LOGISTIK IM FLUSS.

Contrat de sous-traitance du traitement (conformément à l'article 28 du RGPD)

entre

l'**Utilisateur** (tel que défini dans le contrat principal)

(appelé ci-après « **Demandeur** »)

et

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

(appelé ci-après « **Sous-traitant** »)
(Le Demandeur et le Sous-traitant sont ci-après désignés individuellement comme une « **Partie** » et collectivement comme les « **Parties** ».)

Préambule

(A) Le présent contrat de sous-traitance du traitement (ci-après le « **Contrat** ») s'applique à toutes les activités par lesquelles le Sous-traitant entre en contact avec des données personnelles (telles que définies au point 1.5 ci-dessous) du Demandeur, d'un fournisseur tiers ou de toute autre partie concernée en lien avec l'activité décrite au point 2 découlant des conditions-cadres générales de l'utilisation de la plateforme et, éventuellement, des contrats particuliers conclus en vertu de ces dernières pour des services supplémentaires (ci-après dénommé « **Contrat principal** »).

(B) En vertu de ce contrat, le Demandeur agit comme responsable et le Sous-traitant agit comme un sous-traitant dans le cadre d'un contrat de sous-traitance du traitement conformément à l'article 28 du RGPD (comme défini ci-après).

Les Parties conviennent de ce qui suit :

1 Définitions et interprétation

1.1 Le « **Droit européen** » est le droit applicable de l'Union européenne, les lois applicables des États membres actuels de l'Union européenne, ainsi que les lois applicables de tout État devenant par la suite membre de l'Union européenne.

1.2 Le « **Droit européen en matière de protection des données** » est le droit applicable de l'Union européenne en matière de traitement des données personnelles (notamment le RGPD), les lois applicables des États membres actuels de l'Union européenne en matière de traitement des données personnelles (notamment la BDSG dans sa forme actualisée), ainsi que les lois applicables en matière de traitement des données de tout État devenant par la suite membre de l'Union européenne.

1.3 Le « **RGPD** » est le « RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ».

1.4 La « **BDSG** » est la loi fédérale allemande relative à la protection des données.

1.5 Les « **Données personnelles** » ont la même définition que celle présente dans la BDSG / le RGPD.

2 Objet du traitement de données / obligations du Demandeur

2.1 Le présent contrat régit les obligations des Parties en lien avec le traitement des Données personnelles du Demandeur par le Sous-Traitant dans le cadre du Contrat principal évoqué à l'annexe 1.

2.2 L'objet, la durée, le type et l'objectif du traitement, le type de Données personnelles, les catégories de personnes concernées et les droits et devoirs du responsable découlent de l'annexe 1 du présent Contrat et des descriptions de prestations du Contrat principal.

2.3 Le Demandeur reste responsable au sens du RGPD et garantit la légitimité du traitement des Données personnelles des individus concernés (chauffeurs et, le cas échéant, autres personnes). À cet égard, le Demandeur remplit en particulier son devoir étendu d'information et s'assure qu'il existe une base juridique en matière de protection des données pour le traitement des Données personnelles (p. ex. conclusion d'un accord avec l'employeur, limitation du traitement pour la relation de travail).

3 Devoirs du Sous-traitant

3.1 Le Sous-traitant traite des Données personnelles du Demandeur uniquement pour les objectifs décrits à l'annexe 1 et dans le cadre du Contrat principal, ainsi que pour le compte de et selon les instructions du Demandeur telles que documentées à l'annexe 1. En vertu du présent Contrat, le Sous-traitant ne peut traiter les Données personnelles pour aucun autre objectif. Cela ne porte pas atteinte au traitement hors du cadre du présent Contrat à des fins propres selon le point 8.3.4 du Contrat principal. Les copies ou duplicata de Données personnelles ne peuvent être faits à l'insu du Demandeur. Les copies de sécurité, pour autant qu'elles soient nécessaires à un traitement des données en bonne et due forme, ainsi que les données nécessaires pour le respect d'obligations de conservation juridiques, constituent une exception à cette condition.

3.2 Après la prestation de service, le Sous-traitant dispose de toutes les Données personnelles du Demandeur et doit, selon le choix du Demandeur, soit les lui remettre soit les détruire conformément aux lois en matière de protection des données, pour autant que les délais légaux de conservation prévus ne s'y opposent pas et pour autant que le Sous-traitant ne les traite pas à des fins propres hors du cadre prévu par le présent Contrat selon le point 8.3.4 du Contrat principal. Cela s'applique également à tout

matériau de test ou de rebut. La destruction ou la remise complète des données au Demandeur est à confirmer par écrit auprès de ce dernier à sa demande avec énoncé de la date.

3.3 Dans la mesure où la gamme de prestation le prend en compte, le Sous-traitant assiste le Demandeur lorsqu'il remplit les droits des personnes concernées (information, rectification, opposition, effacement) d'après l'instruction correspondante du Demandeur.

3.4 Le Sous-traitant confirme qu'il a désigné un délégué d'entreprise à la protection des données, si requis par la loi (voir l'article 38 de la BDSG / l'article 37 du RGPD).

3.5 Le Sous-traitant s'engage à communiquer immédiatement au Demandeur les résultats des contrôles des autorités de protection des données, pour autant que ceux-ci soient en rapport avec le traitement des données du Demandeur. Le Sous-traitant résout toute réclamation constatée dans un délai raisonnable et en informe le Demandeur.

3.6 Le traitement des données par le Sous-traitant et par les sous-traitants de deuxième niveau autorisés par le Demandeur se fait uniquement sur le territoire de la République fédérale d'Allemagne, dans un État membre de l'Union européenne ou dans un autre État signataire de l'accord sur l'Espace économique européen. Toute délocalisation dans un autre pays (ci-après « **État tiers** ») nécessite l'approbation expresse préalable du Demandeur et ne peut avoir lieu que si les conditions particulières à l'exportation de données dans un État tiers sont remplies (voir les articles 40 et suivants du RGPD). À cet effet, les indications présentes à l'annexe 1 sont nécessaires et des documents (contractuels) supplémentaires doivent être joints, le cas échéant.

3.7 Le Sous-traitant doit faire en sorte que le personnel chargé de l'exécution des travaux soit familiarisé avec les dispositions pertinentes en matière de protection des données et il doit de plus les soumettre à une obligation de confidentialité des données (voir article 28 du RGPD, al. 3 b). Il doit également s'assurer au moyen de mesures appropriées que chaque employé ne traite les Données personnelles que sur instruction du Demandeur.

3.8 Pendant toute la durée du Contrat, le Sous-traitant contrôle régulièrement que les prescriptions applicables en matière de protection des données du présent Contrat, ainsi que les instructions documentées du Demandeur sont bien observées. Les résultats de ces contrôles doivent être présentés au Demandeur à sa demande, pour autant que ceux-ci soient pertinents pour le traitement des données du Demandeur. Les mesures prises pour assurer une telle surveillance sont décrites dans un programme de protection des données à présenter au Demandeur à sa demande.

3.9 En tenant compte de la nature du traitement et si possible en recourant à des mesures techniques et organisationnelles adaptées, le Sous-traitant doit soutenir le Demandeur dans l'accomplissement de son devoir de réponse aux demandes d'exercice des droits de la personne concernée visés au chapitre III du RGPD. Le Demandeur doit alors supporter les coûts encourus par le Sous-traitant.

3.10 En tenant compte de la nature du traitement et des informations à sa disposition, le Sous-traitant doit aider le Demandeur à observer les devoirs visés aux articles 32 à 36 du RGPD.

4 Mesures techniques et organisationnelles en matière de sécurité des données

4.1 Le Sous-traitant prend des mesures techniques et organisationnelles adaptées à la protection des données (voir article 32 du RGPD). Le Sous-traitant est notamment obligé de mettre en œuvre les mesures techniques et organisationnelles convenues contractuellement à l'annexe 2 du présent Contrat. Tout au long des relations contractuelles, le Sous-traitant doit adapter ces mesures aux développements techniques et organisationnels futurs sans que le niveau de protection baisse. Les modifications majeures doivent faire l'objet d'un accord écrit.

4.2 À la demande du Demandeur, le Sous-traitant doit lui prouver que les mesures techniques et organisationnelles sont effectivement appliquées.

4.3 Le Sous-traitant est dans l'obligation d'entretenir une documentation adaptée sur le traitement des données que le Demandeur peut utiliser pour prouver que le traitement des données se fait en bonne et due forme. La preuve peut également être fournie par un mécanisme de certification autorisé conformément à l'article 42 du RGPD.

5 Sous-traitant de deuxième niveau

5.1 Le Sous-traitant est par la présente autorisé à recourir aux services des sous-traitants de deuxième niveau nommés à l'annexe 1.

5.2 Le recours à d'autres sous-traitants de deuxième niveau est par la présente autorisé, de manière générale. Cependant, le Sous-traitant informe le Demandeur de tout changement envisagé en ce qui concerne le recours à des sous-traitants de deuxième niveau ou leur remplacement. Le Demandeur peut s'opposer aux changements envisagés. De telles prestations de services fournies par des tiers auxquels le Sous-traitant peut faire appel pour fournir des prestations accessoires afin de l'aider dans l'exécution du présent Contrat ne peuvent être interprétées comme étant un contrat de sous-traitance en vertu du présent règlement. Cela porte par exemple sur les services de télécommunications, les équipes de nettoyage, les auditeurs ou les services de destruction des supports de données. Le Sous-traitant est cependant dans l'obligation de prendre des mesures de contrôle, ainsi que de conclure des accords contractuels, légalement conformes et adaptés, afin d'assurer la protection et la sécurité des données du Demandeur même dans le cas de recours à des prestations accessoires confiées à des tiers.

5.3 Dans le cas où il ferait appel à un sous-traitant de deuxième niveau, le Sous-traitant doit faire en sorte que ce sous-traitant de deuxième niveau se soumette aux mêmes devoirs de protection des données auxquels le Sous-traitant se soumet en vertu du présent Contrat, et ce au moyen (i) d'un contrat conclu

entre le sous-traitant de deuxième niveau et le Sous-traitant ou (ii) d'autres instruments juridiques indiqués par le Droit européen en matière de protection des données. Le Sous-traitant doit notamment s'assurer que le sous-traitant de deuxième niveau offre suffisamment de garanties commerciales pour que les mesures techniques et organisationnelles adaptées puissent être mises en œuvre de façon à ce que le traitement des Données personnelles se fasse conformément aux dispositions de la BDSG / du RGPD. Sur demande écrite du Demandeur, le Sous-traitant lui communique des informations sur les points principaux du contrat et sur la mise en œuvre des obligations relatives à la protection des données dans la relation contractuelle avec le sous-traitant de deuxième niveau, si besoin en lui donnant accès aux documents contractuels. Dans un tel cas, le Sous-traitant peut noircir les conditions commerciales. Le Demandeur est tenu de garder secrètes les informations obtenues.

6 Droits de contrôle

6.1 Le Demandeur a le droit de contrôler ou de faire contrôler par lui-même ou par un tiers adapté nommé par lui que les engagements découlant du présent Contrat (en ce compris les instructions données) sont bien respectés.

6.2 Le Sous-traitant garantit au Demandeur un soutien raisonnable lors des contrôles. Le Sous-traitant garantit notamment au Demandeur un accès aux installations de traitement des données et lui communique les renseignements nécessaires.

6.3 Dans le cas où un contrôle aboutirait à la conclusion que le Sous-traitant et/ou le traitement ne respectent pas les modalités du présent Contrat et/ou les dispositions du Droit européen en matière de protection des données, le Sous-traitant prend toutes les mesures correctives nécessaires afin de s'assurer que les modalités du présent Contrat et/ou les dispositions du Droit européen en matière de protection des données sont respectées.

6.4 Les coûts encourus par le Demandeur résultant de l'exécution d'un contrôle sont à sa charge. Le Sous-traitant peut réclamer au Demandeur le remboursement de tout coût encouru par lui et résultant de l'exécution d'un contrôle par le Demandeur, pour autant que ce dernier fasse ou fasse faire plus d'un contrôle par année civile.

6.5 Les contrôles du Sous-traitant doivent être annoncés en temps opportun et ne peuvent pas perturber de façon disproportionnée l'activité commerciale du Sous-traitant.

7 Obligations d'information

Lorsque, de l'avis du Sous-traitant, une instruction donnée par le Demandeur enfreint le Droit européen en matière de protection des données, le Sous-traitant en informe immédiatement le Demandeur. Toute instruction mise en cause avec raison ne doit pas être suivie tant qu'elle n'est pas modifiée ou

expressément confirmée par le Demandeur. Le Sous-traitant n'est pas tenu de procéder à un examen approfondi des instructions.

Le Sous-traitant doit informer le Demandeur immédiatement et de façon adéquate s'il détecte des erreurs ou des irrégularités dans le traitement des données ou s'il soupçonne une infraction à la protection des données (collectivement dénommés ci-après « **Incident** »). Le Sous-traitant doit documenter l'Incident, les circonstances de l'Incident, ses conséquences et l'ensemble des mesures de réparation, et remettre immédiatement ces informations au Demandeur à sa demande, par voie postale ou par voie électronique.

8 Responsabilité et exonération

8.1 Le Sous-traitant est responsable de tout dommage causé par une intention délibérée et/ou une grande négligence de sa part ou de celle de ses aides-auxiliaires. Pour les dommages résultant d'une négligence simple du Sous-traitant ou d'un de ses aides auxiliaires, le Sous-traitant n'est responsable que dans les cas de violation d'une obligation majeure. Les obligations majeures sont des obligations contractuelles importantes qui permettent l'exécution en bonne et due forme du contrat et au respect desquelles le Demandeur pouvait légitimement s'attendre. Dans le cas d'une négligence simple concernant une violation de telles obligations majeures, la responsabilité du Sous-traitant est limitée aux dommages habituellement prévisibles.

8.2 Le Demandeur exonère le Sous-traitant de toute réclamation de tiers (y compris de personnes concernées et/ou d'autorité en matière de protection des données), de tout dommage et de tout coût résultant d'une violation par le Demandeur d'une modalité du présent Contrat et/ou d'une disposition du Droit européen en matière de protection des données. Dans le cas où le Demandeur n'est pas responsable d'une telle violation ou si le Sous-traitant a contribué à une telle violation, la présente modalité ne s'applique pas.

9 Durée

La durée du présent Contrat correspond à la durée du Contrat principal. La résiliation du Contrat principal, pour toute raison que ce soit, provoque la résiliation automatique du présent Contrat. Cela n'affecte pas le droit de résiliation extraordinaire.

10 Divers

10.1 Les prestations du Sous-traitant en vertu du présent du Contrat sont rémunérées selon la politique de rémunération définie dans le Contrat principal.

10.2 Dans le cas où les Données personnelles du Demandeur conservées par le Sous-traitant seraient menacées par les mesures d'un tiers (par une saisie ou une confiscation, par exemple), par une insolvabilité ou par un processus comparable ou par d'autres évènements du même genre, le Sous-traitant doit en informer le Demandeur au plus tôt.

10.3 Dans le cas où certaines modalités du présent Contrat seraient ou deviendraient caduques, ceci ne porte aucunement préjudice à la validité des autres modalités du Contrat. En cas de nullité d'une clause, les Parties conviennent d'un règlement de remplacement cohérent vis-à-vis de l'objectif du présent contrat, tant sur le fond que d'un point de vue économique.

10.4 Dans le cas d'un retrait du Royaume-Uni de l'Union européenne, le Sous-traitant s'engage dès maintenant à conclure tout accord et à entreprendre toute négociation nécessaires afin d'organiser le traitement des données faisant l'objet du présent Contrat au Royaume-Uni, à compter de son retrait de l'Union européenne, et ce, conformément au droit en matière de protection des données. Si, au moment du retrait du Royaume-Uni, la Commission européenne n'a pris aucune décision relative à l'adéquation du niveau de protection des données, des clauses de protection des données standard du point de vue actuel s'appliquent conformément à l'article 46 paragraphe 2 c) portant sur la transmission de Données personnelles à un sous-traitant installé dans un pays tiers dans lequel un niveau raisonnable de protection des données n'est pas garanti.

Si le Sous-traitant ne remplit pas ces obligations, le Demandeur est autorisé à exiger du Sous-traitant, à compter du retrait du Royaume-Uni de l'Union européenne, que les prestations concernées soient fournies par une filiale ou une partie de l'entreprise ayant un siège permanent sur le territoire de l'Union européenne, sans que le Demandeur encoure de frais ou de coûts supplémentaires.

10.5 Le présent Contrat de sous-traitance du traitement est disponible en 18 langues, la version originale allemande prévalant en cas de divergence.

10.6 Le présent Contrat est régi par les lois de la République fédérale d'Allemagne, à l'exclusion de la convention des Nations unies sur les contrats de vente internationale de marchandises. Le seul tribunal compétent est celui de Munich.

10.7 Les annexes suivantes constituent des parties intégrantes au contrat :

Annexe 1 : description du traitement réalisé par un sous-traitant
Annexe 2 : mesures techniques et organisationnelles

ANNEXE 1 : description du traitement réalisé par un sous-traitant

1 Contrat principal

Les « Conditions-cadres générales de l'utilisation de la plateforme » constituent le Contrat principal au sens de l'article 2.1 de la partie principale du présent Contrat.

Titre / parties : **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19 – 21, 80807 Munich / **Utilisateur**

2 Objet et durée du Contrat

L'objet du Contrat se fonde sur les points 1 (*Objet*) et 8 (*Données de l'utilisateur et protection des données*) du Contrat principal ; la durée du Contrat se fonde sur le point 7 (*Conclusion et durée du contrat et droit de résiliation*) du Contrat principal.

3 Étendue, type et objectif du traitement des données / des mesures de traitement des données

L'étendue, le type et l'objectif du traitement des Données personnelles ressortent du point 8 du Contrat principal.

Description plus précise de l'objet du contrat du point de vue de l'étendue, du type et de l'objectif :

Afin que le Sous-traitant puisse fournir les services proposés (tels que définis dans le Contrat principal), il doit collecter les Données personnelles du Demandeur au sujet des véhicules connectés ou des appareils mobiles (et, le cas échéant, les Données personnelles transmises à un fournisseur tiers avec lequel l'utilisateur a conclu un accord de prestation de services externes) dans les quantités nécessaires à l'exécution des services, les transférer sur sa plateforme et les y stocker. Le Sous-traitant traite les données stockées sur la plateforme et en traite autant que nécessaire pour la prestation des services (en quantité suffisante pour pouvoir analyser et évaluer le comportement routier des chauffeurs, ainsi que l'utilisation du véhicule connecté ou de l'appareil mobile au moyen de Données personnelles, et pour pouvoir soumettre au Demandeur des offres sur mesure en se basant sur ces analyses et ces évaluations, comme des entraînements à la conduite, des détails d'équipements, ainsi que des propositions visant à améliorer le rendement). L'étendue, le type et l'objectif du traitement découlent donc notamment des contrats distincts supplémentaires encore à conclure.

4 Cercle des concernés (catégories des personnes concernées)

Les cercles de personnes suivants sont concernés par le traitement réalisé par un sous-traitant :

- **les chauffeurs et autres employés** (employés de la propre société du Demandeur), par exemple les employés, apprentis, candidats, anciens employés ;

- **les chauffeurs** qui ne sont pas des employés ;
- **les personnes de contact** des chargeurs / déchargeurs ou d'autres partenaires professionnels du Demandeur ;
- **les employés du groupe** (les employés d'une autre entreprise du groupe du Demandeur).

5 Type des Données personnelles

Le traitement réalisé par un sous-traitant porte sur les types de Données personnelles suivants :

- nom du chauffeur et n° d'identification du chauffeur ;
- n° d'identification du véhicule ;
- données de site ;
- données sur le temps de conduite et de repos ;
- données sur le comportement routier ;
- données d'état du véhicule connecté ;
- données d'état du semi-remorque ;
- données d'état du montage et du démontage, des organes mécaniques et d'autres composants du véhicule ;
- données d'état des appareils IOT connectés, le cas échéant ;
- données d'état des appareils mobiles ;
- données de chargement ;
- données de commande ;
- coordonnées des personnes de contact des chargeurs / déchargeurs ou d'autres partenaires professionnels du Demandeur.

6 Instructions documentées

Par la présente, le Demandeur donne au Sous-traitant l'instruction de traiter les Données personnelles de la façon énoncée au point 8 du Contrat principal. Cela inclut notamment les traitements suivants :

- Les Données personnelles sont transmises à la plateforme dans le cloud du Sous-traitant via le véhicule connecté ou l'appareil mobile et y sont stockées.
- En vertu du présent contrat, les Données personnelles ne sont traitées que dans la mesure nécessaire à l'exécution du Contrat principal ; le point 8.3.4 du Contrat principal reste inchangé.
- Le Sous-traitant transmet les Données personnelles à un fournisseur tiers (tel que défini dans le Contrat principal), dans la mesure où un tel transfert à un fournisseur tiers est nécessaire afin que ce dernier puisse fournir ses services externes (tels que définis dans le Contrat principal) au Demandeur.
- Le Sous-traitant analyse et évalue le comportement routier des chauffeurs, ainsi que l'utilisation du véhicule connecté au moyen des Données personnelles et, en se basant sur cela, soumet au Demandeur

des offres sur mesure, par exemple des entraînements à la conduite, des détails d'équipements ou encore des propositions visant à améliorer le rendement.

7 Lieux du traitement

- Allemagne.
- Royaume-Uni ; dans le cas où des données sont traitées dans l'Union européenne à des fins d'hébergement et/ou d'assistance informatiques, des contrats de sous-traitance du traitement correspondants sont conclus.
- Dans le cas où le Sous-traitant fait appel à des sous-traitants de deuxième niveau établis en-dehors de l'Union européenne à des fins d'hébergement et/ou d'assistance informatiques (voir à ce sujet le point 8 de la présente annexe 1), le transfert de Données personnelles se fait selon les clauses de contrat standard / les clauses de protection des données standard conclues entre le Sous-traitant et le sous-traitant de deuxième niveau et portant sur la transmission des Données entre le Sous-traitant et le sous-traitant de deuxième niveau et portant sur la transmission des Données personnelles à un sous-traitant installé dans un pays tiers selon l'article 46, alinéa 2 c) du RGPD.

8 Sous-traitant de deuxième niveau

Le Sous-traitant engage les sous-traitants de deuxième niveau suivants (qui peuvent également engager des sous-traitants de troisième niveau supplémentaires, le cas échéant) :

N°	Sous-traitant de deuxième niveau (société, adresse, personne de contact)	Catégories de données traitées	Étape du traitement / objectif de la sous-traitance de deuxième niveau du traitement
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, États-Unis d'Amérique	Ensemble des Données personnelles de la plateforme en lien avec une partie de vente (c.-à-d. où un client peut s'inscrire sur la plateforme et passer des commandes)	Hébergement de la plateforme
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, États-Unis d'Amérique	Ensemble des Données personnelles de la plateforme en lien avec une partie de vente (c.-à-d. où un client peut s'inscrire sur la plateforme et passer des commandes)	Assistance informatique pour la plateforme
3	Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 États-Unis d'Amérique https://aws.amazon.com/de/compliance/contact/	Ensemble des autres données d'utilisateur personnelles transmises par le véhicule au Sous-traitant	Hébergement de la plateforme / assistance informatique pour la plateforme
4	Remplace le cas échéant le n° 3 : Amazon Webservices (EU) Amazon Web Services, Inc. P.O. Box 81226 Seattle, WA 98108-1226 États-Unis d'Amérique https://aws.amazon.com/de/compliance/contact/	Ensemble des autres données d'utilisateur personnelles transmises par le véhicule au Sous-traitant	Hébergement de la plateforme
5	MAN Service und Support GmbH Dachauer Straße 667	Ensemble des Données personnelles nécessaires au traitement des demandes des	1er niveau d'assistance

	80995 Munich Allemagne	clients dans le cadre du 1er et du 2e niveau d'assistance	
6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 États-Unis d'Amérique	Ensemble des Données personnelles nécessaires au traitement des factures / des commandes	Hébergement de la plateforme Locataire venant de l'Union européenne : hébergé par Amazon Web Services (EU), voir point 4
7	MAN Truck & Bus AG Dachauer Str. 667 80995 Munich Allemagne	Ensemble des autres Données personnelles d'utilisateur transmises au Sous-traitant par le véhicule connecté et/ou l'appareil mobile.	Hébergement de la plateforme
8	T-Systems International GmbH Hahnstraße 43 d 60528 Francfort-sur-le-Main Allemagne	Ensemble des autres Données personnelles d'utilisateur transmises au Sous-traitant par le véhicule TBM1/2	Hébergement de la plateforme
9	Scania AB Vagnmakarvägen 1 15187 Södertälje Suède	Ensemble des autres données d'utilisateur personnelles transmises par le véhicule au Sous-traitant	Hébergement de la plateforme
10	Volkswagen Nutzfahrzeuge Mecklenheidestr. 74 30419 Hanovre Allemagne	Ensemble des autres données d'utilisateur personnelles transmises par le véhicule au Sous-traitant	Hébergement de la plateforme

ANNEXE 2 : mesures techniques et organisationnelles

Les mesures techniques et organisationnelles que le Sous-traitant doit prendre afin de garantir un niveau de protection adapté aux risques sont décrites dans le programme de protection des données de la plateforme RIO et comprennent notamment :

1. Pseudonymisation

Dans le cas où les Données personnelles sont utilisées à des fins d'évaluation, ce qui est également réalisable avec des données pseudonymisées, des techniques de pseudonymisation sont employées. Pour ce faire, il faut déterminer à l'avance pour chaque champ de donnée s'il doit être pseudonymisé, car il permettrait d'identifier la personne à laquelle se rapportent les données qu'il contient. Les clés de pseudonymisation sont stockées dans un « coffre pour données » pour lequel le maximum de restrictions d'accès est paramétré.

2. Cryptage

Les terminaux mobiles et le serveur communiquent de façon cryptée à l'aide d'un certificat propre à chaque dispositif. Sur la plateforme RIO, les données sont transportées de façon cryptée (« Ubiquitous encryption » ou « encryption everywhere » [cryptage en tout lieu]).

3. Garantie de confidentialité

Tous les employés sont avertis de leur devoir de confidentialité et s'engagent par écrit à respecter la confidentialité des données.

Les infrastructures informatiques utilisées sont mises à disposition via Amazon Web Services (ci-après AWS) dans le cadre d'un cloud (IaaS et PaaS). L'opérateur du centre de données AWS met à disposition un contrôle des accès : les centres de données AWS, hautement sécurisés, utilisent des mesures de surveillance électroniques à la pointe de la technologie et des systèmes de contrôle d'entrée à plusieurs étapes. Les centres de données sont gardés 24 h / 24 par du personnel de sécurité entraîné et l'accès n'est permis que selon le principe de séparation des privilèges et uniquement à des fins d'administration du système.

L'accès aux composants matériels (clients) de la société TB Digital Services GmbH n'est possible que conformément aux mesures standard en vigueur adaptées à chaque cas particulier. Ces mesures sont, par exemple, des restrictions d'accès par des installations de séparation (des tourniquets), des installations de surveillance vidéo, des installations d'alarme et/ou des services de surveillance, des portes avec des sécurités électriques ou mécaniques, des bâtiments antieffraction, des autorisations d'accès documentées (visiteur, tiers) ou des zones de sécurité déclarées.

Les contrôles d'accès comprennent des mesures permettant de garantir la sécurité des appareils, du réseau et des applications.

Plusieurs mesures sont mises en œuvre afin de garantir la sécurité des appareils présents dans un véhicule : les terminaux mobiles sont intégrés au véhicule de manière fixe et disposent du système Secure Boot, ce qui signifie qu'il est impossible de charger et d'exécuter un système d'exploitation étranger. Les terminaux mobiles et le serveur communiquent de façon cryptée à l'aide d'un certificat propre à chaque dispositif. Sur la plateforme RIO, les Données sont transportées de façon cryptée (« Ubiquitous encryption » ou « encryption everywhere » [cryptage en tout lieu]). Des mises à jour de sécurité sont régulièrement installées sur les terminaux mobiles, afin qu'ils disposent d'un niveau de sécurité à jour (gestion des patchs).

De la même manière, plusieurs mesures standard sont mises en œuvre afin de garantir la sécurité du réseau : Des prescriptions concernant les mots de passe adaptées (à la pointe de la technologie) sont implémentées (longueur, complexité, durée de validité du mot de passe, etc.). Une deuxième erreur dans la saisie de la combinaison identifiant / mot de passe conduit à un blocage (temporaire) de l'identifiant. Le réseau de l'entreprise est séparé des réseaux ouverts non sécurisés au moyen d'un pare-feu. Une procédure visant à assurer la fourniture régulière de mises à jour de sécurité aux périphériques mobiles est établie (procédure OTA). Des technologies adaptées (comme des systèmes de détection d'intrusion) sont mises en place afin de détecter et d'éviter toute attaque sur le réseau d'entreprise (l'Intranet). Les employés sont régulièrement sensibilisés aux risques et aux dangers.

Plusieurs mesures standard sont mises en œuvre afin de garantir la sécurité de l'application :

Les applications concernées sont protégées contre les accès non autorisés par des mécanismes d'authentification et d'autorisation adaptés. Des prescriptions concernant les mots de passe adaptées (à la pointe de la technologie) sont implémentées (longueur, complexité, durée de validité du mot de passe, etc.). Pour une application dont les besoins en sécurité sont particulièrement élevés, des mécanismes d'authentification avancés sont utilisés (par exemple par token ou à PKI). Une deuxième erreur dans la saisie de la combinaison identifiant / mot de passe conduit à un blocage (temporaire) de l'identifiant. Les données utilisées dans les processus concernés sont affichées sous format crypté sur un support de données mobiles. Les accès autorisés et les tentatives d'accès à l'application sont enregistrés. Les fichiers journaux produits sont conservés pendant un délai approprié (d'un minimum de 90 jours) et sont contrôlés (aléatoirement).

Les autorisations utilisateur (pour l'accès) sont sécurisées au moyen de différentes mesures et associées fondamentalement à une personne identifiable. L'attribution des autorisations relève de la responsabilité des personnes responsables de la plateforme et est régulièrement contrôlée. L'attribution des autorisations d'accès ne se fait qu'au terme d'un processus défini et documenté. Les modifications aux autorisations d'accès ne se font qu'au terme d'une vérification à double contrôle et sont documentées dans un historique avec numéro de version.

Plusieurs mesures sont mises en œuvre afin de contrôler l'accès aux applications : Les droits d'accès sont définis et documentés dans le cadre d'un programme des rôles / des autorisations et sont attribués en fonction des besoins inhérents à chaque poste. Des rôles / autorisations spécifiques sont configurés pour les administrateurs techniques (qui ne permettent aucun accès aux Données personnelles, dans la mesure du possible). Des rôles /

autorisations spécifiques sont configurés pour l'assistance technique (qui ne comprennent aucun droit d'administration technique).

La définition des rôles / des autorisations et leur attribution ne sont pas faites par les mêmes personnes, pour autant que ce soit possible aux points de vue techniques et organisationnels, mais se font par une procédure (d'autorisation) sécurisée et sont limitées dans le temps. Les accès directs à la banque de données qui contournent les programmes d'autorisations et de rôles ne sont possibles que par les administrateurs de banques de données autorisés. Il y a un règlement concernant l'utilisation de supports de stockage privés ou bien l'utilisation de supports de stockage privés est interdite. Il existe des règlements contraignants concernant l'accès aux données pour des entretiens externes, des télémaintenances et du télétravail. Une destruction / élimination des documents et des supports de stockage conforme à la législation en matière de protection des données par des sociétés d'élimination fiables est prévue (par exemple avec une déchiqueteuse ou par des conteneurs sécurisés).

Le programme des rôles / des autorisations est régulièrement adapté aux structures changeantes de l'organisation du travail (par exemple en créant de nouveaux rôles) et les rôles / autorisations attribués sont régulièrement contrôlés (par exemple par les superviseurs) et, au besoin, adaptés ou retirés. Un contrôle central régulier a lieu envers les profils standard attribués. Les accès en écriture (écriture, suppression) sont enregistrés et les fichiers journaux produits sont conservés pendant un délai approprié (d'un minimum de 90 jours) et contrôlés (aléatoirement).

Plusieurs mesures générales sont mises en œuvre afin de garantir la sécurité de la transmission des données :

les personnes chargées de la transmission sont, au préalable, informées des mesures de sécurité à prendre. Le cercle des destinataires est établi à l'avance afin qu'un contrôle adapté (une authentification) soit possible. L'ensemble du processus de transmission des données est fixé et documenté et la mise en application effective du transfert de données est enregistrée et documentée (par exemple avec un accusé de réception ou un reçu). Les personnes chargées de la transmission procèdent au préalable à un contrôle de plausibilité, d'intégralité et d'exactitude.

Avant de procéder effectivement au transfert des données, l'adresse du destinataire est contrôlée (par exemple, son adresse électronique). La transmission des données via Internet se fait en un format crypté (par exemple en cryptant les fichiers). L'intégrité des données transmises est garantie par l'utilisation d'un processus de signature (de signature numérique), pour autant que ce soit techniquement possible. Les accusés de réception électroniques sont archivés sous un format approprié. Les transferts de données indésirables effectués par Internet sont interrompus au moyen de technologies appropriées (comme un proxy ou un pare-feu).

En outre, plusieurs mesures standard sont mises en œuvre afin de garantir l'application du principe de séparation :

Il existe des règlements contraignants au sujet du respect du principe de séparation en ce qui concerne l'affectation du traitement. Les données collectées dans un but précis sont stockées de façon à être séparées des données collectées pour un autre objectif. Les systèmes informatiques utilisés permettent un stockage séparé des données (selon un principe multientité ou des concepts d'accès). Cela permet de séparer les données dans les systèmes de production et de test. En ce qui concerne les données pseudonymisées, la clé de pseudonymisation permettant de réidentifier les données est sauvegardée et séparée séparément. Le Sous-traitant doit séparer les données venant de différents demandeurs lorsqu'il sous-traite des traitements ou qu'une fonction lui est déléguée. Par leur structure, les programmes de rôles et d'autorisation en place permettent une séparation logique des données traitées.

4. Garantie d'intégrité

Plusieurs mesures standard sont mises en œuvre afin de mettre en place l'enregistrement des saisies :

Les modifications aux droits d'accès ainsi que l'ensemble des activités d'administration sont enregistrés. Les accès en écriture (pour des saisies, des modifications, des suppressions) et les modifications aux champs de données sont enregistrés (par exemple, le contenu d'un ensemble de données nouvellement saisi ou modifié). Les transmissions (comme les téléchargements) et les connexions sont enregistrées.

Les documents d'enregistrements utilisés sont documentés et archivés afin d'assurer la traçabilité des saisies. L'enregistrement comprend la date, l'heure, l'utilisateur, le type d'activité, le programme d'application et le numéro de dossier de l'ensemble de données. Les paramètres d'enregistrement sont documentés.

Il n'est possible d'accéder aux fichiers journaux qu'en lecture seule. Le cercle des personnes disposant d'une autorisation d'accès aux fichiers journaux est très restreint (en se limitant, par exemple, à l'administrateur, au délégué à la protection des données et au réviseur). Les fichiers journaux sont conservés pendant une période de temps convenue (par exemple 1 an) et sont ensuite détruits de façon conforme aux lois en matière de protection des données. Les fichiers journaux sont régulièrement analysés, de façon automatique. Les analyses des fichiers journaux sont effectuées sur des données pseudonymisées, si possible.

5. Garantie de disponibilité

L'architecture est intrinsèquement protégée contre les pertes de données par les mécanismes de réplication internes à la plateforme AWS. En outre, les mesures standard d'AWS suivantes sont mises en œuvre afin de garantir la sécurité de l'installation :

Des mesures de protection contre les incendies sont implantées (comme des portes coupe-feu, des détecteurs de fumée, des murs coupe-feu, une interdiction de fumer, etc.). Les installations informatiques sont protégées contre les inondations (par exemple en les installant au premier étage, en installant des détecteurs à eau). Des mesures de protection contre les vibrations sont mises en œuvre (par exemple en évitant d'installer la salle informatique à proximité d'une autoroute, de voies de chemin de fer ou de salles machines). Les installations

informatiques sont protégées contre les champs électromagnétiques (par des plaques d'acier dans les murs extérieurs, par exemple). Des mesures contre le vandalisme et le vol sont implémentées (voir contrôles d'entrée). Les installations informatiques se trouvent dans des espaces climatisés (la température et l'humidité de l'air sont réglées par la climatisation). Les installations informatiques sont protégées contre les pointes de surtension par une protection contre les surcharges. Des mesures sont mises en place afin d'assurer une alimentation électrique continue et sans dérangement (comme une unité d'alimentation sans coupure ou des groupes électrogènes).

Les inventaires de données font l'objet de sauvegardes de sécurité régulières sur la plateforme AWS. Le programme de sauvegarde de sécurité est documenté et est régulièrement revu et actualisé. Les supports de sauvegarde sont protégés contre tout accès non autorisé. Les programmes de sauvegarde utilisés correspondent aux standards de qualité actuels et, à cette fin, ils sont régulièrement mis à jour. Un centre de données redondant (éloigné du lieu de traitement) est mis en place afin de pouvoir poursuivre le traitement des données en cas de catastrophe. Les différentes mesures pour le contrôle des disponibilités sont décrites dans un plan de gestion en cas d'urgence d'AWS.

Avant qu'une mission de traitement de données soit attribuée, le Sous-traitant est soigneusement contrôlé selon des critères bien définis (mesures techniques et organisationnelles). À cette fin, le Sous-traitant doit présenter de façon détaillée les mesures techniques et organisationnelles de protection des données mises en place (en répondant à un questionnaire ou en présentant un programme de protection des données). Cette présentation est ensuite examinée. Indépendamment de la quantité et de la sensibilité des données traitées, ce contrôle peut se faire dans les locaux du Sous-traitant, le cas échéant. La possession d'une certification appropriée (par exemple de la norme ISO 27001) est prise en compte dans le choix des Sous-traitants. La détermination de l'aptitude du Sous-traitant est documentée de façon adaptée et compréhensible.

La relation contractuelle entre le Demandeur et le Sous-traitant est établie par la conclusion d'un contrat de sous-traitance du traitement. Ce contrat détermine par écrit de façon détaillée les compétences, les responsabilités et les devoirs des deux Parties. Dans le cas où le siège d'un fournisseur de services se situe en dehors de l'Union européenne ou de l'Espace économique européen, les clauses contractuelles types de l'UE sont utilisées. Il est contractuellement établi que le traitement des données par le Sous-traitant ne peut se faire que selon les instructions données par le Demandeur. Lorsque, de l'avis du Sous-traitant, une instruction du Demandeur enfreint les prescriptions légales en matière de protection des données, le Sous-traitant doit immédiatement en avertir le Demandeur. Afin de respecter les droits des personnes concernées, le contrat de sous-traitance du traitement stipule que le Sous-traitant doit apporter son aide au Demandeur, par exemple dans le cas où ce dernier serait obligé de partager des informations avec des personnes concernées.

Par après dans le traitement réalisé par un sous-traitant, le Demandeur contrôle les résultats du Sous-traitant, tant sur la forme que sur le fond. Le respect des mesures techniques et organisationnelles prises par le Sous-traitant est contrôlé régulièrement. À cette fin, les méthodes privilégiées sont la présentation d'attestations véritables ou de certifications appropriées, ou encore la preuve d'audits de sécurité informatique ou de

protection des données. Dans le cas où il serait fait appel à un sous-traitant de deuxième niveau, le contrat stipule que ce dernier soit contrôlé de la même manière.

6. Garantie de la résistance du système

L'infrastructure de cloud AWS a été créée pour être l'un des environnements de cloud parmi les plus flexibles et sûrs qui soient. Il est conçu pour offrir une disponibilité maximale tout en étant totalement séparé du client. Il fournit une plateforme hautement dimensionnable et très fiable qui permet au client de diffuser mondialement applications et contenus de façon sûre et rapide si nécessaire. Les services AWS sont indépendants des contenus en ceci qu'ils offrent à tous les clients le même niveau élevé de sécurité, indépendamment du type de contenu ou de la région géographique dans laquelle le contenu est stocké.

Les centres de données AWS de niveau mondial, hautement sécurisés, utilisent des mesures de surveillance électroniques à la pointe de la technologie et des systèmes de contrôle d'entrée à plusieurs étapes. Les centres de données sont gardés 24 h / 24 par du personnel de sécurité entraîné et l'accès n'est permis que selon le principe de séparation des privilèges et uniquement à des fins d'administration du système.

7. Procédures pour le rétablissement de la disponibilité des Données personnelles suite à un incident physique ou technique

Les centres de données AWS sont installés en cluster dans différentes régions du monde. Tous les centres de données sont en ligne et offrent des services aux clients, aucun n'est désactivé. En cas de défaillance, des processus automatiques détournent le trafic des données clients loin des zones concernées. Les applications clés sont fournies selon une configuration N + 1 afin que, si jamais un incident se produit dans un centre de données, le système soit encore capable de répartir la charge du trafic de données entre les différents sites restants.

AWS permet de placer des instances et de sauvegarder des données dans plusieurs régions géographiques ainsi que dans plusieurs zones de disponibilités au sein d'une région. Chaque zone de disponibilité a été développée pour être une zone indépendante en cas de défaillance. Cela signifie que les zones de disponibilités au sein d'une région urbaine typique sont séparées physiquement et qu'elles se trouvent, par exemple, dans des zones présentant un risque d'inondation faible (il existe différentes catégorisations des zones inondables en fonction des régions). En plus de disposer d'une alimentation électrique sans interruption et indépendante et d'avoir des générateurs de secours sur site, chaque zone de disponibilité est alimentée par différents réseaux électriques de différents fournisseurs de courants afin de minimiser les effets d'une panne seule. Toutes les zones de disponibilités sont reliées de façon redondante à plusieurs fournisseurs d'accès à Internet de niveau 1.

L'équipe Amazon en charge de la gestion des incidents utilise des procédures de diagnostic conformes aux standards du milieu afin de faire progresser la résolution d'incidents critiques pour une entreprise. Le personnel opérationnel est continuellement présent 24 h / 24, sept jours par semaine et 365 jours par an afin d'identifier les pannes, de gérer leurs impacts et de les réparer.

8. Procédures pour un contrôle et une évaluation réguliers de l'efficacité des mesures techniques et organisationnelles

Les directives et consignes actuelles de l'entreprise, ainsi que les normes implémentées sur la sécurité de l'information sont également utilisées pour ce qui est de l'introduction et l'exploitation de la plateforme RIO. Les fonctions opérationnelles pour la protection des données et la sécurité de l'information sont présentes (un responsable de la protection des données et un responsable de la sécurité de l'information). Les employés sont contraints à la confidentialité des données et informés des mesures de protection des données et sur la sécurité Internet au moyen de brochures, de flyers, d'informations présentes sur l'Intranet, etc.

Le respect par les processus internes des mesures techniques et organisationnelles se rapportant à la sécurité des données est contrôlé. Ce contrôle est composé de la révision, de la sécurité des informations et de la protection des données.

Les processus de traitement et les mesures de protection des données sont documentés dans un répertoire des activités de traitement. Des contrôles (internes et externes) de l'efficacité de ces mesures ont lieu régulièrement.