros de su personal sólo en la medida estrictamente necesaria para la ejecución, gestión y seguimiento del contrato. El Encargado del tratamiento se asegurará de que las personas autorizadas a tratar los datos personales recibidos se hayan comprometido a mantener la confidencialidad o estén sometidas a una obligación legal adecuada de confidencialidad.

7.5. Datos Sensibles

Si el tratamiento incluye datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, o la pertenencia a un sindicato, datos genéticos o biométricos con el fin de identificar de forma inequívoca a una persona física, datos relativos a la salud o a la vida sexual u orientación sexual de una persona, o datos relativos a condenas e infracciones penales ("datos sensibles"), el Encargado del tratamiento aplicará restricciones específicas y/o garantías adicionales.

7.6 Documentación y Cumplimiento normativo

a) Las Partes deberán ser capaces de demostrar el cumplimiento de estas Cláusulas.

b) El Encargado gestionará pronta y adecuadamente las solicitudes del responsable sobre el tratamiento de los datos de conformidad con estas cláusulas.

c) El Encargado del Tratamiento pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones que se establecen en estas Cláusulas y que se derivan directamente del Reglamento (UE) 2016/679 y/o del Reglamento (UE) 2018/1725. A petición del responsable, el Encargado del Tratamiento también permitirá y contribuirá a las auditorías de las actividades de tratamiento cubiertas por estas Cláusulas, a intervalos razonables o si hay indicios de incumplimiento. Al decidir sobre una revisión o una auditoría, el responsable tendrá en cuenta las certificaciones pertinentes que posea el Encargado del Tratamiento.

d) El responsable del Tratamiento podrá optar por realizar la auditoría por sí mismo o encargarla a un auditor independiente. Las auditorías también podrán incluir inspecciones en los locales o instalaciones físicas del Encargado del Tratamiento y, en su caso, se llevarán a cabo con una antelación razonable.

e) Las Partes pondrán la información mencionada en esta cláusula, incluidos los resultados de cualquier auditoría, a disposición de la(s) autoridad(es) de control competente(s) que lo solicite(n)

7.7. Uso de Sub-Encargados

a) El Encargado del Tratamiento cuenta con la autorización general del responsable para la contratación de sub-encargados de una lista acordada. El Encargado del Tratamiento informará específicamente por escrito al responsable de cualquier cambio previsto en dicha lista mediante la adición o sustitución de sub-encargados con al menos 30 (treinta) días de antelación, dando así al responsable tiempo suficiente para poder oponerse a dichos cambios antes de la contratación del sub-encargado o sub-encargados en cuestión. El Encargado del tratamiento facilitará al responsable del tratamiento la información necesaria para que éste pueda ejercer su derecho de oposición. Si el responsable del tratamiento no se opone en un plazo de 30 días, se considerará concedido el consentimiento.

El responsable del tratamiento está de acuerdo con la participación de los sub-Encargados que figuran en el anexo III.

b) Cuando el Encargado del Tratamiento contrate a un sub-encargado para la realización de actividades específicas de tratamiento (por cuenta del responsable), lo hará mediante un contrato que imponga al sub-encargado, en esencia, las mismas obligaciones de protección de datos que las impuestas al Encargado del Tratamiento de conformidad con las presentes Cláusulas. El Encargado del Tratamiento se asegurará de que el sub-encargado cumpla con las obligaciones a las que está sujeto el Encargado del Tratamiento de conformidad con estas Cláusulas y con el Reglamento (UE) 2016/679 y/o el Reglamento (UE) 2018/1725

c) A petición del responsable del Tratamiento, el Encargado del Tratamiento facilitará al responsable del Tratamiento una copia de dicho acuerdo con el sub-encargado y de cualquier modificación posterior. En la medida necesaria para proteger el secreto comercial u otra información confidencial, incluidos los datos personales, el Encargado del tratamiento podrá editar el texto del acuerdo antes de compartir la copia.

d) El Encargado del tratamiento seguirá siendo plenamente Responsable ante el responsable del tratamiento del cumplimiento de las obligaciones del sub-encargado del tratamiento de conformidad con su contrato con el Encargado del tratamiento. El Encargado del tratamiento notificará al responsable del tratamiento cualquier incumplimiento de sus obligaciones contractuales por parte del sub-encargado.

7.8. Transferencias internacionales de datos / tratamiento internacional de datos

a)

Toda transferencia de datos a un tercer país o a una organización internacional por parte del Encargado del tratamiento se realizará -sin perjuicio de lo dispuesto en la letra b siguiente- únicamente

i. sobre la base de instrucciones documentadas,
ii. sobre la base de un consentimiento previo (general) del Responsable del tratamiento o
iii. para cumplir un requisito específico en virtud de la legislación de la Unión o del Estado miembro a la que está sujeto el Responsable del Tratamiento, y tendrá lugar de conformidad con el capítulo V del Reglamento (UE) 2016/679 o el Reglamento (UE) 2018/1725.

b) Cuando el Encargado del Tratamiento contrate a un sub-encargado de acuerdo con la cláusula 7.7. para la realización de 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 Responsable acepta que dicho tratamiento esté permitido siempre que

i. el tratamiento se llevará a cabo en un país para el que la Comisión de la UE ha adoptado una decisión de adecuación respectiva sobre la base del artículo 45 del Reglamento (UE) 2016/679, o

ii. el procesador y el sub-encargado garantizan el cumplimiento del capítulo V del Reglamento (UE) 2016/679 mediante el uso de cláusulas contractuales estándar adoptadas por la Comisión de conformidad con el artículo 46, apartado 2, del Reglamento (UE) 2016/679, siempre que se cumplan las condiciones para el uso de dichas cláusulas contractuales estándar.

c) El responsable del tratamiento está de acuerdo con la transferencia y el tratamiento de los datos personales en el sentido del capítulo V del Reglamento (UE) 2016/679 por parte del procesador y/o los sub-encargados que se enumeran en el anexo III.

CLÁUSULA 8
Asistencia al Responsable del Tratamiento

a) El Encargado del tratamiento notificará sin demora al Responsable del tratamiento cualquier solicitud que haya recibido del interesado. No responderá a la solicitud por sí mismo, a menos que el Responsable del tratamiento le autorice a hacerlo.

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

c) Además de la obligación del Encargado del Tratamiento de asistir al Responsable del Tratamiento en virtud de la cláusula 8(b), el Encargado del Tratamiento asistirá además al Responsable del Tratamiento para garantizar el cumplimiento de las siguientes obligaciones, teniendo en cuenta la naturaleza del tratamiento de datos y la información de que dispone el Encargado:

i. la obligación de realizar una evaluación del impacto de las operaciones de tratamiento previstas sobre la protección de los datos personales (una "evaluación de impacto sobre la protección de datos") cuando un tipo de tratamiento pueda suponer 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) antes del tratamiento cuando una evaluación de impacto sobre la protección de datos indique que el tratamiento supondría un riesgo elevado en ausencia de medidas adoptadas por el Responsable del tratamiento para mitigar el riesgo

iii. la obligación de garantizar que los datos personales sean exactos y estén actualizados, informando sin demora al Responsable del tratamiento si éste tiene conocimiento de que los datos personales que está tratando son inexactos o han quedado obsoletos;

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

d) Las Partes establecerán en el Anexo II las medidas técnicas y organizativas apropiadas mediante las cuales el Encargado del tratamiento deberá asistir al Responsable del tratamiento en la aplicación de la presente cláusula, así como el ámbito y el alcance de la asistencia requerida.

CLÁUSULA 9
Notificación de violación de datos personales

En caso de que se produzca una violación de los datos personales, el Encargado del tratamiento cooperará con el Responsable del tratamiento y le prestará asistencia para que este cumpla las obligaciones que le incumben 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 proceda, teniendo en cuenta la naturaleza del tratamiento y la información de que dispone el Encargado.

9.1 Violación de datos relativa a datos tratados por el Responsable

En caso de que se produzca una violación de los datos personales relativos a los datos tratados por el Responsable del tratamiento, el Encargado del tratamiento asistirá al Responsable del tratamiento:

a) en notificar la violación de los datos personales a la(s) autoridad(es) de control competente(s), sin demora indebida después de que el Responsable del tratamiento haya tenido conocimiento de ella, cuando proceda/(salvo que sea improbable que la violación de los datos personales suponga un riesgo para los derechos y libertades de las personas físicas);

b) en la obtención de la siguiente información que, de acuerdo con el artículo 33.3 del Reglamento (UE) 2016/679, se hará constar en la notificación del Responsable del tratamiento, y deberá incluir, al menos:

i. la naturaleza de los datos personales, incluyendo, 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;

ii. las probables consecuencias de la violación de datos personales;

iii. las medidas adoptadas o propuestas por el Responsable del tratamiento para hacer frente a la violación de los datos personales, incluidas, en su caso, las medidas para mitigar sus posibles efectos adversos

Cuando, y en la medida en que no sea posible proporcionar toda esta información al mismo tiempo, la notificación inicial contendrá la información disponible en ese momento y la información adicional, a medida que esté disponible, se proporcionará posteriormente sin demora injustificada

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 los datos personales al interesado, cuando la violación de los datos personales pueda suponer un alto riesgo para los derechos y libertades de las personas físicas

9.2 Violación de datos tratados por el Encargado del Tratamiento

En caso de que se produzca una violación de los datos personales relativos a los datos tratados por el Encargado del tratamiento, éste notificará al Responsable del tratamiento sin demora indebida una vez que haya tenido conocimiento de la 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 y registros de datos afectados);

b) Los datos de un punto de contacto en el que pueda obtenerse más información sobre la violación de los datos personales

c) sus probables consecuencias y las medidas adoptadas o propuestas para hacer frente a la infracción, incluyendo para mitigar sus posibles efectos adversos.

Cuando no sea posible
, y en la medida en que no sea posible proporcionar toda esta información al mismo tiempo, la notificación inicial contendrá la información disponible en ese momento y, posteriormente, se proporcionará más información, a medida que esté disponible, sin demoras indebidas.

Las Partes establecerán en el anexo II todos los demás elementos que debe proporcionar el Encargado del tratamiento cuando asista al Responsable del tratamiento en el cumplimiento de las obligaciones de este último en virtud de los artículos 33 y 34 del Reglamento (UE) 2016/679.

SECCIÓN III
DISPOSICIONES FINALES

CLÁUSULA 10
Incumplimiento de las Cláusulas y terminación

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 del Tratamiento incumpla las obligaciones que le incumben en virtud de las presentes Cláusulas, el Responsable del Tratamiento podrá ordenar al Encargado que suspenda el tratamiento de los datos personales hasta que este último cumpla las presentes Cláusulas o sea resuelto el Contrato. El Encargado del Tratamiento informará sin demora al Responsable del Tratamiento en caso de que no pueda cumplir las presentes Cláusulas, cualquiera que sea el motivo.

b) El Responsable del tratamiento tendrá derecho a rescindir 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 parte del Encargado del Tratamiento ha sido suspendido por el Responsable del Tratamiento en virtud de la letra a) y si no se restablece el cumplimiento de las presentes Cláusulas en un plazo razonable y, en cualquier caso, en el plazo de un mes tras la suspensión

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

   i. El Encargado del tratamiento incumple una decisión vinculante de un tribunal competente o de la(s) autoridad(es) de supervisión competente(s) en relación con sus obligaciones en virtud de las presentes cláusulas o del Reglamento (UE) 2016/679 y/o del Reglamento (UE) 2018/1725.

c) El Encargado del tratamiento tendrá derecho a rescindir el contrato en la medida en que se refiera al tratamiento de datos personales con arreglo a las presentes cláusulas cuando, tras haber informado al Responsable del tratamiento de que sus instrucciones infringen los requisitos legales aplicables de conformidad con la cláusula 7.1 b), el Responsable del tratamiento insista en el cumplimiento de las instrucciones

d) Tras la finalización del contrato, el Encargado del tratamiento deberá, a elección del Responsable del tratamiento, suprimir todos los datos personales tratados por cuenta del Responsable del tratamiento y certificar al Responsable del tratamiento que lo ha hecho, o bien devolver todos los datos personales al Responsable del tratamiento y suprimir las copias existentes, a menos que la legislación de la Unión o del Estado miembro exija la conservación de los datos personales. Hasta que se eliminen o devuelvan los datos, el Encargado del tratamiento seguirá garantizando el cumplimiento de estas cláusulas.

CLÁUSUL A11
Lista de Anexos

Anexo I: Detalles del tratamiento
Anexo II: Medidas técnicas y organizativas implementadas por CONTINENTAL.
Anexo III: Sub-Encargados, transferencias internacionales de datos / tratamiento de datos

ANEXO I – DETALLES DEL TRATAMIENTO

1. OBJETO DEL ENCARGO

CONTINENTAL queda instruido para actuar como encargado del tratamiento, con el fin de tratar por cuenta del CLIENTE (el responsable del tratamiento) los datos personales que son necesarios para la prestación de los servicios de la aplicación VDO FLEET.

2. FORMA Y FINALIDAD DEL TRATAMIENTO

2.1 CONTINENTAL está facultada para recoger, tratar y utilizar los datos personales únicamente de acuerdo con el CONTRATO DE SERVICIOS TIS WEB y las instrucciones del CLIENTE (véase cláusula 7.1).

2.2 Los detalles sobre el alcance, la naturaleza y la finalidad de la recopilación, el tratamiento y/o el uso de los datos personales están sujetos a las Condiciones Generales del Contrato Principal, su Descripción de Servicios, así como las descripciones funcionales de los productos.

3. CATEGORÍAS DE INTERESADOS

☒ Clientes
☐ Participantes en eventos
☒ Participantes en comunicaciones
☐ Partes interesadas
☐ Suministradores y/o Proveedores de Servicios (contactos individuales en esos vendedores)
☒ Empleados
☐ Antiguos empleados
☐ Familiares de empleados
☒ Representantes de ventas
☒ Personas de Contacto de Negocio
☒ Socios de Negocios
☐ Visitantes
☒ Usuarios de Servicios
☒ Suscriptores
☐ Solicitantes de empleo
☐ Aprendices / becarios
☐ Consultores
☐ Accionistas / Órganos Colegiados
☐ Proveedores de bienes y servicios
☒ Otros, por favor especificar: empleados de los clientes, por ejemplo, conductores y usuarios de los Servicios VDO FLEET

4. CLASES DE DATOS PERSONALES

Datos Generales / datos privados de contacto:

☒ Nombres, perfiles personales
☒ Dirección particular
☒ Número de identificación (e.g. Pasaporte, NIF, carnet de conducir, nº TGSS)
☐ Otros, por favor especificar:
☐ Imagen
☒ Fecha de nacimiento

_____

Datos contractuales:

☒ Datos de pago
☒ Estado Financiero / Solvencia
☒ Datos bancarios / tarjeta de crédito
☒ Historial de contratación

☐ Otros por favor especificar:_____

Datos Profesionales:

☒ Detalles Personales
☒ Gestión del Desempeño
☐ Detalles de Puesto y Empleo
☐ Detalles de cualificación y académicos

☒ Datos de Seguridad Social ☒ Ausencias del trabajo
☒ Otros, por favor especificar:

- Datos de admisión del cliente y de sus operadores / usuarios
- Datos del conductor
- Datos del vehículo y perfil del vehículo
- Datos de comunicación (e.g. teléfono, email)
- Datos de movimientos, datos del GPS
- Actividad de los conductores y perfiles de sus movimientos, incluyendo tiempos de conducción y de descanso conforme al Anexo 1B del Reglamento UE 561/2006, Reglamento (CE) nº 1360/2002, Reglamento nº 165/2014 y Reglamento UE nº 2016/799.
- Datos para el uso del servicio, descargas de datos para la tarjeta del conductor y el tacógrafo

Datos de Servicio y de uso de IT:

☐ Identificadores de dispositivo
☐ Datos de imagen / video
☐ Datos de audio / voz
☒ Datos de acceso
☐ Metadatos
☐ Otros, por favor especificar:

☒ Datos de uso y conexión
☒ Datos de telecomunicaciones/contenido
☐ Datos de identificación
☐ Autorizaciones

_____

Categorías especiales de datos personales:

☐ Raza u origen étnico
☐ Salud física o mental
☐ Datos biométricos
☐ Afiliación Sindical
☐ Condenas, Sentencias, antecedentes penales
☐ Otros, por favor especificar:

☐ Creencias religiosas o filosóficas
☐ Opiniones Políticas
☐ Datos genéticos
☐ Vida Sexual

_____

5. DURACIÓN DEL TRATAMIENTO

5.1 La duración del tratamiento de datos depende de la duración del Contrato y/o cualquier contrato u orden individual basada en un acuerdo marco.

5.2 Hasta la finalización del tratamiento y sin perjuicio de otras instrucciones escritas del Responsable del Tratamiento, el Encargado del Tratamiento devolverá al Responsable del Tratamiento o a un tercero designado por éste, todos los documentos, soportes de datos, resultados del tratamiento y datos que hayan llegado a su poder, y que estén relacionados con la relación contractual o se hayan generado en el curso de la ejecución del Contrato y/o de la presente DPA.

Esta obligación se extiende a las copias y/o reproducciones de los soportes de datos y/o de los datos almacenados. No hay derecho de retención con respecto a los datos y soportes de datos mencionados. Salvo que se disponga lo contrario en el Contrato, el Encargado del Tratamiento devolverá todos los datos y soportes de datos al Responsable del Tratamiento de forma gratuita. El Encargado del tratamiento correrá con los costes y otros gastos relacionados con la devolución de los datos.

5.3 El Responsable del tratamiento no puede exigir la supresión de los datos almacenados por el Encargado del tratamiento, siempre y cuando éste esté sujeto a obligaciones legales de conservación. En lugar de la supresión, se puede restringir el tratamiento de los datos, en la medida en que lo permita la legislación local/específica del país en materia de protección de datos. Esto se aplica en particular si, debido al método de almacenamiento específico, la eliminación no es posible o sólo es posible con un gasto desproporcionado.

ANEXO II – MEDIDAS TÉCNICAS Y ORGANIZATIVAS IMPLEMENTADAS POR CONTINENTAL

La Guía Continental sobre Política Corporativa en Materia de Seguridad de la Información (CISG, Corporate Policy Continental Information Security Guideline), define los requisitos mínimos de las medidas a adoptar en Continental para el tratamiento de la información. Dependiendo de la clasificación de la información, se implementan medidas que van más allá de los requisitos mínimos.

Los requisitos de la CISG se implementan en la Empresa sobre la base del Marco Estandarizado Corporativo en Materia de Seguridad de la Información (Corporate Standard Information Security Framework) y el correspondiente Sistema de Gestión de Seguridad de la Información (ISMS, Information Security Management System).

Política Corporativa en Materia de Seguridad de la Información (CISG)
Marco Estandarizado Corporativo en Materia de Seguridad de la Información
Anexo 1 - Sistema de Gestión de Seguridad de la Información (ISMS)
Anexo 2 – Papeles & Responsabilidades en Seguridad de la Información - Diagrama RACI

1.- CONTROL FÍSICO DE ACCESOS

Asegurar contra personas no autorizadas el acceso físico/el acceso a los sistemas de tratamiento con los que se lleva a cabo el mismo (por ejemplo, mediante la protección de objetos físicos: valla, personal de seguridad, cerraduras de puertas, torniquete, puerta con lector de tarjetas, vigilancia con cámaras, protección de objetos de la organización, autorización de acceso, registro de acceso).

Clasificación Corporativa Estándar de Zonas de Seguridad

Anexo 1 – Diagrama y Requisitos de Seguridad

Anexo 2 – Grabaciones Audio/Video

Tarjetas Estándar de Identificación Corporativas de Continental

Especificaciones de las medidas:

☒	Sistema de alarma
☒	Sistema de control automático de acceso
☐	Cerraduras con código
☐	Barreras de acceso biométrico
☐	Barreras de luz / sensores de movimiento
☒	Sistema de cerraduras manuales incluyendo normas sobre llaves (libro de llaves, realización de copias de llaves)
☒	Registro de visitantes
☒	Selección cuidadosa del personal de seguridad
☒	Tarjetas con chip / sistemas de cierre con transpondedor
☒	Videovigilancia de las puertas de acceso
☒	Cierres de seguridad
☒	Escaneado del personal por parte del vigilante de puerta / recepcionista
☒	Selección cuidadosa del personal de limpieza
☒	Obligación de portar tarjetas de identificación de empleado / visitante
☐	Otros:

2.- CONTROL DE ACCESO A LOS DATOS / CONTROL DE USUARIOS

Prevención del uso de sistemas de tratamiento automatizados por parte de terceros con equipos para la transmisión de datos (por ejemplo, salvapantallas con contraseña).

Manual Corporativo de Reglas de Contraseñas (M60.02.01)
Procedimiento Corporativo Estándar para la Identificación y Autorización de Usuarios de Sistemas de IT
Reglamento Corporativo Estándar de Seguridad de Cliente (sustituye al M60.02.10)
Regulación Corporativa Estándar de Entorno Móvil (sustituye a la M60.05.01)

Especificaciones de las medidas:

☒	Autenticación con usuario y contraseña (contraseñas asignadas según las normas sobre contraseñas vigentes)
☐	Uso de sistemas de detección de intrusiones
☒	Uso de software antivirus
☒	Uso de firewall
☒	Creación de perfiles de usuario
☒	Asignación de perfiles de usuario a los sistemas de IT
☒	Uso de tecnología VPN
☒	Encriptación de los medios de almacenamiento de datos móviles
☐	Encriptación de los medios de almacenamiento de datos en portátiles
☐	Uso de software de administración centralizada de teléfonos inteligentes (e.g. para el borrado desde el exterior de datos)
☐	Otros:

3.- CONTROL DEL USO DE LOS DATOS / CONTROL DE LOS MEDIOS DE ALMACENAMIENTO DE DATOS/CONTROL DE MEMORIA

Prevención de la lectura, copia, modificación o borrado no autorizados de soportes de almacenamiento de datos (control de soportes de almacenamiento de datos), prevención de la introducción no autorizada de información personal y del acceso no autorizado a la misma, modificación y borrado de información personal almacenada (control de almacenamiento de datos).

Asegurar que las partes autorizadas para el uso de un sistema de tratamiento automático solo tengan acceso a la información personal adecuada a su autorización de acceso (por ejemplo, mediante autorizaciones específicas, contraseñas, reglamentaciones relativas a la dimisión / salida o abandono de la empresa y para el traslado de empleados a otros departamentos) (control de uso de los datos).

Manual Corporativo de Reglas de Contraseñas (M60.02.01)
Procedimiento Corporativo Estándar para la Identificación y Autorización de Usuarios de Sistemas de IT
Clasificación Corporativa Estándar y Control de la Información
Manual de Directrices Corporativas de Seguridad para Bases de Datos - 3.4.6 Integridad de los Datos

Especificaciones para las medidas:

☒	Funciones y autorizaciones basadas en el principio de "necesidad de saber"
☒	Número de administradores reducido a lo esencial
☒	Registro de acceso a las aplicaciones, en especial la entrada, cambio y borrado de datos
☒	Borrado físico de los soportes de almacenamiento de datos antes de su reutilización
☒	Uso de destructoras o de proveedores de este servicio
☒	Administración de los derechos por administradores de sistemas identificados
☒	Directrices para contraseñas, incluyendo longitud y cambios
☒	Almacenamiento seguro de los soportes de almacenamiento de datos

☒	Destrucción adecuada de los soportes (DIN 32757)
☐	Registro de la destrucción
☐	Otros:

4.- CONTROL DE TRANSFERENCIAS / CONTROL DE TRANSPORTE

Asegurar que se protejan la confidencialidad y la integridad de los datos durante la transmisión de información personal y durante el transporte de soportes de almacenamiento de datos (por ejemplo, mediante el cifrado potente de las transmisiones de datos, uso de sobres cerrados en los *mailings*, cifrado en los soportes de almacenamiento de datos).

Clasificación Corporativa Estándar y Control de la Información

Especificaciones para las medidas:

☒	Establecimiento de líneas específicas o túneles VPN
☒	Transmisión de datos encriptados en Internet (como HTTPS, SFTP, etc.)
☒	Encriptación de emails (encriptación de transporte)
☒	Documentación de los receptores de datos y tiempos previstos de transmisión, o fechas límite de borrado de datos definidas
☐	En caso de transporte físico, selección cuidadosa del personal y vehículos de transporte
☐	Transmisión de datos de forma anónima o seudónima
☐	En caso de transporte físico: contenedores / embalajes seguros.
☐	Otros:

5.- CONTROL DE ENTRADAS / CONTROL DE TRANSMISIÓN

Garantizar el registro y la verificación posterior de los cambios (qué datos personales se han introducido o modificado, cuándo y por quién) en los sistemas de tratamiento automatizado (control de entrada). Garantizar la transferencia suficientemente segura y documentada (incluidos los métodos de transferencia seguros y adecuados utilizados) de los datos personales según la transferencia geográfica, física o electrónica a otros lugares (control de la transferencia).

Guía Continental sobre Información en materia de Seguridad de la Información (CISG) – 3.5.10.1 Auditoría de Entradas
Procedimiento Corporativo Estándar para Identificación y Autorización de Usuarios de Sistemas de IT
Clasificación Corporativa Estándar y Control de la Información
Manual de Directrices Corporativas de Seguridad para Bases de Datos - 3.4.6 Integridad de los Datos

Especificaciones para las medidas:

☒	Registro de entrada, cambio y borrado de datos
☒	Trazabilidad de entradas, cambios y borrados de datos por medio de nombres de usuario únicos (no grupos de usuarios)
☒	Asignación de derechos de entrada, cambio y borrado de datos con base en el concepto de autorización
☐	Creación de vista general que muestre qué datos pueden introducirse, cambiarse y borrarse y con qué aplicaciones
☐	Mantenimiento de formularios de los que se tomen los datos en el tratamiento automatizado de datos
☐	Otros:

6.- CONTROL DE DISPONIBILIDAD / RESTAURACION / FIABILIDAD / INTEGRIDAD DE LOS DATOS

Garantizar que los sistemas utilizados puedan restablecerse en caso de un mal funcionamiento (recuperabilidad). Asegurar que todas las funciones del sistema estén disponibles y que cualquier fallo de funcionamiento se notifica (fiabilidad). Asegurar que los datos personales almacenados no pueden dañarse por fallos de funcionamiento del sistema (integridad de los datos). Asegurar que los datos personales estén protegidos contra la destrucción o la pérdida accidental (control de disponibilidad), por ejemplo, mediante la implementación de procedimientos adecuados de copia de seguridad y de recuperación en caso de catástrofe.

Manual de Reglas Corporativas en materia de Backup y Recuperación de Datos (M60.02.08)

Especificaciones para las medidas:

☒	Suministro no interrumpible de corriente (UPS)
☒	Dispositivos de control de temperatura y humedad en las salas de servidores
☒	Sistemas de detección de fuego y de humos
☐	Alarmas contra accesos no autorizados a los cuartos de servidores
☒	Pruebas de recuperación de datos
☒	Almacenamiento de las copias de seguridad en lugares separados y seguros
☐	En zonas inundables, cuartos de servidores por encima del nivel de las inundaciones
☒	Aire acondicionado en los cuartos de servidores
☐	Regletas protegidas en cuartos de servidores
☒	Extintores en cuartos de servidores
☒	Creación de conceptos de copias de seguridad y recuperación de datos
☐	Creación de un plan de emergencias
☐	Otros:

7. CONTROL DE SEPARACIÓN / SEPARABILIDAD

Asegurar que los datos recopilados para finalidades diferentes puedan tratarse por separado (por ejemplo, mediante la separación lógica de datos de clientes, controles de acceso especializado - concepto de autorización-, separación de datos de pruebas y producción).

Directrices de Seguridad en la Información de Continental (CISG) – 3.5.1.4 Separación de los lugares de desarrollo, pruebas y de operaciones

Especificaciones para las medidas:

☒	Almacenamiento separado físicamente de los sistemas o de los medios de almacenamiento de datos
☐	Inclusión de atribuciones de objeto / campos de datos en los conjuntos de datos
☒	Establecimiento de derechos sobre las bases de datos
☐	Separación lógica de clientes (basada en el software)
☐	Para datos pseudonimizados, separación del fichero y almacenamiento en un sistema de IT seguro y aparte
☒	Separación de los sistemas de producción y de pruebas
☐	Otros:

ANEXO III - SUBCONTRATISTA

CONTINENTAL asegura un nivel adecuado de medidas de seguridad organizativas y técnicas en las entidades designadas por CONTINENTAL como entidades de apoyo con el fin de poder procesar los datos personales relevantes dentro de una estructura adecuada y segura (adecuación de CONTINENTAL).

Si se utilizan subcontratistas (por ejemplo, para alojamiento, provisión de espacio en un centro de datos, servicios en la nube, software operativo utilizado para tratar datos personales, etc.) para el tratamiento de datos personales, la implementación de las medidas técnicas y organizativas por parte del subcontratista en cuestión debe regularse mediante los contratos de tratamiento de datos correspondientes. El Subcontratista debe, con las garantías suficientes, asegurar al menos las medidas técnicas y organizativas acordadas con CONTINENTAL.

Para prevenir y/o evitar el acceso no autorizado y/o el intento de acceso no autorizado a los sistemas informáticos y las instalaciones de almacenamiento de CONTINENTAL, incluidos los datos almacenados allí, ya sea externos o internos o por Procesadores Sup, CONTINENTAL ha implementado medidas permanentes de control y monitoreo para sus sistemas de TI, incluido el control de acceso / monitoreo de acceso (24/7, 365 días) mediante la implementación de sistemas de detección de intrusos / firewalls / control de acceso de última generación, etc. Si se detecta un acceso no autorizado o un intento de acceso no autorizado, se terminará automáticamente sin demora. El equipo de servicio de Continental Automotive Technologies GmbH en Europa tiene el control exclusivo sobre estos sistemas de seguridad; se excluye el acceso a estos sistemas por parte de los Procesadores u otros.

Los siguientes Subprocesadores / Subcontratistas han sido contratados por CONTINENTAL:

	APLICABLE SOLO EN CASO DE QUE CONTINENTAL AUTOMOTIVE TECHNOLOGIES GMBH NO SEA LA PARTE CONTRATANTE DIRECTA DEL CLIENTE Y ACTÚE COMO SUBPROCESADOR DE <RSO/CONCESIONARIOS/SOCIOS NACIONALES> (APLICABLE PARA TODOS LOS PAÍSES / CLIENTES):
☐	**Continental Automotive Technologies GmbH**, Vahrenwalder Straße 9, 30165 Hannover, Germany (Soporte y mantenimiento)

	SUBPROCESADORES DE CONTINENTAL AUTOMOTIVE TECHNOLOGIES GMBH (APLICABLE PARA TODOS LOS PAÍSES / CLIENTES):
☒	**Com-a-tec GmbH**, Am Krebsgraben 15, 78048 Villingen-Schwenningen, Germany (Support Level 2)
☒	**Continental AG,** Hauptverwaltung, Vahrenwalder Straße 9, D-30165 Hannover Continental AG es el titular del contrato en relación con la prestación de servicios por parte del Subprocesador de Continental AG a Continental Automotive Technologies GmbH, tal como se enumeran a continuación por separado.
☒	**Continental Automotive Components (India) Private Limited** Technical Center India, Parque Tecnológico South Gate, Parcela No. 1, Área Industrial de Veerasandra, Hosur Main Road, Bangalore - 560 100, India. Continental Automotive Components India es una empresa del Grupo Continental que proporciona desarrollo, monitoreo y soporte en los servicios. **Nota:** Cualquier acceso por parte de Continental Automotive Components India a los datos (personales) del cliente de TIS-Web dentro del EEE está sujeto a las Normas Corporativas Vinculantes del Grupo Continental, que garantizan un nivel adecuado de protección de datos en el sentido del artículo 45 y siguientes del RGPD.

☒	**Continental Digital Services France SAS**, 1 avenue Paul Ourliac B.P.13704 31037 Toulouse, France Continental Digital Services France es una empresa del Grupo Continental que proporciona desarrollo, seguimiento y soporte de los servicios.
☒	**Eviden Germany GmbH** , Otto-Hahn Ring 6, 81739 München (Soporte y mantenimiento)
☒	**Google Ireland Limited,** Gordon House, Barrow Street, Dublin 4, Ireland (Proveedor de servicios en la nube, por ejemplo, Google Cloud Platform) **Nota:** Google se utilizará como "Subprocesador" para la prestación de servicios en la nube. En este sentido, CONTINENTAL se ha asegurado de que los datos originados dentro del Espacio Económico Europeo (EEE) solo se procesarán dentro del EEE, exentos según se acuerde lo contrario con el CLIENTE. Además, y como alternativa, se aplican a Google LLC las cláusulas contractuales estándar de la Comisión de la UE (según lo dispuesto en la Decisión de Ejecución (UE) 2021/914 de la Comisión de 04.06.2021), así como la nueva decisión de adecuación de la Comisión de la UE para el procesamiento de datos en los EE. UU. de 10.07.2023. Además, Continental ha implementado medidas de seguridad técnicas específicas como se describe anteriormente para evitar el acceso no autorizado a los datos, especialmente desde fuera del EEE..
☒	**kernel concepts GmbH**, Hauptstraße 16, 57074 Siegen (Proveedor de servicios de kernel, mejora, mantenimiento, etcétera, los datos se procesarán solo dentro del EEE)
☒	**Zonar Systems, Inc.**, 18200 Cascade Ave S, Seattle, WA 98188, USA, a Continental Group Company. Zonar Systems proporciona servicios de soporte, mantenimiento y desarrollo para los servicios web TIS de CONTINENTAL. **Nota:** Cualquier acceso por parte de Zonar Systems a los datos (personales) del cliente de TIS-Web dentro del EEE está sujeto a las Normas Corporativas Vinculantes del Grupo Continental, que garantizan un nivel adecuado de protección de datos en el sentido del artículo 45 y siguientes del RGPD. Además, Continental ha implementado medidas de seguridad técnicas específicas como se describe anteriormente para evitar el acceso no autorizado a los datos, especialmente desde fuera del EEE. En la medida en que Zonar Systems contrate más Subprocesadores para la prestación de sus servicios, dichos Subprocesadores se enumeran a continuación.

	SUBPROCESADOR DE CONTINENTAL AUTOMOTIVE TRADING FRANCE SAS (SOLO APLICABLE PARA FRANCIA / CLIENTES FRANCESES):
☒	**IMA TECHNOLOGIES**, 31 Route de Gachet 44300 Nantes, France (Support Hotline)

	SUBPROCESADOR DE CONTINENTAL AG **(APLICABLE PARA TODOS LOS PAÍSES / CLIENTES):**
☒	**SYZYGY Deutschland GmbH**, Im Atzelnest 3, 61352 Bad Homburg, Germany (Hosting-Services)
☒	**MongoDB Limited, Ireland,** 3 Shelbourne Buildings, Ballsbridge, Dublin 4, Ireland (Proveedor de servicios en la nube; los servicios en la nube están restringidos al EEE)

	SUBPROCESADORES DE ZONAR SYSTEMS, INC. **(APLICABLE PARA TODOS LOS PAÍSES / CLIENTES):**
☒	**Clearblade Inc**., 1701 Directors BLVD STE 250, Austin, TX 78744, USA (Solución para la gestión de conexiones de dispositivos telemáticos, Soporte / Mantenimiento) **Nota:** Continental se ha asegurado de que los servicios y datos originados dentro del EEE solo se procesen en servidores dentro del EEE. Además, y como alternativa, se han acordado con Clearblade las cláusulas contractuales tipo de la Comisión de la UE (véase la Decisión de Ejecución (UE) 2021/914 de la Comisión de 04.06.2021). Además, Continental ha implementado medidas de seguridad técnicas específicas como

	se describe anteriormente para evitar el acceso no autorizado a los datos, especialmente desde fuera del EEE.
☒	**DataDog Inc.,** New York Times Bldg, 620 8th Ave 45th Floor, New York, MA, USA (Servicios de soporte y disponibilidad) **Nota:** Data Dog solo procesa datos agregados seudonimizados; Además, y como alternativa, existen las cláusulas contractuales estándar de la Comisión de la UE (según lo dispuesto en la Decisión de Ejecución (UE) 2021/914 de la Comisión de 4.6.2021), así como la nueva decisión de adecuación de la Comisión de la UE para el procesamiento de datos en los Estados Unidos de 10.07.2023. Además, Continental ha implementado medidas de seguridad técnicas específicas como se describe anteriormente para evitar el acceso no autorizado a los datos, especialmente desde fuera del EEE.
☒	**OKTA Inc.**, 100 First Street, 6th Floor, San Francisco, CA 94105, USA (Gestión de acceso e identidad del cliente del proveedor de servicios (CIAM)) **Nota:** Continental se ha asegurado de que los servicios y datos originados dentro del EEE solo se procesarán en servidores dentro del EEE. Además, y como alternativa, las cláusulas contractuales estándar de la Comisión de la UE (véase la Decisión de Ejecución (UE) 2021/914 de la Comisión de 04.06.2021) se han acordado con Okta, así como la nueva decisión de adecuación de la Comisión de la UE para el procesamiento de datos en los Estados Unidos de 10.07.2023. Además, Continental ha implementado medidas de seguridad técnicas específicas como se describe anteriormente para evitar el acceso no autorizado a los datos, especialmente desde fuera del EEE.
☒	**MongoDB Limited, Ireland,** 3 Shelbourne Buildings, Ballsbridge, Dublin 4, Ireland (Proveedor de servicios en la nube; los servicios en la nube están restringidos al EEE)
☒	**pendo.io Inc.,** 150 Fayetteville St., Raleigh, NC 27601, USA; European Representative (Art. 27 GDPR): DP-Dock GmbH, Ballindamm 39, 20095 Hamburg (Servicios de soporte y desarrollo) **Nota:** pendo.io solo procesa datos agregados seudonimizados. Los datos solo se procesarán y almacenarán dentro del EEE. Además, y como alternativa, existen las cláusulas contractuales estándar de la Comisión de la UE (según lo dispuesto en la Decisión de Ejecución (UE) 2021/914 de la Comisión de 04.06.2021) y también se aplica la nueva decisión de adecuación de la Comisión de la UE para el procesamiento de datos en los Estados Unidos de 10.07.2023. Además, Continental ha implementado medidas de seguridad técnicas específicas como se describe anteriormente para evitar el acceso no autorizado a los datos, especialmente desde fuera del EEE.

Información general: Sus derechos como parte del Reglamento General Europeo de Protección de Datos permanecen sin cambios. Además, CONTINENTAL confirma que sus datos se almacenarán en centros de datos de la Unión Europea. CONTINENTAL utiliza los más altos estándares de seguridad (por ejemplo.ISO/DIN/https/encryption) y protege los datos personales durante la transmisión y el almacenamiento.

***