LOGISTIK IM FLUSS.

Contrato para la gestión de pedidos (según el art. 28 del RGPD)

entre

el **usuario** (como se establece en el contrato principal)

(en adelante «**cliente**»)

y

TB Digital Services GmbH, Oskar-Schlemmer-Str. 19-21, 80807 Múnich

(en adelante «**proveedor**»)
(cliente y proveedor serán en adelante una «**parte**» cada uno y juntos serán las «**partes**»).

Preámbulo

(A) Este contrato para la gestión de pedidos (en adelante «**contrato**») se aplica a todas las actividades en las que el proveedor esté en contacto con datos personales (como se define en el punto 1.5 más abajo) del cliente, de un tercer proveedor o de cualquier otro implicado en relación con la actividad descrita en el punto 2 del Marco general de condiciones para la utilización de la plataforma y, dado el caso, en los contratos individuales que se celebren para otros servicios dentro de este marco general (en adelante «**contrato principal**»).

(B) En este contrato, el cliente actúa como responsable y el proveedor, como encargado de gestionar los pedidos en el contexto de un contrato para la gestión de pedidos de conformidad con § 28 del RGPD (como se define más abajo).

Por este motivo, las partes acuerdan lo siguiente:

1 Definiciones e interpretación

1.1 El «**derecho europeo**» engloba el derecho aplicable de la Unión Europea, las leyes aplicables de los Estados miembro actuales, así como las leyes aplicables de todos los Estados que lleguen a ser miembros de la Unión Europea con posterioridad.

1.2 El «**derecho europeo de protección de datos**» es el derecho aplicable de la Unión Europea para el tratamiento de datos personales (especialmente el RGPD), las leyes aplicables de los Estados miembro actuales para el tratamiento de datos personales (especialmente la Ley federal alemana de protección de datos (BDSG) en su edición vigente), así como las leyes aplicables de todos los Estados que lleguen a ser miembros de la Unión Europea con posterioridad para el tratamiento de datos personales.

1.3 «**RGDP**» es el «REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO del 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)».

1.4 «**BDSG**» es la Ley federal alemana de protección de datos.

1.5 Los «**datos personales**» son aquellos cuyo significado se define en BDSG/RGDP.

2 Sujeto del tratamiento de datos / obligaciones del cliente

2.1 Este contrato regula las obligaciones de las partes en relación con el tratamiento de datos personales del cliente por parte del proveedor en el marco del contrato principal mencionado en el Anexo 1.

2.2 El objeto y la duración del tratamiento, el tipo y la finalidad del tratamiento, el tipo de datos personales, las categorías de las personas implicadas, así como las obligaciones y derechos del responsable, resultan del Anexo 1 del este contrato y de la descripción del servicio del contrato principal.

2.3 El cliente sigue siendo responsable en el marco del RGPD y debe garantizar la admisibilidad para tramitar los datos personales de las personas en cuestión (conductores y, dado el caso, otras personas). En relación a esto, el cliente acata especialmente su obligación de información completa y garantiza que el procesamiento de datos personales se basa en un fundamento jurídico sobre protección de datos (p. ej. llegar a un acuerdo laboral, la limitación del tratamiento con fines de la relación laboral).

3 Obligaciones del proveedor

3.1 El proveedor efectuará el tratamiento de los datos personales del cliente exclusivamente para los fines establecidos en el Anexo 1 y en el marco del contrato principal, así como por encargo y de conformidad con las instrucciones del cliente documentadas en el Anexo 1; según lo establecido en este contrato, el proveedor no efectuará el tratamiento de datos personales con ninguna otra finalidad. Esto no afecta al tratamiento de datos fuera de lo establecido en este contrato para fines propios según el punto 8.3.4 del contrato principal. No se realizarán copias ni duplicados de datos personales sin el conocimiento del cliente. Quedan excluidas de esto las copias de seguridad, siempre que sean necesarias para garantizar el correcto tratamiento de los datos, así como aquellos datos que sean necesarios para el cumplimiento de las obligaciones legales de conservación de datos.

3.2 Tras finalizar la prestación de los servicios de tratamiento, el proveedor tiene que, según su elección, entregar todos los datos personales del cliente al cliente y/o eliminarlos por su cuenta conforme a la protección de datos, siempre que esto no contravenga los plazos de conservación legales y que el proveedor no esté efectuando el tratamiento de los datos para fines propios fuera de lo establecido en este contrato según el punto 8.3.4 del contrato principal. Lo mismo se aplica al material de prueba y

desechable. La eliminación o entrega completas de los datos al cliente debe confirmarse por escrito e indicando la fecha si este así lo requiere.

3.3 Hasta donde alcancen las prestaciones, el proveedor apoyará al cliente para llevar a cabo los derechos en cuestión (información, rectificación, objeción, eliminación) según las instrucciones del cliente.

3.4 El proveedor confirmará, siempre que la ley lo exija, que ha solicitado un encargado de protección de datos (véase § 38 del art. 37 la ley BDSG).

3.5 El proveedor está obligado a poner inmediatamente en conocimiento del cliente el resultado de las verificaciones de las autoridades de supervisión de protección de datos, siempre que estas tengan relación con el tratamiento de los datos del cliente. En caso de constatarse alguna irregularidad, el proveedor la subsanará dentro de un plazo razonable y se lo comunicará al cliente.

3.6 El tratamiento de datos por parte del proveedor y de las empresas subcontratadas autorizadas por el cliente tendrá lugar exclusivamente en el ámbito de la República Federal de Alemania, de un Estado miembro de la Unión Europea o de un Estado firmante del Acuerdo sobre el Espacio Económico Europeo. Cualquier ampliación a otro país (en adelante «**país tercero**») requiere el consentimiento expreso previo del cliente y, además, solo puede efectuarse si se cumplen los requisitos especiales para la exportación de datos a un país tercero (véase Art. 40 y ss. del RGPD). Además, se necesitan las indicaciones del Anexo 1, así como adjuntarse documentación (contractual) adicional si fuera necesario.

3.7 El proveedor tiene que familiarizar a los empleados encargados de realizar los trabajos con las disposiciones fundamentales para ellos y hacer que traten los datos de forma confidencial (véase Art. 28 párrafo 3 b) de RGPD) así como garantizar a través de los pasos apropiados que todos los trabajadores procesen datos personales solo bajo las instrucciones del cliente.

3.8 El proveedor supervisará de forma periódica el cumplimiento de las disposiciones legales sobre protección de datos de este contrato y las instrucciones documentadas del cliente durante toda la vigencia del contrato. Los resultados de los controles deben ponerse a disposición del cliente si este así lo solicita, siempre que estos sean relevantes para el tratamiento de los datos del cliente. Las medidas para la supervisión se describen en un concepto de protección de datos que debe ponerse a disposición del cliente si este así lo requiere.

3.9 El proveedor tiene que asistir al cliente, atendiendo al tipo de tratamiento y en la medida de lo posible con medidas técnicas y organizativas adecuadas, a cumplir con su obligación de responder a las solicitudes para el ejercicio de los derechos mencionados en el capítulo III del RGPD por parte de las personas implicadas. El cliente está obligado a correr con los gastos que esto origine al proveedor.

3.10 El proveedor tiene que asistir al cliente, atendiendo al tipo de tratamiento y a la información puesta a su disposición, en el cumplimiento de las obligaciones mencionadas en los art. 32 a 36 del RGPD.

4 Medidas técnicas y organizativas para la seguridad de los datos

4.1 El proveedor adoptará medidas técnicas y organizativas razonables para la protección de datos (véase Art. 32 del RGPD). El proveedor está especialmente obligado a poner en práctica las medidas técnicas y organizativas acordadas en el Anexo 2 de este contrato. El proveedor adaptará estas medidas a las mejoras técnicas y organizativas durante la relación contractual sin que ello suponga un perjuicio del nivel de protección. Las modificaciones relevantes deberán acordarse por escrito.

4.2 El proveedor acreditará al cliente el cumplimiento real de las medidas técnicas y organizativas si este así lo solicita

4.3 El proveedor está obligado a efectuar una documentación adecuada del tratamiento de los datos mediante la que podrá acreditar al cliente el correcto tratamiento de los mismos. La acreditación también puede efectuarse mediante un procedimiento de certificación autorizado de acuerdo con el art. 42 del RGPD.

5 Proveedores subcontratados

5.1 Por la presente, al proveedor se le permite la incorporación de los proveedores subcontratados mencionados en el Anexo 1.

5.2 En general, de esta forma, se autoriza la incorporación de otros proveedores subcontratados. No obstante, el proveedor informará al cliente acerca de toda modificación prevista en lo que respecta a la incorporación o sustitución de proveedores subcontratados, el cliente podrá formular objeciones a las modificaciones que se prevean. En el marco de esta regulación, estas prestaciones de servicios no deben entenderse como las relaciones de subcontrata que consideran al proveedor en caso de terceros como servicio secundario para asistir en la ejecución del contrato. Entre estas se incluyen, p. ej., los servicios de telecomunicación, los equipos de limpieza, los comprobadores o la eliminación de soportes de datos. Sin embargo, el proveedor está obligado a cerrar acuerdos contractuales adecuados y de conformidad con la ley, así como a adoptar medidas de control, para garantizar la protección y la seguridad de los datos del cliente incluso en el caso de servicios secundarios que hayan encargado a una empresa externa.

5.3 Si el proveedor contrata a un subcontratado, este debe garantizar, con arreglo (i) a un contrato que debe celebrarse entre el subcontratado y el proveedor o (ii) a otro instrumento legal de conformidad con el derecho europeo de protección de datos, que el subcontratado está sometido a las mismas obligaciones de protección de datos a las que el proveedor se somete con este contrato. Además, el proveedor debe garantizar en particular que el subcontratado ofrezca garantías suficientes de que aplica las medidas técnicas y organizativas adecuadas que permiten efectuar el tratamiento de los datos personales conforme a los requerimientos del RGPD. Si este así lo solicita por escrito, el proveedor informará al

cliente sobre el contenido fundamental del contrato y la aplicación de las obligaciones relativas a la protección de datos dentro de la relación con la empresa subcontratada, en caso necesario, podrán examinarse los documentos relevantes del contrato. El proveedor puede ocultar las condiciones comerciales. El cliente está obligado a tratar la información obtenida de forma confidencial.

6 Derechos de control

6.1 El cliente tiene derecho a supervisar el cumplimiento de las obligaciones de este contrato por sí mismo (incluidas las instrucciones otorgadas) o a hacer que un tercero adecuado y designado por él las supervise.

6.2 El proveedor prestará al cliente la asistencia adecuada durante los controles. Especialmente, el cliente concederá acceso a las instalaciones de tratamiento de datos y proporcionará la información necesaria.

6.3 En el caso de que un control lleve a la conclusión de que el proveedor y/o el tratamiento de los datos no cumplen con las prescripciones de este contrato y/o del derecho europeo de protección de datos, el proveedor tomará todas las medidas correctivas necesarias para cumplir con las prescripciones de este contrato y/o con el derecho europeo de protección de datos.

6.4 El cliente asumirá los gastos que se deriven de realizar un control. El proveedor puede exigir al cliente los gastos que se deriven de un control realizado por este, siempre y cuando el cliente realice o encargue más de un control por año natural.

6.5 Los controles deben notificarse a tiempo al proveedor y no pueden perjudicar de forma desproporcionada el funcionamiento de la empresa del proveedor.

7 Deberes de advertencia

El proveedor informará inmediatamente al cliente cuando, en la opinión del proveedor, una instrucción dada por cliente conculque el derecho europeo de protección de datos. Una instrucción que se considere irregular de forma justificada no tiene que cumplirse, siempre que esta no haya sido modificada por el cliente o expresamente confirmada. El proveedor no está obligado a comprobar las instrucciones objetivamente en cuando a su legalidad.

En caso de determinarse errores o irregularidades del tratamiento de datos, o bien si se sospecha de una violación del derecho de protección de datos (en conjunto y en adelante «**incidente**»), el proveedor debe informar inmediata y adecuadamente al cliente. El cliente debe documentar el incidente incluidas todas las circunstancias del hecho, sus repercusiones y todas las medidas para la subsanación, así como debe transmitir de inmediato esta información documentada por escrito o en formato electrónico al cliente si este así lo requiere.

8 Responsabilidad y exenciones

8.1 El proveedor asumirá la responsabilidad por los daños que se deriven del dolo y/o la negligencia grave por parte del proveedor o de sus auxiliares ejecutivos. El proveedor asumirá la responsabilidad por los daños que resulten de la negligencia leve del proveedor o de sus auxiliares ejecutivos solo en caso de que estos violen una obligación fundamental. Las obligaciones fundamentales son obligaciones contractuales básicas que permiten la correcta viabilidad del contrato y en cuyo cumplimiento confía y debería confiar el cliente. En caso de una negligencia leve que viole tales obligaciones fundamentales, la responsabilidad del proveedor se limita a los daños típicos previsibles.

8.2 El cliente exime al proveedor de todas las reclamaciones de terceros (incluidas las personas afectadas y/o autoridades de protección de datos), así como de daños y gastos relacionados con una violación por parte del cliente de las disposiciones de este contrato y/o del derecho europeo de protección de datos. Esto no se aplica en caso de que el cliente no sea el culpable de la violación o cuando el proveedor haya contribuido a dicha violación.

9 Duración

La duración de este contrato se corresponde con la duración del contrato principal. Con la finalización del contrato principal por cualquier motivo, el presente contrato también finaliza automáticamente. Esto no afecta al derecho de rescisión por causa justa.

10 Otros

10.1 Los servicios del proveedor según este contrato se abonarán conforme al acuerdo de remuneración del contrato principal.

10.2 Si los datos personales del cliente se vieran amenazados en las instalaciones del proveedor debido a medidas por parte de terceros (como un embargo o confiscación), a causa de insolvencia, de procedimientos de liquidación o de cualquier otro evento similar, el proveedor debe informar inmediatamente al cliente.

10.3 Si alguna de las disposiciones de este contrato resultara ineficaz ahora o en el futuro, esto no afectará a la validez del resto de las disposiciones. En caso de resultar una cláusula ineficaz, las partes acordarán una regulación sustitutiva teniendo en cuenta la finalidad objetiva y económica del contrato.

10.4 En caso de que Gran Bretaña abandone la Unión Europea, el proveedor se compromete desde ahora a finalizar todos los acuerdos y llevar a cabo todas las actuaciones necesarias para que el tratamiento de datos objeto de este contrato en Gran Bretaña se desarrolle de forma admisible de conformidad con la legislación de protección de datos desde el momento de la salida de la Unión Europea. En tanto que en el momento de la salida no se cuente con ninguna decisión de adecuación positiva de la Comisión

Europea, desde la perspectiva actual se trata, especialmente, de las cláusulas de protección de datos estándar según el artículo 46, párrafo 2 c) para la transmisión de datos personales a encargados del tratamiento de datos que están establecidos en países terceros en los que no se garantiza un nivel de protección adecuado.

Si el proveedor no cumple con estas obligaciones, desde el momento de la salida de Gran Bretaña de la Unión Europea, el cliente tiene derecho a exigir del proveedor que una empresa asociada o una parte de la empresa con domicilio permanente en el área de la Unión Europea preste los servicios afectados sin que esto suponga un esfuerzo o gastos adicionales para el cliente.

10.5 Este contrato para la gestión de pedidos está disponible en 18 idiomas, aunque, en caso de divergencias, tiene prioridad la edición original en alemán.

10.6 El presente contrato se somete al derecho de la República Federal de Alemania con exclusión del derecho de compra de la ONU. La jurisdicción exclusiva será la de Múnich.

10.7 Los siguientes anexos forman parte del contrato:

Anexo 1: Descripción de la gestión de pedidos
Anexo 2: Medidas técnicas y organizativas

ANEXO 1: Descripción de la gestión de pedidos

1 Contrato principal

El contrato principal en el sentido del punto 2.1 de la parte principal del contrato es el «Marco general de condiciones para la utilización de la plataforma».

Cargo/partes: **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19-21, 80807 Múnich / **usuario**

2 Objeto y duración del contrato

El objeto del contrato se deduce del punto 1 (*Objeto*) y del punto 8 (*Datos del usuario y protección de datos*) del contrato principal. La duración del contrato se deduce del punto 7 (*Finalización del contrato, duración del contrato y derecho de rescisión*) del contrato principal.

3 Volumen, tipo y finalidad del tratamiento de datos/de las medidas para el tratamiento de datos

El volumen, el tipo y la finalidad del tratamiento de datos personales resulta del punto 8 del contrato principal.

Descripción más detallada del objeto del contrato respecto a volumen, tipo y finalidad:

Para que el proveedor pueda prestar los servicios ofrecidos (como se establece en el contrato principal), el proveedor debe recopilar los datos personales del cliente a través de vehículos conectados (Connected Vehicles) o dispositivos móviles (Mobile Devices) (dado el caso, de los datos personales transferidos de un proveedor tercero con el que el usuario ha acordado servicios de terceros) en la medida necesaria para la prestación de los servicios, así como transmitirlos a la plataforma del proveedor y almacenarlos allí. El proveedor realizará el tratamiento de los datos almacenados en la plataforma en la medida necesaria para la prestación de los servicios (como analizar y evaluar el comportamiento en carretera del conductor, así como el uso del vehículo conectado o del dispositivo móvil, mediante los datos personales y formular así ofertas a su medida basadas en ello, por ejemplo, formación de conductores, detalles de equipamiento, así como propuestas para mejorar la eficiencia). Una descripción más detallada de volumen, tipo y finalidad del contrato se deduce, especialmente, de los contratos individuales que deben celebrarse adicionalmente.

4 Grupo de implicados (categorías de las personas implicadas)

Los siguientes grupos de personas están implicados en la gestión de pedidos:

- **Conductores y otros empleados** (empleados de la misma empresa que el cliente), p. ej., empleados, personas en formación, aspirantes a un puesto, antiguos empleados*;*
- **Conductores** que no son empleados

- **Personas de contacto** de empresas de carga/descarga o de otros socios comerciales del cliente
- **Empleados del grupo** (empleados de otra empresa del grupo del cliente).

5 Tipo de datos personales

La gestión de pedidos abarca los siguientes tipos de datos personales:

- Nombre del conductor y número de identificación del conductor
- Número de identificación del vehículo
- Datos de ubicación
- Datos de tiempos de conducción y descanso
- Datos de comportamiento de marcha
- Datos de estado del vehículo conectado
- Datos de estado del semirremolque
- Datos de estado de la carrocería, elementos agregados, grupos y otros componentes del vehículo
- Dado el caso, datos de estado de los dispositivos IoT conectados
- Datos de estado de dispositivos móviles
- Datos de carga
- Datos de encargos
- Datos de contacto de personas de contacto de empresas de carga/descarga o de otros socios comerciales del cliente

6 Instrucciones documentadas

Por la presente, el cliente señala al proveedor que el tratamiento de los datos personales debe efectuarse como se describe en el punto 8 del contrato principal. Esto incluye especialmente el siguiente tratamiento de datos:

- Los datos personales se transmiten a través del vehículo conectado o del dispositivo móvil a la plataforma basada en la nube del proveedor y se almacenan allí.
- Según este contrato, solo se realizará el tratamiento de los datos personales cuando sea necesario para el cumplimiento del contrato principal, esto no afecta al punto 8.3.4 del contrato principal.
- El proveedor transmite los datos personales a un proveedor tercero (como se establece en el contrato principal), siempre y cuando dicha transmisión a un proveedor tercero sea necesaria para que este puede prestar sus servicios de terceros al cliente (como se establece en el contrato principal).
- El proveedor analiza y evalúa el comportamiento en carretera del conductor, así como el uso del vehículo conectado, mediante los datos personales y formula así ofertas a la medida del cliente basándose en ello, por ejemplo, formación de conductores, detalles de equipamiento, así como propuestas para mejorar la eficiencia.

7 Lugar del tratamiento de datos

- Alemania.
- Reino Unido, siempre que se traten datos para el alojamiento de datos TI y/o con fines de asistencia TI dentro de la Unión Europea, tienen que haberse celebrado los contratos correspondientes de gestión de pedidos.
- Siempre que el proveedor emplee subcontratados para el alojamiento de datos TI y/o con fines de asistencia TI fuera de la Unión Europea (véase al respecto el punto 8 del presente Anexo 1), la transmisión de datos personales se efectúa sobre la base de cláusulas de contrato estándar/cláusulas de protección de datos estándar acordadas entre el proveedor y el subcontratado para la transmisión de datos personales al encargado de gestionar los pedidos en países terceros según el Art. 46, párrafo 2 c) del RGPD.

8 Proveedores subcontratados

El proveedor emplea los siguientes proveedores subcontratados (que a su vez pueden emplear a otras empresas de subcontrata):

N.º	Proveedor subcontratado (empresa, dirección, persona de contacto)	Categorías de datos tratados	Pasos del tratamiento/finalidad de la gestión de pedidos por parte del subcontratado
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, EE. UU.	Todos los datos personales de la plataforma que tienen que ver con la parte de ventas (es decir, donde el cliente se registra en la plataforma y puede realizar pedidos)	Alojamiento de datos de la plataforma
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, EE. UU.	Todos los datos personales de la plataforma que tienen que ver con la parte de ventas (es decir, donde el cliente se registra en la plataforma y puede realizar pedidos)	Asistencia TI relacionada con la plataforma
3	Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 EE. UU. https://aws.amazon.com/de/compliance/contact/	Todos los demás datos personales de usuario que se trasmiten al proveedor a través del vehículo	Alojamiento de datos de la plataforma/asistencia TI relacionada con el alojamiento de datos de la plataforma
4	Dado el caso, en el futuro en lugar del n.º 3: Amazon Webservices (EU) Amazon Web Services, Inc. P.O. Box 81226 Seattle, WA 98108-1226 EE. UU. https://aws.amazon.com/de/compliance/contact/	Todos los demás datos personales de usuario que se trasmiten al proveedor a través del vehículo	Alojamiento de datos de la plataforma
5	MAN Service und Support GmbH Dachauer Straße 667	Todos los datos personales necesarios para procesar solicitudes de clientes en el contexto de los	1.er nivel de asistencia

	80995 Múnich Alemania	niveles de asistencia 1.º y 2.º	
6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 EE. UU.	Todos los datos personales necesarios para procesar la facturación/tramitación de pedidos	Alojamiento de datos de la plataforma (EU Tenant – Gehosted by Amazon Web Services (EU)), véase el punto 4
7	MAN Truck & Bus AG Dachauer Str. 667 80995 Múnich Alemania	Todos los demás datos personales de usuario que se trasmiten al proveedor a través del vehículo conectado y/o del dispositivo móvil	Alojamiento de datos de la plataforma
8	T-Systems International GmbH Hahnstraße 43 d 60528 Frankfurt am Main Alemania	Todos los demás datos personales de usuario que se trasmiten al proveedor a través del TMB1/2 de los vehículos	Alojamiento de datos de la plataforma
9	Scania AB Vagnmakarvägen 1 15187 Södertälje Suecia	Todos los demás datos personales de usuario que se trasmiten al proveedor a través del vehículo	Alojamiento de datos de la plataforma
10	Volkswagen Nutzfahrzeuge Mecklenheidestr. 74 30419 Hannover Alemania	Todos los demás datos personales de usuario que se trasmiten al proveedor a través del vehículo	Alojamiento de datos de la plataforma

ANEXO 2: Medidas técnicas y organizativas

Las medidas técnicas y organizativas que debe adoptar el proveedor para garantizar un nivel de protección proporcionado al riesgo se describen en el concepto de protección de datos de la plataforma RIO e incluyen en particular:

1. Anonimización

Siempre que los datos personales se utilicen con fines de evaluación que también sean factibles siendo los datos anónimos, se emplearán técnicas de anonimización. Además, primero se establece para cada campo de datos si este debe anonimizarse o no, dado que podría permitir la asociación a una persona concreta. Las claves de anonimización se guardan de modo seguro, «Data Safe», para lo que se configura la máxima limitación de acceso posible.

2. Encriptación

Los dispositivos móviles se comunican de forma encriptada con el terminal final mediante un certificado de dispositivo individual. Los datos se siguen transmitiendo encriptados dentro de la plataforma RIO («ubiquitous encryption» o «encryption everywhere»).

3. Garantía de confidencialidad

Se indica a todos los empleados su deber de tratar los datos de forma confidencial y se obligan por escrito a guardar el secreto informático.

Amazon Web Services (en lo que sigue AWS) pone a disposición la infraestructura TI utilizada basada en la nube (IaaS & PaaS). El operador de centros de datos AWS pone a disposición el control de acceso: los centros informáticos AWS más seguros utilizan medidas de supervisión electrónicas de última tecnología y sistemas de control de acceso de varios niveles. Los centros informáticos están cubiertos todo el día con personal de seguridad cualificado y el acceso se otorga de forma estricta según el principio de los derechos mínimos y exclusivamente con fines de administración del sistema.

El acceso a los componentes de hardware (clientes) en TB Digital Services GmbH tiene lugar según las medidas estándar adecuadas válidas en cada caso individual. Estas son, p. ej., limitaciones de acceso mediante instalaciones de aislamiento (centros neurálgicos), instalaciones de vigilancia por vídeo, alarmas y/o servicio de vigilancia, puertas aseguradas mecánica o electrónicamente, edificios blindados, derechos de acceso documentados (visitantes, personal externo) o áreas declaradas de seguridad.

Los controles de acceso abarcan medidas para la protección de dispositivos, redes y aplicaciones.

Como medidas para la protección de dispositivos en el vehículo se aplican diferentes soluciones: Los dispositivos móviles están montados de forma fija en el vehículo y disponen de una función de arranque seguro, es decir, no hay ninguna posibilidad de cargar e iniciar un sistema operativo externo. Los dispositivos móviles se

comunican de forma encriptada con el terminal final mediante un certificado de dispositivo individual. Los datos se siguen transmitiendo encriptados dentro de la plataforma RIO («ubiquitous encryption» o «encryption everywhere»). Los dispositivos finales se mantienen en un nivel de seguridad actual (administración de parches) gracias a la ejecución periódica de actualizaciones de seguridad.

Como medidas para la protección de redes también se aplican diferentes soluciones estándar: se han implementado requisitos adecuados (de la última tecnología) para las contraseñas (longitud, complejidad, duración de la validez, etc., de las contraseñas). La introducción errónea repetida de la combinación de identificación de usuario/contraseña resulta en un bloqueo (temporal) de la identificación de usuario. La red de la empresa está protegida mediante un cortafuegos frente a redes abiertas no seguras. Se ha establecido un proceso que garantiza la llegada periódica de actualizaciones de seguridad a los dispositivos móviles (proceso OTA). Para detectar y evitar los ataques a la red de la empresa (intranet) se emplean las tecnologías adecuadas (p. ej., sistemas de detección de intrusión). Se sensibiliza a los empleados periódicamente acerca de los peligros y riesgos que esto implica.

Como medidas para la protección de aplicaciones se adoptan algunas soluciones estándar:

Las aplicaciones relevantes están protegidas del acceso no autorizado mediante mecanismos de autentificación y autorización adecuados. Se han implementado requisitos adecuados (de la última tecnología) para las contraseñas (longitud, complejidad, duración de la validez, etc., de las contraseñas). En el caso de aplicaciones con una necesidad de protección mayor se emplean mecanismos de autentificación más estrictos (p. ej., Token, PKI). La introducción errónea repetida de la combinación de identificación de usuario/contraseña resulta en un bloqueo (temporal) de la identificación de usuario. Los datos empleados en un proceso relevante se encuentran encriptados en un soporte de datos de uso móvil. Se registran tanto los accesos efectuados como los intentos de acceso a las aplicaciones. Los archivos de registro generados se conservan durante un período adecuado (mín. 90 días) y se comprueban (aleatoriamente).

Los derechos de usuario (para entrada y acceso) se garantizan con diferentes medidas, a cuyo efecto estos están asignados por principio a una persona identificable. El otorgamiento de los derechos pertenece al ámbito del responsable de la plataforma y se comprueba periódicamente. La concesión de los derechos de entrada solo se efectúa según un proceso establecido y documentado. Las modificaciones de los derechos de entrada se efectúan siguiendo el principio de «cuatro ojos», dos personas revisan, y se documentan en un archivo de registro versionado.

Como medidas para el control de acceso se aplican diferentes soluciones: los derechos de acceso se establecen y documentan en el marco de un concepto de roles/derechos, así como se asignan de forma correspondiente a las necesidades condicionadas por las tareas del rol respectivo. Se han establecido roles/derechos específicos para administradores técnicos (que, en tanto que sea posible técnicamente, no permiten el acceso a datos personales). Se ha establecidos roles/derechos para la asistencia especializada (que no incluyen derechos de administración técnica).

La definición y asignación de roles/derechos, en tanto que sea técnica y organizativamente posible, no las realiza la misma persona y se efectúan siguiendo un proceso (de autorización) con archivado seguro para la revisión posterior, así como existe una limitación temporal. Los accesos directos a la base de datos eludiendo el concepto de roles/derechos solo son posibles para los administradores de la base de datos autorizados. Existe una regulación para el empleo de soportes de datos privados o el empleo de soportes de datos privados está prohibido. Existen regulaciones vinculantes respecto al acceso a los datos en caso de trabajos de mantenimiento externos, trabajos de mantenimiento remotos y teletrabajo. La destrucción/eliminación de documentos y soportes de datos (p. ej., trituradora, contenedor para documentos confidenciales) la lleva a cabo una empresa de eliminación de desechos fiable.

El concepto de roles/derechos se adapta periódicamente a las estructuras organizativas del trabajo que se modifican (p. ej., nuevos roles) y los roles/derechos asignados se comprueban con regularidad (p. ej., por parte de los superiores), así como, dado el caso, se ajustan o suprimen. Tiene lugar un control centralizado regular respecto a los perfiles estándar asignados. Los accesos que suponen modificaciones (escritura, borrado) se registran y los archivos de registro generados se conservan durante un período adecuado (mín. 90 días) y se comprueban (aleatoriamente).

Como medidas para la protección de la transmisión se adoptan diferentes soluciones estándar:

las personas encargadas de la transmisión se familiarizan previamente con las medidas de seguridad que deben adoptarse. El grupo destinatario se determina con anterioridad, de manera que sea posible realizar el control correspondiente (autentificación). El proceso completo de transmisión de datos está establecido y documentado y su realización concreta se registra y documenta (p. ej., confirmación de recepción, justificante). Las personas encargadas de la transmisión realizan previamente una comprobación de plausibilidad, integridad y corrección.

Antes de realizar una transmisión concreta de datos se comprueba la dirección del destinatario (p. ej., dirección de correo electrónico). La transmisión de datos a través de internet se realiza encriptada (p. ej., encriptación de archivos). La integridad de los datos transmitidos, en tanto que sea técnicamente posible, se garantiza utilizando un proceso de firma (firma digital). Las confirmaciones de recepción electrónicas se archivan en el formato adecuado. Las transmisiones no deseadas de datos a través de internet se impiden con las tecnologías adecuadas (p. ej., proxy, cortafuegos).

Además, como medidas para la protección de la demanda de separación se adoptan las siguientes soluciones estándar:

existen regulaciones vinculantes respecto a la finalidad reservada del tratamiento para cumplir con la demanda de separación. Los datos recopilados para determinados fines se almacenan separados de los datos obtenidos para otros fines. Los sistemas TI empleados permiten el almacenamiento separado de datos (mediante tenencia múltiple o conceptos de acceso). Se efectúa una separación de los datos en los sistemas de prueba y productivos. En el caso de datos seudonimizados, el puente de encriptación que permite la identificación de la

persona se almacena y conserva por separado. En el caso de tratamiento de datos por cuenta de terceros o de transmisión de funciones, en las instalaciones del proveedor, se efectúa un tratamiento separado de los datos de diferentes clientes. Los conceptos de roles/derechos permiten, gracias a su estructura, la separación lógica de los datos tratados.

4. Garantía de integridad

Como medidas para realizar el registro de introducción se adoptan diferentes soluciones estándar:

se registran las modificaciones de los derechos de acceso, así como todas las actividades del administrador. Se registran los accesos de escritura (introducciones, modificaciones, eliminaciones) y las modificaciones en los campos de datos (p. ej., contenido del nuevo registro de datos o del modificado). Se efectúa la documentación de las transmisiones (p. ej., descargas) y de los registros.

La documentación de registro utilizada se documenta y archiva para la trazabilidad de las introducciones. El registro incluye fecha, hora, usuario, tipo de actividad, programa de aplicación y número del registro de datos. Se documentan los ajustes de registro.

Solo se otorga acceso de lectura a los archivos de registro. El grupo con derechos de acceso a los archivos de registro está estrictamente limitado (p. ej., al administrador, a los encargados de protección de datos, al revisor). Los archivos de registro se conservan durante un período establecido (p. ej., 1 año) y se eliminan conforme a la protección de datos. Los archivos de registro se evalúan periódicamente de forma automática. Las evaluaciones de los archivos de registro se elaboran de forma seudonimizada siempre que sea posible.

5. Garantía de disponibilidad

La arquitectura dentro de la plataforma AWS está garantizada *per se* contra la pérdida de datos mediante mecanismos de replicación internos. Además, como medidas para la protección perimetral se adoptan las siguientes soluciones estándar de AWS:

se adoptan medidas de protección contra incendios (p. ej., puertas cortafuegos, detectores de humo, barreras cortafuegos, prohibición de fumar). Los equipos informáticos están protegidos contra inundaciones (p. ej., salas de equipos informáticos en el 1.er piso con detectores de agua). Se toman medidas contra sacudidas (p. ej., salas de equipos informáticos cerca de autopistas, andenes de tren, salas de maquinaria). Los equipos informáticos están protegidos frente a campos electromagnéticos (p. ej., placas de acero en las paredes exteriores). Se adoptan medidas contra vandalismo y robo (consúltese el control de acceso). Los equipos informáticos se encuentran en espacios climatizados (la temperatura y la humedad del aire se regulan mediante aire acondicionado). Los equipos informáticos están asegurados mediante una protección contra sobretensión contra picos de sobretensión. Se toman medidas para garantizar una alimentación eléctrica libre de perturbaciones y continuada (p. ej., sistemas de alimentación ininterrumpida, generadores de emergencia).

Las existencias de datos se aseguran regularmente en forma de copias «backup» dentro de la plataforma AWS. El concepto de «backup» se documenta, así como se comprueba y actualiza regularmente. Los medios para el «backup» están protegidos del acceso no autorizado. Los programas de «backup» utilizados corresponden al estándar de calidad actual y se actualizan periódicamente al respecto. Se ha dispuesto un centro informático redundante (alejado del lugar del tratamiento de datos) que puede continuar con el tratamiento de datos en caso de catástrofe. Las diferentes medidas para el control de disponibilidad se documentan en un plan de gestión de emergencias de AWS.

Antes de asignar un encargo de tratamiento de datos, se somete al proveedor a una comprobación exhaustiva y siguiendo los criterios establecidos (medidas técnicas y organizativas). Para ello se requiere especialmente una declaración detallada de todas las medidas de protección de datos técnicas y organizativas adoptadas por parte del proveedor (responder al catálogo de preguntas o concepto de protección de datos). En función del volumen y la sensibilidad de los datos tratados, esta comprobación también se efectúa, dado el caso, *in situ* en las instalaciones del proveedor. Las certificaciones adecuadas (p. ej., ISO 27001) se tienen en cuenta al seleccionar los proveedores. La determinación de la idoneidad del proveedor se documenta de forma correcta y comprensible.

Como fundamento de las relaciones contractuales, se celebra un contrato para la gestión de pedidos entre el cliente y el proveedor. Este establece detalladamente y por escrito las competencias y responsabilidades, así como las obligaciones, de ambas partes. En caso de que un proveedor de servicios encargado tenga su domicilio fuera de la UE o del EEE, se aplicarán las cláusulas contractuales estándar de la UE. Se establece de forma vinculante por contrato, que el proveedor solo puede realizar el tratamiento de datos en el marco de las instrucciones cliente. El proveedor se obliga a advertir inmediatamente al cliente cuando, en su opinión, alguna de las instrucciones de este conculque las prescripciones de protección de datos. Para satisfacer los derechos de los implicados, en el contrato para la gestión de pedidos se acuerda que el proveedor debe asistir al cliente de forma adecuada, siempre que esto sea necesario, p. ej., en caso de que la comunicación de la información a los implicados sea necesaria.

Durante el desarrollo posterior del tratamiento de datos por cuenta de terceros, el cliente controla los resultados del trabajo del proveedor en cuanto a forma y contenido. El cumplimiento de las medidas técnicas y organizativas adoptadas por el proveedor se comprueba periódicamente. Para ello se utilizan preferentemente la presentación de datos de prueba actuales o de certificaciones adecuadas, o bien del justificante de auditorías de seguridad TI o de protección de datos. Siempre que se emplee un proveedor subcontratado, está establecido por contrato que este se supervisará correspondientemente.

6. Garantía de capacidad de los sistemas

La infraestructura basada en la nube de AWS se ha creado como uno de los entornos informáticos más flexibles y seguros basados en la nube. Se ha concebido para alcanzar la mejor disponibilidad en la separación completa del cliente. Proporciona una plataforma extremadamente ampliable y de funcionamiento muy seguro que permite al cliente aprovechar en todo el mundo las aplicaciones y contenidos que necesite de forma rápida y

segura. Los servicios de AWS son independientes del contenido, en tanto que se ofrece a todos los clientes el mismo nivel de seguridad, independientemente del tipo de contenidos o de la región geográfica en la que se almacenan dichos contenidos.

Los centros informáticos AWS más seguros de categoría mundial utilizan medidas de supervisión electrónicas de última tecnología y sistemas de control de acceso de varios niveles. Los centros informáticos están cubiertos todo el día con personal de seguridad cualificado y el acceso se otorga de forma estricta según el principio de los derechos mínimos y exclusivamente con fines de administración del sistema.

7. Proceso para restablecer la disponibilidad de datos personales tras un accidente físico o técnico

Los centros informáticos de AWS se establecen en clústeres en diferentes regiones del mundo. Todos los centros informáticos están online y atienden a clientes, ningún centro informático está desconectado. En caso de fallo, los procesos automáticos desplazan el tráfico de datos del cliente lejos de las áreas afectadas. Las aplicaciones clave se ponen a disposición en una configuración N+1, de forma que, en caso de un fallo del centro informático, hay disponible suficiente capacidad para distribuir el tráfico de datos en función de la carga a las ubicaciones restantes.

AWS ofrece la flexibilidad de ubicar instancias y de almacenar datos dentro de varias regiones geográficas, así como también de almacenarlos dentro de las diferentes regiones a través de varias zonas de disponibilidad. Cada zona de disponibilidad se ha desarrollado como zona de fallos independiente. Esto significa que las zonas de disponibilidad dentro de una típica región urbana están distribuidas y se encuentran, p. ej., en áreas con bajo riesgo de inundación (en función de la región existen diferentes categorizaciones de las zonas de inundación). Adicionalmente a una alimentación eléctrica autónoma sin interrupciones y a los generadores de emergencia *in situ*, todas las zonas de disponibilidad se alimentan a través de diferentes redes eléctricas de proveedores de electricidad independientes con el fin de minimizar las zonas de fallo individual. Todas las zonas de disponibilidad están conectadas de forma redundante con varios proveedores de tránsito Tier 1.

El equipo de Amazon para la administración de incidentes aplica procesos de diagnóstico de uso comercial para impulsar la subsanación de incidentes críticos para la empresa. El personal operativo trabaja continuamente 24 horas al día, 7 días a la semana y 365 días al año para identificar los casos de avería y gestionar sus repercusiones y subsanación.

8. Procedimiento de la comprobación regular, evaluación de la eficacia de las medidas técnicas y organizativas

Las directivas e instrucciones disponibles en la empresa, así como los estándares implementados para la seguridad de la información, también se aplican en relación con la introducción y funcionamiento de la plataforma RIO. Están disponibles las funciones operativas para la protección de datos (encargado de protección de datos y jefe de seguridad de la información). Los empleados se obligan a guardar el secreto

informático y a informarse sobre las medidas de seguridad de los datos y de seguridad TI mediante folletos, panfletos, indicaciones de la intranet, etc.

Los procesos internos se comprueban en relación con el cumplimiento de las medidas técnicas y organizativas para la seguridad de los datos mediante revisión, la seguridad de la información y la protección de datos.

Los procesos de tratamiento y las medidas de seguridad de los datos se documentan en un directorio con las actividades de tratamiento de datos. Se realiza una comprobación periódicamente (interna y externa) en cuanto a la eficacia de las medidas.