# *Contrato para a prestação de serviços RIO e tratamento de dados (de acordo com a Lei Geral de Proteção de Dados e o Regulamento Geral sobre a Proteção de Dados)*

celebrado entre

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

(a seguir designado por ***Cliente***)

e

a Volkswagen Truck & Bus Indústria e Comércio de Veículos Ltda e RIO Soluções Digitais Ltda., Rua Volkswagen, 291, Jabaquara, São Paulo – SP, CEP. 04344-901

(a seguir designada por ***Contratada***)
(a Cliente e a Contratada são a seguir designadas, individualmente, por ***Parte*** e, conjuntamente, por ***Partes***).

***Preâmbulo***

(A) O presente Contrato para a prestação de serviços e tratamento de dados (a seguir designado por ***Contrato***) é aplicável a todas as atividades em que a Contratada tenha contato com dados pessoais (conforme definidos no item 1.5 abaixo) da Cliente, de terceiros ou de outros titulares de dados no âmbito da atividade descrita no item 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 Cliente age na qualidade de responsável (controladora) e a Contratada na qualidade de operadora de dados para efeitos de tratamento de dados relativos à prestação de serviços nos termos da LGPD e do artigo 28.º do RGPD (como definido em baixo).

Posto isto, as partes acordam no seguinte:

## *1 Definições e interpretações*

***1.1*** Entende-se por ***Direito Europeu de Proteção de Dados*** o direito aplicável da União Europeia em matéria de tratamento de dados pessoais (designadamente, o RGPD), as leis aplicáveis em matéria de tratamento de dados pessoais dos atuais Estados-Membros da União Europeia, bem como as leis aplicáveis em matéria de tratamento de dados pessoais de qualquer Estado que venha a aderir, futuramente, à União Europeia.

***1.2*** Entende-se por ***Direito Brasileiro de Proteção de Dados*** o direito aplicável da República Federativa do Brasil em matéria de tratamento de dados pessoais (designadamente, a LGPD e outras legislações aplicáveis).

**1.3** Entende-se por ***RGPD*** 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 ***LGPD*** a Lei nº 13.709, de 14 de agosto de 2018, conforme alterada de tempos em tempos, que dispõe sobre a proteção de dados pessoais (Lei Geral de Proteção de Dados).

**1.5** O conceito de ***dados pessoais*** tem o significado que lhe é atribuído na LGPD e no RGPD.

**1.6** Entende-se por ***ANPD*** a Autoridade Nacional de Proteção de Dados, órgão da administração pública federal, atualmente integrante da Presidência da República, responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.

## *2 Objeto do tratamento de dados / Obrigações do Cliente*

**2.1** O presente Contrato rege as obrigações das Partes no contexto do tratamento de dados pessoais do Cliente pela Contratada 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 Cliente permanecerá como responsável (controlador) no âmbito da LGPD e do RGPD e garante a admissibilidade do tratamento de dados pessoais dos titulares (motoristas e possivelmente outras pessoas). Em particular, o Cliente deverá cumprir sua obrigação extensiva de fornecer informações e assegurar que o tratamento de dados pessoais se baseie em uma hipótese legal de tratamento de dados.

## *3 Obrigações da Contratada*

**3.1** A Contratada procederá ao tratamento dos dados pessoais do Cliente exclusivamente para as finalidades referidas no Anexo 1 e no âmbito do contrato principal, agindo por conta do Cliente e de acordo com as suas instruções documentadas no Anexo 1. A Contratada 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 item 8.3.4 do contrato principal. A Contratada não produzirá cópias ou duplicatas dos dados pessoais sem o conhecimento do Cliente. 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 e/ou necessários para fins de interesse legítimo.

***3.2*** Uma vez concluída a prestação dos serviços de tratamento, a Contratada deverá, consoante a escolha do Cliente, entregar-lhe todos os dados pessoais que lhe digam respeito e/ou eliminá-los salvaguardando a proteção dos dados, a não ser que a tal obstem os prazos legais de conservação de dados ou que a Contratada proceda ao tratamento dos dados para uso próprio fora do âmbito de aplicação do presente contrato, nos termos do item 8.3.4 do contrato principal. O mesmo se aplica ao material de teste e eliminado. A pedido do Cliente, a Contratada confirmará, por escrito e com indicação da data, que apagou por completo ou entregou todos os dados ao Cliente ou anonimizou tais dados.

***3.3*** Desde que abrangido pelo âmbito dos serviços, a Contratada apoiará o Cliente no cumprimento dos direitos do titular dos dados (informação, correção, oposição, eliminação) de acordo com as instruções do Cliente.

***3.4*** A Contratada confirma que – caso seja obrigatório por lei – designou um encarregado pela proteção de dados (nos termos do artigo 41 LGPD e do artigo 37.º do RGPD).

***3.5*** A Contratada compromete-se a comunicar, sem demora, ao Cliente o resultado de auditorias realizadas pelas autoridades de controle da proteção de dados, na medida em que estas digam respeito aos dados do Cliente. Caso sejam detectadas eventuais desconformidades, a Contratada irá corrigi-las dentro de um prazo razoável e informará o Cliente a este respeito.

***3.6*** O tratamento dos dados pela Contratada e por operadores de dados aprovados pelo Cliente é realizado exclusivamente no território da República Federativa do Brasil, da República Federal da Alemanha, dos Estados Membros da União Europeia, dos países signatários do Acordo sobre o Espaço Económico Europeu, e/ou dos países onde os parceiros da Contratada mantenham servidores. Qualquer transferência para outro país (a seguir designado por ***País Terceiro***) depende do prévio consentimento expresso do Cliente, além de só ser permitida se estiveram reunidas as condições especiais para a exportação de dados para países terceiros (nos termos do artigo 33, I, da LGPD e do artigo 40.º ss. do RGDP). Para esse efeito, é necessário prestar as informações referidas no Anexo 1 e, eventualmente, juntar outros documentos (contratuais).

***3.7*** A Contratada dará conhecimento aos colaboradores contratados para o tratamento dos dados das disposições relevantes em matéria de proteção de dados e exigirá que assumam um compromisso de confidencialidade (nos termos da LGPD e do artigo 28.º do RGPD, n.º 3, alínea b)), assim como garantirá, através de medidas apropriadas, que esses colaboradores processam dados pessoais apenas quando instruídos pelo Cliente.

***3.8*** Durante todo o período de vigência do Contrato, a Contratada procederá regularmente à supervisão do cumprimento das disposições legais em matéria de proteção de dados estabelecidas no presente Contrato e das instruções documentadas do Cliente. Os resultados dos controles devem ser apresentados ao Cliente, mediante pedido, desde que sejam relevantes para o tratamento dos dados do Cliente. As medidas de supervisão encontram-se descritas em um plano de proteção de dados, que deve ser apresentado ao Cliente, mediante pedido.

***3.9*** A Contratada prestará assistência ao Cliente, 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 da LGPD e no capítulo III do RGPD. O Cliente suportará as despesas incorridas pela Contratada neste contexto.

***3.10*** A Contratada prestará assistência ao Cliente no sentido de assegurar o cumprimento das obrigações previstas no capítulo VII nos artigos 32.º a 36.º do RGPD, tendo em conta a natureza do tratamento e a informação disponível.

## *4 Medidas técnicas e organizativas para garantir a segurança dos dados*

***4.1*** A Contratada adotará medidas técnicas e organizativas adequadas para assegurar a proteção de dados (nos termos do artigo 46 da LGPD e do artigo 32.º do RGPD). Compete, em especial, à Contratada aplicar as medidas técnicas e organizativas acordadas contratualmente no Anexo 2 do presente Contrato. Ao longo da vigência do Contrato, a Contratada 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 do Cliente, a Contratada deverá demonstrar o cumprimento efetivo das medidas técnicas e organizativas.

***4.3*** A Contratada está obrigada a manter um registro adequado do tratamento dos dados, com base no qual o Cliente possa comprovar que o tratamento dos dados é realizado corretamente. Essa prova também pode ser prestada mediante um procedimento de certificação aprovado nos termos definidos pela ANPD e do artigo 42.º do RGPD.

## *5 Operadores de dados*

***5.1*** A Contratada fica, pela presente, autorizada a recorrer aos operadores de dados referidos no Anexo 1.

***5.2*** É concedida uma autorização geral de contratação de outros operadores de dados. A Contratada informará, no entanto, o Cliente de quaisquer alterações pretendidas quanto ao aumento do número ou à substituição de outros operadores de dados; o Cliente 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 Contratada 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 Contratada tem a obrigação de celebrar acordos contratuais adequados e conformes com a lei e de adotar medidas de controle para garantir a proteção e segurança dos dados do Cliente.

**5.3** Se a Contratada contratar um operador de dados, deverá garantir que lhe são impostas, (i) por contrato celebrado entre o operador de dados e a Contratada ou (ii) por outro ato normativo ao abrigo do Direito Europeu de Proteção de Dados e do Direito Brasileiro de Proteção de Dados, as mesmas obrigações em matéria de proteção de dados a que a Contratada está sujeita ao abrigo do presente Contrato. A Contratada deverá assegurar, em particular, que o operador de dados 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 da LGPD e do RGPD. Mediante pedido escrito do Cliente, a Contratada 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 Contratada poderá ocultar as condições comerciais. O Cliente está obrigado a manter sigilo sobre as informações obtidas.

## *6 Direitos de fiscalização*

**6.1** O Cliente tem o direito de fiscalizar ele próprio ou de designar uma entidade terceira competente para fiscalizar o cumprimento das obrigações emergentes do presente Contrato (incluindo as instruções dadas).

**6.2** A Contratada prestará o devido apoio ao Cliente durante a fiscalização. A Contratada facultará, designadamente, acesso aos sistemas de processamento de dados e prestará as informações necessárias.

**6.3** Caso reste comprovado que a Contratada e/ou o tratamento não estão em conformidade com as disposições do presente Contrato e/ou do Direito Europeu de Proteção de Dados e do Direito Brasileiro de Proteção de Dados, a Contratada tomará todas as ações corretivas necessárias para garantir o cumprimento das disposições do presente Contrato e/ou do Direito Europeu de Proteção de Dados e do Direito Brasileiro de Proteção de Dados.

**6.4** Os custos resultantes da realização de uma fiscalização serão suportados pelo próprio Cliente. A Contratada poderá exigir ao Cliente que suporte os custos que lhe sejam causados por uma fiscalização realizada pelo Cliente, nos casos em que o Cliente realize ou mande realizar mais do que uma fiscalização por ano civil.

**6.5** As fiscalizações a serem realizadas nas instalações da Contratada devem ser anunciadas antecipadamente e não devem prejudicar as operações comerciais da Contratada.

## *7 Deveres de informação*

A Contratada informará, de imediato, o Cliente se considerar que uma instrução dada pelo Cliente viola o Direito Europeu de Proteção de Dados ou o Direito Brasileiro de Proteção de Dados. A instrução legitimamente contestada não precisa ser cumprida enquanto não for alterada ou expressamente confirmada pelo Cliente. A Contratada não está obrigada a submeter as instruções a um exame de direito substantivo.

A Contratada informará de forma adequada e em prazo razoável o Cliente no caso de serem detectados erros ou irregularidades no tratamento dos dados ou em caso de suspeita de violação da privacidade (a seguir conjuntamente designados por ***Incidente***). O Cliente terá de documentar o incidente, incluindo todos os fatos, as respectivas consequências e todas as medidas corretivas adotadas, e enviar em prazo razoável ao Cliente, mediante pedido, estas informações documentadas, por escrito ou por via eletrônica.

## *8 Responsabilidade e exoneração de responsabilidade*

***8.1*** A Contratada responde por danos causados por dolo e/ou culpa grave sua ou dos seus agentes. A Contratada só responde por danos causados por culpa leve ou média sua 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 o Cliente tomou e podia tomar por garantia. Se a violação de tais obrigações fundamentais dever-se a culpa leve ou média, a responsabilidade da Contratada ficará limitada aos danos normalmente previsíveis.

***8.2*** O Cliente exonera a Contratada 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 do Cliente, das disposições do presente Contrato e/ou do Direito Europeu de Proteção de Dados e/ou do Direito Brasileiro de Proteção de Dados; esta exoneração de responsabilidade não se aplica se a violação não for imputável ao Cliente ou na medida em que a Contratada 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 disposição não prejudica o direito de rescisão do Contrato por justa causa.

Não obstante, a Contratada reserva-se o direito de manter por prazo indeterminado os dados que sejam necessários para cumprimento de obrigações legais e/ou necessários para aprimorar os seus serviços, tratando-os com base em seu legítimo interesse.

## *10 Outras disposições*

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

***10.2*** A Contratada informará, de imediato, o Cliente na eventualidade de os dados pessoais desta última correrem perigo devido a medidas de terceiros (p. ex., penhora ou apreensão), insolvência, processo de recuperação judicial ou falência 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 demais disposições. Em caso de nulidade de uma cláusula, as partes adotarão uma cláusula de substituição inspirada no objetivo material e econômico do Contrato.

***10.4*** O presente Contrato rege-se pelo direito da República Federativa do Brasil. O foro competente é São Paulo, com expressa renúncia a qualquer outro.

***10.5*** Os anexos seguintes constituem parte integrante do presente Contrato:

Anexo 1 – Descrição do tratamento de dados relativos à prestação de serviços
Anexo 2 – Medidas técnicas e organizativas

Volkswagen Truck & Bus Indústria e Comércio de Veículos Ltda e RIO Soluções Digitais Ltda
Rua Volkswagen, 291, Jabaquara, São Paulo – SP, CEP. 04344-901

***ANEXO 1 – Descrição do tratamento de dados relativos à prestação de serviços***

## *1 Contrato principal*

Entende-se por Contrato Principal, nos termos do parágrafo 2.1 da parte principal do contrato, as Condições Gerais de Utilização da Plataforma.

Título / Partes: Volkswagen Truck & Bus Indústria e Comércio de Veículos Ltda  e RIO Soluções Digitais Ltda./ ***Usuário***

## *2 Objeto e duração do contrato*

O objeto do Contrato está definido no parágrafo 1 (*Objeto*) e 8 (*Dados do Usuário e proteção de dados*) do Contrato Principal; a duração do Contrato está definida no parágrafo 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 estão descritos no parágrafo 8 do Contrato Principal.

Descrição mais detalhada do objeto do Contrato 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 Contratada necessita coletar dados pessoais do Cliente através de veículos conectados (Veículos Conectados) ou dispositivos móveis (e, eventualmente, dados pessoais transmitidos por operadores terceiros com quem o Usuário tenha acordado a prestação de serviços), na medida necessária para a prestação dos serviços, e transmitir esses dados para a plataforma da Contratada onde serão armazenados. A Contratada 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 ao Cliente 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 celebrados adicionalmente.

## *4 Titulares de Dados (categorias de titulares dos dados)*

O tratamento de dados relativos a prestação de serviços afeta os seguintes titulares de dados:

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

## *5 Natureza dos dados pessoais*

A prestação de serviços RIO abrange o tratamento dos 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 relativos à prestação de serviços; e
- Dados de contato dos interlocutores de agentes de carga/descarga ou de outros parceiros comerciais do Cliente.

## *6 Instruções documentadas*

Pelo presente, o Cliente dá instruções à Contratada para tratar os dados pessoais de acordo com o disposto no parágrafo 8 do Contrato Principal. Tal parágrafo inclui, designadamente, o seguinte tratamento:

- Os dados pessoais são transferidos através do veículo conectado ou do equipamento móvel para a plataforma baseada na nuvem da Contratada 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 item 8.3.4 do Contrato Principal.
- A Contratada 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) ao Cliente.

- A Contratada analisará e avaliará, com base nos dados pessoais, o comportamento de condução dos motoristas, bem como a utilização do veículo conectado e apresentará ao Cliente 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*

- Brasil.
- Alemanha.
- Países onde os parceiros da Contratada mantenham servidores
- Se, para efeitos de alojamento e/ou suporte informático, a Contratada contratar operadores de dados fora do Brasil e/ou da União Europeia (nos termos do parágrafo 8 do presente Anexo 1), a transferência de dados pessoais terá por base cláusulas-padrão de proteção de dados celebradas entre a Contratada e o operador de dados aplicáveis à transferência de dados pessoais em países terceiros nos termos dos artigos 33, II, alínea b, e 35 da LGPD e do artigo 46.º n.º 2, alínea c do RGPD.

## *8 Operadores de dados*

A Contratada recorre aos seguintes operadores de dados (que poderão, eventualmente, contratar outros operadores de dados):

| N.° | Operador de dados (empresa e endereço) | Categorias de dados objeto de tratamento | Fases de tratamento/ Finalidade do tratamento pelo subcontratado |
|---|---|---|---|
| 1 | Salesforce.com EMEA Limited<br><br>Sales force.com Privacy, The landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA | Todos os dados pessoais da plataforma relacionados com a venda (local onde um cliente se cadastrou na plataforma e adquiriu um serviço) | Armazenamento 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 venda (local onde um cliente se cadastrou na | Suporte de TI em relação a plataforma |

| | | | |
|---|---|---|---|
| | | plataforma e adquiriu um serviço) | |
| 3 | Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 EUA<br><br>https://aws.amazon.com/de/compliance/contact/ | Todos os demais dados pessoais usuário, é transmitido para o contratante através do veículo | Armazenamento da plataforma/ Suporte de TI sobre o armazenamento da plataforma |
| 4 | Amazon Webservices Brasil<br><br>Av. Pres. Juscelino Kubitschek, 2041 CEP 04543-011 São Paulo, SP – Brazil | Todos os demais dados pessoais usuário, é transmitido para o contratante através do veículo | Armazenamento da plataforma/ Suporte de TI sobre o armazenamento da plataforma |
| 5 | NEOBPO Terceirização de processos, serviços e tecnologia S.A<br><br>Rua Conselheiro Nébias, 14 CEP 01203-900 São Paulo SP | Todos os dados pessoais necessário para processamento de consultas de cliente (Primeiro e segundo nível de suporte) | Primeiro e segundo nível de suporte |
| 6 | TB Digital Services GmbH, Oskar-Schlemmer-Str. 19-21, 80807 München | Todos os outros dados pessoais do usuário transmitido ao contratante através de o veículo | Armazenamento da plataforma |
| 7 | Zuora Inc. 3050 S. Delaware Streer, Suite 301 San Mateo, CA 94403 EUA | Todos os dados pessoais necessários para o processamento de faturas / pedidos em processamento | Armazenamento da Plataforma |
| 8 | T-Systems International GmbH Hahnstraße 43 d 60528 Frankfurt am Main Germany | Todos os outros dados pessoais do usuário transmitido através do | Armazenamento da plataforma |

| | | | |
|---|---|---|---|
| | | veículo TBM1 / 2 ao contratante | |
| 9 | MAN Truck & Bus SE Dachauer Strasse 667, 80995 Munique, Alemanha | Todos os demais dados pessoais do usuário transmitido ao contratante através do veículo conectado e/ ou dispositivo móvel | Armazenamento da plataforma |
| 10 | Volkswagen Truck & Bus Industria e Comercio de Veiculos LTDA; R Volkswagen, 291 7, 8 E 9 ANDARES \| São Paulo - SP, CEP: 04344-901 CNPJ: 06.020.318/0001-10 \| 06020318000110 | Todos os outros dados pessoais do usuário transmitido ao contratante através de o veículo | Armazenamento da plataforma |
| 11 | Volkswagen Truck & Bus Indústria e Comercio de Veiculos LTDA; Av Engenheiro Alan Da Costa Batista, 100, Parte W06 \| Resende - RJ, CEP: 27511-970 ; CNPJ: 14.442.049/0001-09 \| 14442049000109 | Todos os outros dados pessoais do usuário transmitido ao contratante através de o veículo | Armazenamento da plataforma |
| 12 | Stoneridge Do Brasil Participacoes Ltda ; CNPJ: 02.207.195/0001-70 \| 02207195000170 Av Alan Turing, 385 CONJ 1 \| Campinas - SP, CEP: 13083-898 | Todos os demais dados do veículo | Armazenamento da plataforma/ Suporte de TI sobre o armazenamento da plataforma/ Hardware |
| 13 | ATOS Brasil<br>Rua Werner Won Siemens, 111 – Lapa<br>São Paulo – SP, CEP 05069-900 | Todos os dados pessoais necessário para processamento de consultas de cliente (Segundo nível de suporte) | Segundo nível de suporte |
| 14 | IT LEAN TECH LTDA<br>Rua SamueL Morse, 134, conj. 132, São Paulo -SP | Todos os dados pessoais necessário para processamento de | Segundo nível de suporte |

| | | | |
|---|---|---|---|
| | CEP 04576-060<br><br>CNPJ 12.082.645-0001-08 | consultas de cliente (Segundo nível de suporte) | |
| 15 | Move Truly Lead Management<br><br>Avenida das Nações Unidas, 18801 Village Park 33 - Santo Amaro, São Paulo - SP, 04795-100 | Todos os dados pessoais necessário para processamento de consultas de cliente (Segundo nível de suporte) | Segundo nível de suporte |

***ANEXO 2 – Medidas técnicas e organizativas***

As medidas técnicas e organizativas adequadas a adotar pela Contratada 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 controle 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 eletrônica e sistemas de controle de acessos com vários níveis. Os centros de dados dispõem de pessoal de segurança qualificado 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 RIO Soluções Digitais Ltda. processa-se de acordo com as medidas-padrão 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 eletrônico ou mecânico, edifícios blindados, direitos de acesso documentados (visitantes, funcionários externos) ou áreas de segurança declaradas.

O controle de acesso abrange 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-padrão: Foram definidos requisitos de senha (comprimento, complexidade, validade das senhas, etc.) adequados (correspondentes às melhores técnicas disponíveis). A introdução repetida de uma combinação errada da identificação do Usuário/senha implica um bloqueio (temporário) da autenticação do Usuário. A rede da empresa está protegida por meio de um 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 detecção de invasões) para detectar 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-padrão:

As aplicações relevantes estão protegidas contra acessos não autorizados por meio de mecanismos de autenticação e autorização. Foram definidos requisitos de senha (comprimento, complexidade, validade das senhas, 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 Usuário/senha implica um bloqueio (temporário) da autenticação do Usuário. Os dados utilizados no processo correspondente estão disponíveis em formato encriptado num suporte de dados móvel. Os acessos e as tentativas de acesso às aplicações ficam registrados. Os arquivos de registro criados são guardados durante um período adequado (pelo menos 90 dias) e controlados (por amostragem).

As permissões de Usuário (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 duplo controle e são documentadas num ficheiro de registro cujas versões sucessivas são mantidas.

Para efeitos de controle 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 respectivas 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 manutenção remota e de trabalho remoto. Os documentos e suportes de dados são destruídos/eliminados de forma a salvaguardar a proteção dos dados (p. ex., destruidoras, fragmentadoras de documentos confidenciais) por empresas de eliminação idôneas.

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 controle regular centralizado dos perfis-padrão atribuídos. Os acessos de modificação (gravar, apagar) são registados, e os arquivos de registro 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-padrão:

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 respectivo controle (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 recebimento). As pessoas incumbidas da transferência dos dados procedem, inicialmente, 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 eletrônico). A transferência de dados através da Internet ocorre de forma encriptada (p. ex., codificação dos arquivos). A integridade dos dados transferidos é garantida, na medida do tecnicamente possível, pela utilização de processos de assinatura (assinatura digital). Os avisos de recebimento eletrônicos 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-padrão:

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 anonimizados, os códigos que permitem restabelecer a identificação das pessoas são armazenados ou guardados em locais separados. Em caso de tratamento de dados relativos à prestação de serviços ou delegação de funções, a Contratada procederá ao

tratamento separado dos dados de diferentes Clientes. Os esquemas de funções/permissões já existentes permitem a separação lógica dos dados tratados.

### *4. Garantia da integridade*

Para efeitos de registro das entradas efetuadas são aplicadas diferentes medidas-padrão:

As alterações dos direitos de acesso e todas as atividades dos administradores ficam registradas. 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 registro são documentados e arquivados a fim de permitir a inteligibilidade das entradas efetuadas. No registro constam a data e a hora, o Usuário, o tipo de atividade, a aplicação informática e o número de ordem do conjunto de dados. As definições de registro são documentadas.

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

### *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-padrão 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. controle de acessos). Os sistemas informáticos estão localizados em compartimentos climatizados (temperatura e umidade 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 controle da disponibilidade encontram-se documentadas num plano de gestão de emergências da AWS.

Antes da autorização para tratamento de dados ser dada, a Contratada 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 Contratada (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 Contratada, se for o caso. Na seleção das entidades adjudicatárias são levadas em consideração as certificações adequadas. O reconhecimento da aptidão da Contratada é documentado de uma forma adequada e inteligível.

Para efeitos de estabelecimento da relação contratual é celebrado um contrato de tratamento de dados relativos à prestação de serviços entre o Cliente e a Contratada. 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 fora do Brasil, da UE ou do EEE, aplicam-se as cláusulas-padrão indicadas pela ANPD ou pelo RGPD. Está estabelecido no contrato que a Contratada só pode proceder ao tratamento de dados de acordo com as instruções do Cliente. A Contratada compromete-se a informar, de imediato, o Cliente se entender que uma das instruções recebidas do Cliente 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 dados relativos à prestação de serviços que a Contratada prestará o devido apoio ao Cliente, caso seja necessário, p. ex., para a prestação de informações aos titulares de dados.

No decurso do tratamento, o Cliente controlará os resultados do trabalho da Contratada do ponto de vista formal e de conteúdo. O cumprimento das medidas técnicas e organizativas adotadas pela Contratada é controlado regularmente. Para esse efeito, recorre-se sobretudo à apresentação de pareceres recentes ou certificações adequadas ou de comprovantes de auditorias de segurança informática ou de proteção de dados realizadas. Caso haja operadores de dados, 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 conteúdo 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 eletrônica e sistemas de controle 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 autônomas 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 detectar falhas e gerir os seus efeitos e a respectiva 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 controle 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 registro das atividades de tratamento. A eficácia das medidas é controlada regularmente por meio de uma auditoria (interna e externa).