Contrato para o tratamento de encomendas (segundo artigo 28.º do RG-PD)

celebrado entre

o **utilizador** (conforme definido no contrato principal)

(a seguir designado por «**entidade adjudicante**»)

e

a **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19 - 21, 80807 München

(a seguir designada por «**entidade adjudicatária**»)
(a entidade adjudicante e a entidade adjudicatária são a seguir designadas, individualmente, por «**parte**» e, conjuntamente, por «**partes**»).

Preâmbulo

(A) O presente contrato para o tratamento de encomendas (a seguir designado por «**contrato**») é aplicável a todas as atividades em que a entidade adjudicatária tenha contacto com dados pessoais (conforme definidos no n.º 1.5 abaixo) da entidade adjudicante, de terceiros ou de outros titulares de dados no âmbito da atividade descrita no n.º 2 decorrentes das condições gerais de utilização da plataforma e de eventuais contratos individuais respeitantes a outros serviços celebrados ao abrigo das mesmas (a seguir designadas por «**contrato principal**»).

(B) No âmbito do presente contrato, a entidade adjudicante age na qualidade de responsável e a entidade adjudicatária na qualidade de subcontratante para efeitos de tratamento de encomendas nos termos do artigo 28.º do RG-PD (como definido em baixo).

Posto isto, as partes acordam no seguinte:

1 Definições e interpretações

1.1 Entende-se por «**direito europeu**» o direito aplicável da União Europeia, as leis aplicáveis dos atuais Estados-Membros da União Europeia, bem como as leis aplicáveis de qualquer Estado que venha a aderir, futuramente, à União Europeia.

1.2 Entende-se por «**direito europeu de proteção de dados**» o direito aplicável da União Europeia em matéria de tratamento de dados pessoais (designadamente, o RG-PD), as leis aplicáveis em matéria de tratamento de dados pessoais dos atuais Estados-Membros da União Europeia (designadamente a BDSG, na versão em vigor), bem como as leis aplicáveis em matéria de tratamento de dados pessoais de qualquer Estado que venha a aderir, futuramente, à União Europeia.

1.3 Entende-se por «**RG-PD**» o «REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)».

1.4 Entende-se por «**BDSG**» a lei federal alemã relativa à proteção de dados.

1.5 O conceito de «**dados pessoais**» tem o significado que lhe é atribuído na BDSG/no RG-PD.

2 Objeto do tratamento de dados / Obrigações da entidade adjudicante

2.1 O presente contrato rege as obrigações das partes no contexto do tratamento de dados pessoais da entidade adjudicante pela entidade adjudicatária ao abrigo do contrato principal referido no Anexo 1.

2.2 O objeto e a duração do tratamento, a natureza e as finalidades do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento constam do Anexo 1 do presente contrato e do caderno de encargos do contrato principal.

2.3 A entidade adjudicante é responsável no âmbito do RG-PD e garante a admissibilidade do tratamento de dados pessoais dos titulares (motoristas e possivelmente outras pessoas). Em particular, a entidade adjudicante cumpre com a sua obrigação extensiva de fornecer informações e assegura que o tratamento de dados pessoais se baseia numa base legal de proteção de dados (por exemplo, a celebração de um acordo de empresa, restrições de tratamento motivadas pela relação laboral).

3 Obrigações da entidade adjudicatária

3.1 A entidade adjudicatária procederá ao tratamento dos dados pessoais da entidade adjudicante exclusivamente para as finalidades referidas no Anexo 1 e no âmbito do contrato principal, agindo por conta da entidade adjudicante e de acordo com as suas instruções documentadas no Anexo 1. A entidade adjudicatária não tratará os dados pessoais ao abrigo do presente contrato para quaisquer outras finalidades, sem prejuízo do tratamento para uso próprio fora do âmbito de aplicação do presente contrato, nos termos do n.º 8.3.4 do contrato principal. A entidade adjudicatária não produzirá cópias ou duplicados dos dados pessoais sem o conhecimento da entidade adjudicante. Excluem-se as cópias de segurança, desde que sejam necessárias para garantir o correto tratamento dos dados, bem como os dados necessários para o cumprimento das obrigações legais de conservação de dados.

3.2 Uma vez concluída a prestação dos serviços de tratamento, a entidade adjudicatária deverá, consoante a escolha da entidade adjudicante, entregar-lhe todos os dados pessoais a ela respeitantes e/ou apagá-los salvaguardando a proteção dos dados, a não ser que a tal obstem os prazos legais de conservação de dados ou que a entidade adjudicatária proceda ao tratamento dos dados para uso próprio fora do âmbito de aplicação do presente contrato, nos termos do n.º 8.3.4 do contrato principal. O mesmo se

aplica ao material de teste e refugo. A pedido da entidade adjudicante, a entidade adjudicatária confirmar-lhe-á, por escrito e com indicação da data, que apagou por completo ou entregou todos os dados à entidade adjudicante.

3.3 Desde que abrangido pelo âmbito dos serviços, a entidade adjudicatária apoia entidade adjudicante no cumprimento dos direitos do titular dos dados (informação, correção, oposição, eliminação) de acordo com as instruções da entidade adjudicante.

3.4 A entidade adjudicatária confirma que – caso seja obrigatório por lei – designou um encarregado da proteção de dados (cf. § 38 da BDSG artigo 37.º do RG-PD).

3.5 A entidade adjudicatária compromete-se a comunicar, sem demora, à entidade adjudicante o resultado de auditorias realizadas pelas autoridades de controlo da proteção de dados, na medida em que estas digam respeito aos dados da entidade adjudicante. Caso sejam detetadas eventuais não conformidades, a entidade adjudicatária corrigi-las-á dentro de um prazo razoável e informará a entidade adjudicante a este respeito.

3.6 O tratamento dos dados pela entidade adjudicatária e por subcontratantes aprovados pela entidade adjudicante é realizado exclusivamente no território da República Federal da Alemanha, dos Estados-Membros da União Europeia ou dos países signatários do Acordo sobre o Espaço Económico Europeu. Qualquer transferência para outro país (a seguir designado por «**país terceiro**») carece do prévio consentimento expresso da entidade adjudicante, além de só ser permitida se estiveram reunidas as condições especiais para a exportação de dados para países terceiros (cf. artigo 40.º ss. do RG-DP). Para esse efeito, é necessário prestar as informações referidas no Anexo 1 e, eventualmente, juntar outros documentos (contratuais).

3.7 A entidade adjudicatária dará a conhecer aos colaboradores contratados para o tratamento dos dados as disposições relevantes em matéria de proteção de dados e exigirá que assumam um compromisso de confidencialidade (cf. artigo 28.º do RG-PD n.º 3 alínea b)), assim como garantirá, através de medidas apropriadas, que esses colaboradores processam dados pessoais apenas quando instruídos pela entidade adjudicante.

3.8 Durante todo o período de vigência do contrato, a entidade adjudicatária procederá regularmente à supervisão do cumprimento das disposições legais em matéria de proteção de dados estabelecidas no presente contrato e das instruções documentadas da entidade adjudicante. Os resultados dos controlos devem ser apresentados à entidade adjudicante, mediante pedido, desde que sejam relevantes para o tratamento dos dados da entidade adjudicante. As medidas de supervisão encontram-se descritas num esquema de proteção de dados, que deve ser apresentado à entidade adjudicante, mediante pedido.

3.9 A entidade adjudicatária prestará assistência à entidade adjudicante, tendo em conta a natureza do tratamento e, na medida do possível, através de medidas técnicas e organizativas adequadas, a fim de

permitir que esta cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos seus direitos previstos no capítulo III do RG-PD. A entidade adjudicante suportará as despesas incorridas pela entidade adjudicatária neste contexto.

3.10 A entidade adjudicatária prestará assistência à entidade adjudicante no sentido de assegurar o cumprimento das obrigações previstas nos artigos 32.º a 36.º do RG-PD, tendo em conta a natureza do tratamento e a informação ao seu dispor.

4 Medidas técnicas e organizativas para garantir a segurança dos dados

4.1 A entidade adjudicatária adotará medidas técnicas e organizativas adequadas para assegurar a proteção de dados (cf. artigo 32.º do RG-PD). Compete, em especial, à entidade adjudicatária aplicar as medidas técnicas e organizativas acordadas contratualmente no Anexo 2 do presente contrato. Ao longo da vigência do contrato, a entidade adjudicatária adaptará estas medidas à evolução técnica e organizativa, sem, no entanto, reduzir o nível de proteção. As alterações substanciais devem ser acordadas por escrito.

4.2 A pedido da entidade adjudicante, a entidade adjudicatária demonstrar-lhe-á o cumprimento efetivo das medidas técnicas e organizativas.

4.3 A entidade adjudicatária está obrigada a manter um registo adequado do tratamento dos dados, com base no qual a entidade adjudicante possa comprovar que o tratamento dos dados é realizado corretamente. Essa prova também pode ser prestada mediante um procedimento de certificação aprovado nos termos do artigo 42.º do RG-PD.

5 Subcontratantes

5.1 A entidade adjudicatária fica, pela presente, autorizada a recorrer aos subcontratantes referidos no Anexo 1.

5.2 É concedida uma autorização geral de contratação de outros subcontratantes. A entidade adjudicatária informará, no entanto, a entidade adjudicante de quaisquer alterações pretendidas quanto ao aumento do número ou à substituição de outros subcontratantes; a entidade adjudicante pode opor-se a tais alterações. Para efeitos da presente disposição, não serão consideradas relações de subcontratação as prestações de serviços de terceiros a que a entidade adjudicatária recorre como serviço acessório para assegurar a execução do contrato. Estes incluem, p. ex., serviços de telecomunicações, limpeza, auditoria ou eliminação de suportes de dados. Ainda assim, mesmo tratando-se de serviços acessórios prestados por terceiros, a entidade adjudicatária tem a obrigação de celebrar acordos contratuais adequados e conformes com a lei e de adotar medidas de controlo para garantir a proteção e segurança dos dados da entidade adjudicante.

5.3 Se a entidade adjudicatária contratar um subcontratante, deverá garantir que lhe são impostas, (i) por contrato a celebrar entre o subcontratante e a entidade adjudicatária ou (ii) por outro ato normativo ao abrigo do direito europeu de proteção de dados, as mesmas obrigações em matéria de proteção de dados a que a entidade adjudicatária está sujeita ao abrigo do presente contrato. A entidade adjudicatária deverá assegurar, em particular, que o subcontratante apresente garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento dos dados pessoais seja conforme com os requisitos do RG-PD. Mediante pedido escrito da entidade adjudicante, a entidade adjudicatária prestar-lhe-á informações sobre o teor essencial do contrato e o cumprimento das obrigações relevantes em matéria de proteção de dados no âmbito da relação de subcontratação, se necessário, mediante consulta da documentação contratual relevante. A entidade adjudicatária poderá ocultar as condições comerciais. A entidade adjudicante está obrigada a manter sigilo sobre as informações obtidas.

6 Direitos de controlo

6.1 A entidade adjudicante tem o direito de controlar ela própria ou de designar uma entidade terceira competente para controlar o cumprimento das obrigações emergentes do presente contrato (incluindo as instruções dadas).

6.2 A entidade adjudicatária prestará o devido apoio à entidade adjudicante durante os controlos. A entidade adjudicatária facultará, designadamente, acesso aos sistemas de processamento de dados e prestará as informações necessárias.

6.3 Caso resulte de um controlo que a entidade adjudicatária e/ou o tratamento não estão em conformidade com as disposições do presente contrato e/ou do direito europeu de proteção de dados, a entidade adjudicatária tomará todas as ações corretivas necessárias para garantir o cumprimento das disposições do presente contrato e/ou do direito europeu de proteção de dados.

6.4 Os custos resultantes da realização de um controlo serão suportados pela própria entidade adjudicante. A entidade adjudicatária poderá exigir à entidade adjudicante que suporte os custos que lhe sejam causados por um controlo realizado pela entidade adjudicante, nos casos em que a entidade adjudicante realize ou mande realizar mais do que um controlo por ano civil.

6.5 Os controlos a realizar nas instalações da entidade adjudicatária devem ser anunciados atempadamente e não devem prejudicar demasiado as operações comerciais da entidade adjudicatária.

7 Deveres de informação

A entidade adjudicatária informará, de imediato, a entidade adjudicante se considerar que uma instrução dada pela entidade adjudicante viola o direito europeu de proteção de dados. A instrução

legitimamente contestada não precisa de ser cumprida enquanto não for alterada ou expressamente confirmada pela entidade adjudicante. A entidade adjudicatária não está obrigada a submeter as instruções a um exame de direito substantivo.

A entidade adjudicatária informará de forma adequada e imediata a entidade adjudicante no caso de serem detetados erros ou irregularidades no tratamento dos dados ou em caso de suspeita de violação da privacidade (a seguir conjuntamente designados por «**incidente**»). A entidade adjudicante terá de documentar o incidente, incluindo todos os factos, as respetivas consequências e todas as medidas corretivas adotadas, e enviar de imediato à entidade adjudicante, mediante pedido, estas informações documentadas por escrito ou por via eletrónica.

8 Responsabilidade e exoneração de responsabilidade

8.1 A entidade adjudicatária responde por danos causados por dolo e/ou negligência grosseira da entidade adjudicatária ou dos seus agentes. A entidade adjudicatária só responde por danos causados por negligência simples da entidade adjudicatária ou dos seus agentes, no caso de violação de uma obrigação fundamental. Consideram-se obrigações fundamentais as obrigações contratuais que são essenciais à correta execução do contrato e cujo cumprimento a entidade adjudicante tomou e podia tomar por garantido. Se a violação de tais obrigações fundamentais se dever a negligência simples, a responsabilidade da entidade adjudicatária ficará limitada aos danos normalmente previsíveis.

8.2 A entidade adjudicante exonera a entidade adjudicatária de todos os direitos reclamados por terceiros (incluindo titulares de dados e/ou autoridades de proteção de dados), danos e despesas, que sejam decorrentes de uma violação, por parte da entidade adjudicante, das disposições do presente contrato e/ou do direito europeu de proteção de dados; esta exoneração de responsabilidade não se aplica se a violação não for imputável à entidade adjudicante ou se a entidade adjudicatária tiver contribuído para essa violação.

9 Duração do contrato

A duração do presente contrato corresponde à duração do contrato principal. O presente contrato cessa automaticamente com o termo do contrato principal, qualquer que seja a causa. Tal não prejudica o direito de rescisão do contrato por justa causa.

10 Outras disposições

10.1 Os serviços prestados pela entidade adjudicatária ao abrigo do presente contrato são remunerados de acordo com o regime de remuneração acordado no contrato principal.

10.2 A entidade adjudicatária informará, de imediato, a entidade adjudicante na eventualidade de os dados pessoais desta última correrem perigo devido a medidas de terceiros (p. ex., penhora ou apreensão), insolvência ou processo de concordata ou devido a acontecimentos similares.

10.3 A eventual nulidade presente ou futura de alguma das disposições do presente contrato não afetará a validade das restantes disposições. Em caso de nulidade de uma cláusula, as partes adotarão uma cláusula de substituição inspirada no objetivo material e económico do contrato.

10.4 Caso a Grã-Bretanha venha a sair da União Europeia, a entidade adjudicatária compromete-se, desde já, a celebrar todos os acordos e a realizar todos os atos que se revelem necessários para assegurar que, a partir da data de saída da União Europeia, o tratamento dos dados objeto do presente contrato seja legalmente admissível na Grã-Bretanha do ponto de vista do direito de proteção de dados. Na falta de uma decisão de adequação positiva da Comissão Europeia à data da saída da União Europeia, trata-se, à luz da situação atual, sobretudo de cláusulas-tipo de proteção de dados, nos termos do artigo 46.º, n.º 2, alínea c), do RG-PD, aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros onde não esteja garantido um nível de proteção adequado.

Se a entidade adjudicatária não cumprir estas obrigações, a entidade adjudicante tem o direito de exigir à entidade adjudicatária, com efeitos a partir da data de saída da Grã-Bretanha da União Europeia, que os serviços em questão sejam prestados por uma empresa associada ou por uma parte da empresa com sede permanente no território da União Europeia, sem acréscimo de custos ou encargos adicionais para a entidade adjudicante.

10.5 O presente contrato para o tratamento de encomendas existe em 18 versões linguísticas, mas em caso de divergências faz fé a versão original em língua alemã.

10.6 O presente contrato rege-se pelo direito da República Federal da Alemanha, excluindo a Convenção das Nações Unidas sobre os Contratos de Compra e Venda Internacional de Mercadorias. O foro competente é Munique, com expressa renúncia a qualquer outro.

10.7 Os anexos seguintes constituem parte integrante do presente contrato:

Anexo 1 – Descrição do tratamento de encomendas
Anexo 2 – Medidas técnicas e organizativas

ANEXO 1 – Descrição do tratamento de encomendas

1 Contrato principal

Entende-se por «contrato principal», na aceção do n.º 2.1 da parte principal do contrato, as «Condições gerais de utilização da plataforma».

Título / Partes: **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19 - 21, 80807 München / **Utilizador**

2 Objeto e duração do mandato

O objeto do mandato resulta do n.º 1 (*Objeto*) e do n.º 8 (*Dados do utilizador e proteção de dados*) do contrato principal; a duração do mandato resulta do n.º 7 (*Celebração do contrato, duração do contrato e direitos de rescisão*) do contrato principal.

3 Âmbito, natureza e finalidade do tratamento de dados / das medidas de tratamento de dados

O âmbito, a natureza e a finalidade do tratamento de dados pessoais resultam do n.º 8 do contrato principal.

Descrição mais detalhada do objeto do mandato no que diz respeito ao âmbito, à natureza e à finalidade:

De modo a poder prestar os serviços propostos (conforme definidos no contrato principal), a entidade adjudicatária necessita de recolher dados pessoais da entidade adjudicante através de veículos conectados («Connected Vehicles») ou dispositivos móveis (e, eventualmente, dados pessoais transmitidos por operadores terceiros com quem o utilizador tenha acordado a prestação de serviços), na medida necessária para a prestação dos serviços, e transmitir esses dados para a plataforma da entidade adjudicatária onde serão armazenados. A entidade adjudicatária procederá ao tratamento dos dados armazenados na plataforma na medida necessária para a prestação dos serviços (p. ex., para analisar e avaliar, com base nos dados pessoais, o comportamento de condução dos motoristas, bem como a utilização do veículo conectado ou do dispositivo móvel e para apresentar à entidade adjudicante propostas especificamente concebidas com base nesses dados, tais como ações de formação prática para os motoristas, equipamentos personalizados e propostas de melhoria da eficiência). O âmbito, a natureza e a finalidade concretas resultam, de modo particular, dos contratos individuais a celebrar adicionalmente.

4 Círculo de pessoas afetadas (categorias de titulares dos dados)

O tratamento de encomendas afeta os seguintes titulares de dados:

- **Motoristas e outros colaboradores** (colaboradores da própria sociedade da entidade adjudicante), p. ex.
  trabalhadores, formandos, candidatos, ex-funcionários;
- **Motoristas** que não sejam colaboradores;
- **Interlocutores** de agentes de carga/descarga ou de outros parceiros comerciais da entidade adjudicante; e
- **Colaboradores do grupo** (colaboradores de outras sociedades do grupo da entidade adjudicante).

5 Natureza dos dados pessoais

O tratamento de encomendas abrange os seguintes tipos de dados pessoais:

- Nome do motorista e número de identificação do motorista;
- Número de identificação do veículo;
- Dados de localização;
- Dados relativos aos períodos de condução e de descanso;
- Dados sobre o comportamento de condução;
- Dados sobre o estado do veículo conectado;
- Dados sobre o estado do reboque;
- Dados sobre o estado das superestruturas ou peças de montagem, dos agregados e de outros componentes do veículo;
- Dados sobre o estado de dispositivos IOT eventualmente conectados;
- Dados sobre o estado de dispositivos móveis;
- Dados sobre a carga;
- Dados sobre a encomenda; e
- Dados de contacto dos interlocutores de agentes de carga/descarga ou de outros parceiros comerciais da entidade adjudicante.

6 Instruções documentadas

Pelo presente, a entidade adjudicante dá instruções à entidade adjudicatária para tratar os dados pessoais de acordo com o disposto no n.º 8 do contrato principal. Tal inclui, designadamente, o tratamento seguinte:

- Os dados pessoais são transferidos através do veículo conectado ou do equipamento móvel para a plataforma baseada na nuvem da entidade adjudicatária onde serão armazenados.
- Os dados pessoais só são tratados ao abrigo do presente contrato, na medida do necessário para o cumprimento do contrato principal, sem prejuízo no disposto no n.º 8.3.4 do contrato principal.

- A entidade adjudicatária transfere os dados pessoais para um operador terceiro (conforme definido no contrato principal), na medida em que essa transferência seja necessária para que este possa prestar os seus serviços terceiros (conforme definidos no contrato principal) à entidade adjudicante.
- A entidade adjudicatária analisará e avaliará, com base nos dados pessoais, o comportamento de condução dos motoristas, bem como a utilização do veículo conectado e apresentará à entidade adjudicante propostas especificamente concebidas com base nesses dados, tais como ações de formação prática para os motoristas, equipamentos personalizados e propostas de melhoria da eficiência.

7 Local do tratamento

- Alemanha.
- Reino Unido; em caso de tratamento de dados para fins de alojamento e/ou suporte informático no seio da União Europeia, devem ser celebrados os devidos contratos para tratamento de encomendas.
- Se, para efeitos de alojamento e/ou suporte informático, a entidade adjudicatária contratar subcontratantes fora da União Europeia (v., a este respeito, n.º 8 do presente Anexo 1), a transferência de dados pessoais terá por base cláusulas contratuais-tipo/cláusulas-tipo de proteção de dados celebradas entre a entidade adjudicatária e o subcontratante aplicáveis à transferência de dados pessoais em países terceiros nos termos do artigo 46.º n.º 2 alínea c do RG-PD.

8 Subcontratantes

A entidade adjudicatária recorre aos seguintes aos subcontratantes (que poderão, eventualmente, contratar outros subcontratantes):

N.º	Subcontratante (firma, morada, pessoa de contacto)	Categorias de dados objeto de tratamento	Fases de tratamento / Finalidade do tratamento pelo subcontratante
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Todos os dados pessoais da plataforma relacionados com a componente de venda (ou seja, o local onde um cliente pode registar-se na plataforma e efetuar encomendas)	Alojamento da plataforma
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Todos os dados pessoais da plataforma relacionados com a componente de venda (ou seja, o local onde um cliente pode registar-se na plataforma e efetuar encomendas)	Suporte informático relacionado com a plataforma
3	Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 EUA https://aws.amazon.com/de/compliance/contact/	Todos os demais dados pessoais dos utilizadores que são transmitidos para a entidade adjudicatária através do veículo	Alojamento da plataforma / suporte informático relacionado com o alojamento da plataforma
4	No futuro, eventualmente, em vez do n.º 3: Amazon Webservices (UE) Amazon Web Services, Inc. P.O. Box 81226 Seattle, WA 98108-1226 EUA https://aws.amazon.com/de/compliance/contact/	Todos os demais dados pessoais dos utilizadores que são transmitidos para a entidade adjudicatária através do veículo	Alojamento da plataforma
5	MAN Service und Support GmbH Dachauer Straße 667	Todos os dados pessoais necessários para o processamento de pedidos de clientes no âmbito do	Primeiro nível de suporte

	80995 München Alemanha	primeiro e segundo nível de suporte	
6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 EUA	Todos os dados pessoais necessários para efeitos de faturação/processamento de encomenda	Alojamento da plataforma (Locatário na UE – Alojada pela Amazon Web Services (UE) – v. n.º 4
7	MAN Truck & Bus AG Dachauer Straße 667 80995 München Alemanha	Todos os demais dados pessoais dos utilizadores que são transmitidos para a entidade adjudicatária através do veículo conectado e/ou do dispositivo móvel	Alojamento da plataforma
8	T-Systems International GmbH Hahnstraße 43 d 60528 Frankfurt am Main Alemanha	Todos os demais dados pessoais dos utilizadores que são transmitidos para a entidade adjudicatária através do módulo de telemática de bordo 1/2 dos veículos	Alojamento da plataforma
9	Scania AB Vagnmakarvägen 1 15187 Södertälje Suécia	Todos os demais dados pessoais dos utilizadores que são transmitidos para a entidade adjudicatária através do veículo	Alojamento da plataforma
10	Volkswagen Veículos utilitários Mecklenheidestr. 74 30419 Hannover Alemanha	Todos os demais dados pessoais dos utilizadores que são transmitidos para a entidade adjudicatária através do veículo	Alojamento da plataforma

ANEXO 2 – Medidas técnicas e organizativas
As medidas técnicas e organizativas adequadas a adotar pela entidade adjudicatária para assegurar um nível de segurança adequado ao risco estão descritas no esquema de proteção de dados da plataforma RIO e incluem, designadamente, as seguintes:

1. Pseudonimização

Na medida em que a utilização dos dados pessoais se destine a fins de avaliação, que também possam ser realizados com dados pseudonimizados, serão aplicadas técnicas de pseudonimização. Nesse âmbito, define-se, previamente, para cada campo de dados se existe necessidade de pseudonimização dos dados em virtude de permitirem a identificação de uma determinada pessoa. Os códigos de pseudonimização são guardados num cofre de dados para o qual serão configuradas as máximas restrições de acesso possíveis.

2. Cifragem

Os equipamentos terminais móveis comunicam de forma encriptada com o ponto terminal usando certificados individuais para cada equipamento. Na própria plataforma RIO, os dados são reencaminhados de forma encriptada («Ubiquitous encryption» ou «encryption everywhere»).

3. Garantia da confidencialidade

Todos os colaboradores foram e estão informados sobre as suas obrigações de confidencialidade e assumiram um compromisso de confidencialidade dos dados.

A infraestrutura informática utilizada é fornecida pela Amazon Web Services (a seguir designado por AWS) em nuvem (IaaS & PaaS). O controlo de acessos é assegurado pelo operador do centro de dados da AWS: os centros de dados de alta segurança da AWS aplicam sofisticadas medidas de vigilância eletrónica e sistemas de controlo de acessos com vários níveis. Os centros de dados dispõem de pessoal de segurança qualificado em permanência, durante 24 horas por dia, e o acesso é concedido na estrita observância do princípio do menor privilégio e unicamente para fins de administração do sistema.

O acesso aos componentes de hardware («Clients») na TB Digital Services GmbH processa-se de acordo com as medidas-tipo em vigor, adequadas a cada caso. Trata-se, p. ex., de restrições de acesso através de sistemas de individualização (torniquetes), sistemas de videovigilância, sistemas de alarme e/ou serviços de segurança, portas com bloqueio eletrónico ou mecânico, edifícios blindados, direitos de acesso documentados (visitantes, funcionários externos) ou áreas de segurança declaradas.

Os controlos de acesso abrangem medidas para garantir a segurança dos equipamentos, da rede e das aplicações.

Para efeitos de segurança dos equipamentos no veículo são aplicadas diferentes medidas: os equipamentos terminais móveis encontram-se instalados de forma fixa no veículo e dispõem de um sistema de arranque

seguro («Secure Boot»), ou seja, não existe qualquer possibilidade de carregar e forçar o arranque de um sistema operativo externo. Os equipamentos terminais móveis comunicam de forma encriptada com o ponto terminal usando certificados individuais para cada equipamento. Na própria plataforma RIO, os dados são reencaminhados de forma encriptada («Ubiquitous encryption» ou «encryption everywhere»). Os equipamentos terminais móveis cumprem os níveis de segurança atuais, graças à instalação regular das atualizações de segurança (Gestão de Patches).

Para efeitos de segurança da rede são igualmente aplicadas diferentes medidas-tipo: Foram definidos requisitos de palavra-passe (comprimento, complexidade, validade das palavras-passe, etc.) adequados (correspondentes às melhores técnicas disponíveis). A introdução repetida de uma combinação errada da identificação do utilizador/palavra-passe implica um bloqueio (temporário) da autenticação do utilizador. A rede da empresa está protegida por meio de uma firewall contra redes abertas sem segurança. Está instituído um processo que assegura a instalação regular de atualizações de segurança nos dispositivos móveis (processo OTA). São utilizadas tecnologias apropriadas (p. ex., sistemas de deteção de intrusões) para detetar e evitar ataques à rede da empresa (Intranet). Os colaboradores são sensibilizados regularmente para os perigos e riscos.

Para efeitos de segurança das aplicações são aplicadas algumas medidas-tipo:

As aplicações relevantes estão protegidas contra acessos não autorizados por meio de mecanismos de autenticação e autorização. Foram definidos requisitos de palavra-passe (comprimento, complexidade, validade das palavras-passe, etc.) adequados (correspondentes às melhores técnicas disponíveis). Para as aplicações que requerem especial proteção são utilizados mecanismos de autenticação fortes (p. ex., Token, PKI). A introdução repetida de uma combinação errada da identificação do utilizador/palavra-passe implica um bloqueio (temporário) da autenticação do utilizador. Os dados utilizados no processo relevante estão disponíveis em formato encriptado num suporte de dados móvel. Os acessos e as tentativas de acesso às aplicações ficam registados. Os ficheiros de registo criados são guardados durante um período adequado (pelo menos 90 dias) e controlados (por amostragem).

As permissões de utilizador (para efeitos de entrada e acesso) são asseguradas através de diferentes medidas, geralmente associadas a uma determinada pessoa. A atribuição das permissões compete ao responsável pela plataforma e é controlada regularmente. As permissões de acesso só são atribuídas segundo um processo definido e documentado. As alterações às permissões de acesso obedecem ao princípio do controlo duplo e são documentadas num ficheiro de registo cujas versões sucessivas são mantidas.

Para efeitos de controlo e gestão dos acessos são aplicadas diferentes medidas: os direitos de acesso são definidos e documentados num esquema de funções/permissões e estão associados a cada uma das funções de acordo com as respetivas necessidades. Existem funções/permissões específicas para a administração técnica (que, sendo viável do ponto de vista técnico, não permitem o acesso a dados pessoais). Existem funções/permissões específicas para o suporte técnico (que não abrangem direitos de administração técnica).

Na medida do possível em termos técnicos e organizativos, as funções/permissões são definidas e atribuídas por pessoas distintas segundo um procedimento (de aprovação) passível de auditoria e têm duração limitada. O acesso direto às bases de dados, contornando o esquema de funções/permissões, só é permitido a administradores de bases de dados autorizados. Existem regras para a utilização de suportes de dados privados, ou o uso de suportes de dados privados é proibido. Existem regras obrigatórias relativas ao acesso a dados durante operações de manutenção externas, de telemanutenção e de teletrabalho. Os documentos e suportes de dados são destruídos/eliminados de forma a salvaguardar a proteção dos dados (p. ex., destruidoras, contentores de recolha de documentos confidenciais) por empresas de eliminação fiáveis.

O esquema de funções/permissões é adaptado regularmente à evolução das estruturas de organização do trabalho (p. ex., novas funções); as novas funções/permissões atribuídas são controladas regularmente (p. ex., pelos superiores hierárquicos) e adaptadas ou retiradas, se for caso disso. Existe um controlo regular centralizado dos perfis-tipo atribuídos. Os acessos de modificação (gravar, apagar) são registados, e os ficheiros de registo criados são guardados durante um período adequado (pelo menos 90 dias) e controlados (por amostragem).

Para efeitos gerais de proteção da transferência são aplicadas diferentes medidas-tipo:

As pessoas incumbidas da transferência dos dados são, previamente, familiarizadas com as medidas de segurança a adotar. O círculo de destinatários é definido previamente de modo a permitir o respetivo controlo (autenticação). O processo completo de transferência de dados encontra-se definido e documentado, e a execução da transferência concreta dos dados é registada ou documentada (p. ex., aviso de receção, recibo). As pessoas incumbidas da transferência dos dados procedem, logo à partida, à verificação da plausibilidade, integridade e exatidão dos dados.

Antes da execução da transferência concreta dos dados é realizada uma verificação do endereço do destinatário (p. ex., endereço eletrónico). A transferência de dados através da Internet ocorre de forma encriptada (p. ex., codificação dos ficheiros). A integridade dos dados transferidos é garantida, na medida do tecnicamente possível, pela utilização de processos de assinatura (assinatura digital). Os recibos de leitura eletrónicos são arquivados de forma adequada. As transferências de dados indesejadas através da Internet são impedidas através de tecnologias apropriadas (p. ex., proxy, firewall).

Para efeitos de cumprimento da obrigação de separação são ainda aplicadas as seguintes medidas-tipo:

Existem regras obrigatórias relativas à limitação do tratamento às finalidades previstas, de modo a cumprir a obrigação de separação. Os dados recolhidos para determinadas finalidades são armazenados em locais separados dos dados recolhidos para outras finalidades. Os sistemas informáticos utilizados permitem o armazenamento separado de dados (através de uma arquitetura *multi-tenancy* ou de esquemas de acesso). Existe uma separação dos dados nos sistemas de teste e nos sistemas produtivos. No caso de dados pseudonimizados, os códigos que permitem restabelecer a identificação das pessoas são armazenados ou guardados em locais separados. Em caso de tratamento de encomendas ou delegação de funções, a entidade

adjudicatária procederá ao tratamento separado dos dados de diferentes entidades adjudicantes. Os esquemas de funções/permissões já existentes permitem a separação lógica dos dados tratados.

4. Garantia da integridade

Para efeitos de registo das entradas efetuadas são aplicadas diferentes medidas-tipo:

As alterações dos direitos de acesso e todas as atividades dos administradores ficam registadas. Os acessos de escrita (introduzir, alterar, apagar dados) e as alterações efetuadas nos campos de dados ficam registadas (p. ex., conteúdo do conjunto de dados criado ou alterado). As transferências de dados (p. ex., o download) e os inícios de sessão ficam registados.

Os documentos utilizados para o registo são documentados e arquivados a fim de permitir a inteligibilidade das entradas efetuadas. No registo ficam a constar a data e a hora, o utilizador, o tipo de atividade, a aplicação informática e o número de ordem do conjunto de dados. As definições de registo são documentadas.

Aos ficheiros de registo é concedido exclusivamente acesso de leitura. O círculo de pessoas com permissão de acesso aos ficheiros de registo é muito limitado (p. ex., o administrador, o encarregado da proteção de dados, o auditor). Os ficheiros de registo são guardados durante um período predefinido (p. ex., 1 ano) e, posteriormente, eliminados de uma forma que salvaguarde a proteção dos dados. Os ficheiros de registo são avaliados regularmente de forma automatizada. As avaliações dos ficheiros de registo serão, sempre que possível, pseudonomizadas.

5. Garantia da disponibilidade

A arquitetura da própria plataforma da AWS dispõe de mecanismos internos de replicação dos dados que a protegem contra a perda de dados. Para efeitos de proteção das instalações são ainda aplicadas as seguintes medidas-tipo da AWS:

São aplicadas medidas de proteção contra incêndios (p. ex., portas corta-fogo, sensores de fumo, barreiras ao fogo, proibição de fumar). Os sistemas informáticos estão protegidos contra inundações (p. ex., sala de informática no 1.º piso, sensores de água). São adotadas medidas de proteção contra vibrações (p. ex., sala de informática não localizada nas proximidades de vias rápidas, vias férreas, casas de máquinas). Os sistemas informáticos estão protegidos contra campos eletromagnéticos (p. ex., chapas de aço nas paredes exteriores). São adotadas medidas de prevenção de vandalismo, roubo ou furto (v. controlo de acessos). Os sistemas informáticos estão localizados em compartimentos climatizados (temperatura e humidade do ar reguladas por ar condicionado). Os sistemas informáticos estão equipados com dispositivos de proteção contra sobretensão que os protegem de picos de tensão. São adotadas medidas para garantir uma alimentação de corrente contínua e sem interferências (p. ex., UPS, agregados de alimentação de emergência).

São efetuadas cópias de segurança regulares dos dados armazenados na plataforma da AWS. O esquema de cópias de segurança está documentado e é sujeito a verificações e atualizações regulares. Os suportes de cópia

de segurança estão protegidos contra acessos não autorizados. Os programas de cópia de segurança usados cumprem as normas de qualidade atuais e são regularmente atualizados de modo a garantir essa conformidade. Foi criado um centro de dados redundante (afastado do local de tratamento) que permite assegurar a continuidade do tratamento dos dados em caso de catástrofe. As diversas medidas de controlo da disponibilidade encontram-se documentadas num plano de gestão de emergências da AWS.

Antes da adjudicação do tratamento de dados, a entidade adjudicatária é sujeita a um exame rigoroso segundo determinados critérios (medidas técnicas e organizativas). Para esse efeito, é solicitada uma apresentação detalhada das medidas técnicas/organizativas de proteção de dados aplicadas pela entidade adjudicatária (resposta a um questionário ou esquema de proteção de dados) que são depois analisadas. Dependendo do volume e da sensibilidade dos dados tratados, esse exame também poderá ser realizado nas instalações da entidade adjudicatária, se for caso disso. Na seleção das entidades adjudicatárias são levadas em consideração as certificações adequadas (p. ex., ISO 27001). O reconhecimento da aptidão da entidade adjudicatária é documentado de uma forma adequada e inteligível.

Para efeitos de estabelecimento da relação contratual é celebrado um contrato de tratamento de encomendas entre a entidade adjudicante e a entidade adjudicatária. Neste contrato são definidas de forma detalhada e por escrito as competências, responsabilidades e obrigações de ambas as partes. Se um prestador de serviços contratado tiver a sua sede no exterior da UE ou do EEE, aplicam-se as cláusulas contratuais-tipo da UE. Está estabelecido no contrato que a entidade adjudicatária só pode proceder ao tratamento de dados de acordo com as instruções da entidade adjudicante. A entidade adjudicatária compromete-se a informar, de imediato, a entidade adjudicante se entender que uma das instruções recebidas da entidade adjudicante viola as normas em matéria de proteção de dados. A fim de garantir o respeito dos direitos dos titulares de dados, fica estabelecido no contrato de tratamento de encomendas que a entidade adjudicatária prestará o devido apoio à entidade adjudicante, caso seja necessário, p. ex., para a prestação de informações aos titulares de dados.

No decurso do tratamento de encomendas, a entidade adjudicante controlará os resultados do trabalho da entidade adjudicatária do ponto de vista formal e de conteúdo. O cumprimento das medidas técnicas e organizativas adotadas pela entidade adjudicatária é controlado regularmente. Para esse efeito, recorre-se sobretudo à apresentação de pareceres recentes ou certificações adequadas ou de comprovativos das auditorias de segurança informática ou de proteção de dados realizadas. Caso haja subcontratantes, está estabelecido no contrato que estes serão controlados em conformidade.

6. Garantia da resiliência dos sistemas

A infraestrutura em nuvem da AWS foi concebida como um dos ambientes mais flexíveis e seguros de computação em nuvem. Proporciona um ótimo nível de disponibilidade, garantindo ao mesmo tempo a separação total dos clientes. Oferece uma plataforma extremamente expansível com elevada segurança operacional, que permite aos seus clientes uma propagação rápida e segura de aplicações e conteúdos a nível mundial. Os serviços da AWS são independentes dos conteúdos, na medida em que oferecem a todos os clientes

o mesmo nível elevado de segurança, independentemente do tipo de conteúdos ou da região geográfica onde os conteúdos são armazenados.

Os centros de dados de alta segurança e excelência mundial da AWS aplicam sofisticadas medidas de vigilância eletrónica e sistemas de controlo de acessos com vários níveis. Os centros de dados dispõem de pessoal de segurança qualificado em permanência, durante 24 horas por dia, e o acesso é concedido na estrita observância do princípio do menor privilégio e unicamente para fins de administração do sistema.

7. Procedimento para restabelecer a disponibilidade e o acesso aos dados pessoais no caso de um incidente físico ou técnico

Os centros de dados da AWS são criados em agrupamentos (*clusters*) em diversas regiões do mundo. Todos os centros de dados estão em linha e servem os seus clientes; nenhum centro de dados se encontra desligado. Em caso de falha, existem processos automáticos que direcionam o tráfego de dados de clientes para fora das áreas afetadas. As aplicações centrais são disponibilizadas numa configuração N+1 para que, em caso de falha de um dos centros de dados, exista capacidade suficiente para distribuir o tráfego de dados pelos restantes centros, repartindo a carga.

A AWS oferece flexibilidade em termos de posicionamento de instâncias e de armazenamento de dados espalhados por várias regiões geográficas e por diversas zonas de disponibilidade dentro de cada uma das regiões. Cada uma das zonas de disponibilidade foi concebida como zona de falha independente. Isso significa que as zonas de disponibilidade se encontram fisicamente distribuídas por uma região urbana típica e se situam, p. ex., em regiões de baixo risco de inundações (em cada região existem diferentes categorias de zonas de inundação). Para além de possuírem fontes autónomas de alimentação ininterrupta de corrente e de agregados de alimentação de emergência no local, todas as zonas de disponibilidade são alimentadas por diferentes redes elétricas exploradas por companhias de eletricidade independentes, de modo a minimizar os pontos únicos de falha. Todas as zonas de disponibilidade possuem uma ligação redundante a diversos fornecedores de trânsito de primeiro nível.

A equipa da Amazon responsável pela gestão de incidentes aplica os procedimentos de diagnóstico normalmente utilizados no setor para agilizar a resolução de incidentes críticos para a empresa. O pessoal operacional está permanentemente disponível, durante 24 horas por dia, sete dias por semana e 365 por ano, para detetar falhas e gerir os seus efeitos e a respetiva reparação.

8. Processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas

As orientações e instruções existentes na empresa e as normas implementadas para garantir a segurança da informação são igualmente aplicáveis ao lançamento e à exploração da plataforma RIO. Na empresa existem cargos específicos para a proteção de dados e a segurança da informação (encarregado da proteção de dados e Information Security Officer). Os empregados assumem um compromisso de confidencialidade dos dados e são

informados sobre as medidas de segurança de dados e de segurança informática por meio de brochuras, panfletos, avisos na Intranet, etc.

Existe um controlo dos processos internos no que diz respeito ao cumprimento das medidas técnicas e organizativas para garantir a segurança de dados por meio de auditoria, segurança da informação e proteção de dados.

Os processos de tratamento e as medidas de segurança de dados são documentados num registo das atividades de tratamento. A eficácia das medidas é controlada regularmente por meio de uma auditoria (interna e externa).