ANNEXE C : ACCORD DE TRAITEMENT DES DONNÉES (DPA) POUR LES SERVICES VDO FLEET ONLINE

Le présent Accord sur le traitement des données stipule les obligations légales des PARTIES en matière de protection des données résultant du traitement des données personnelles liées au contrat respectif concernant les SERVICES VDO FLEET et le Client. Le DPA suivant est basé sur les conditions contractuelles types officielles établies par la Commission européenne dans le cadre de la décision d'exécution (UE) 2021/915 de la Commission.
Le Client en tant que « responsable du traitement » CONTINENTAL AUTOMOTIVE TRADING FRANCE SAS en tant que « sous-traitant » conviennent de ce qui suit :

SECTION I

Clause 1

Objet et champ d'application

a) Les présentes clauses contractuelles types (ci-après les « clauses ») ont pour objet de garantir la conformité avec l'article 28, paragraphes 3 et 4, du 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.
b) Les responsables du traitement et les sous-traitants énumérés à l'annexe I ont accepté ces clauses afin de garantir le respect des dispositions de l'article 28, paragraphes 3 et 4, du règlement (UE) 2016/679 et/ou des dispositions de l'article 29, paragraphes 3 et 4, du règlement (UE) 2018/1725.
c) Les présentes clauses s'appliquent au traitement des données à caractère personnel tel que décrit à l'annexe II.
d) Les annexes I à IV font partie intégrante des clauses.
e) Les présentes clauses sont sans préjudice des obligations auxquelles le responsable du traitement est soumis en vertu du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.
f) Les clauses ne suffisent pas à elles seules pour assurer le respect des obligations relatives aux transferts internationaux conformément au chapitre V du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.

Clause 2

Invariabilité des clauses

a) Les Parties s'engagent à ne pas modifier les clauses, sauf en ce qui concerne l'ajout d'informations aux annexes ou la mise à jour des informations qui y figurent.
b) Les Parties ne sont pour autant pas empêchées d'inclure les clauses contractuelles types définies dans les présentes clauses dans un contrat plus large, ni d'ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses ou qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

Clause 3

Interprétation

a) Lorsque des termes définis respectivement dans le règlement (UE) 2016/679 ou dans le règlement (UE) 2018/1725 figurent dans les clauses, ils s'entendent comme dans le règlement en question.
b) Les présentes clauses doivent être lues et interprétées à la lumière des dispositions du règlement (UE) 2016/679 et du règlement (UE) 2018/1725 respectivement.
c) Les présentes clauses ne doivent pas être interprétées d'une manière contraire aux droits et obligations prévus par le règlement (UE) 2016/679 / le règlement (UE) 2018/1725 ou d'une manière qui porte atteinte aux libertés ou droits fondamentaux des personnes concernées.

Clause 4

Hiérarchie

En cas de contradiction entre les présentes clauses et les dispositions des accords connexes qui existent entre les Parties au moment où les présentes clauses sont convenues ou qui sont conclus ultérieurement, les présentes clauses prévaudront.

Clause 5

Clause d'amarrage

a) Toute entité qui n'est pas partie aux présentes clauses peut, avec l'accord de toutes les Parties, y adhérer à tout moment, en qualité soit de responsable du traitement soit de sous-traitant, en complétant les annexes et en signant l'annexe I.
b) Une fois que les annexes mentionnées au point a) sont complétées et signées, l'entité adhérente est considérée comme une partie aux présentes clauses et jouit des droits et est soumise aux obligations d'un responsable du traitement ou d'un sous-traitant, conformément à sa désignation à l'annexe I.
c) Les présentes clauses ne créent pour la partie adhérente aucun droit ni aucune obligation pour la période précédant l'adhésion.

SECTION II – OBLIGATIONS DES PARTIES

Clause 6
Description du ou des traitements

Les détails des opérations de traitement, et notamment les catégories de données à caractère personnel et les finalités du traitement pour lesquelles les données à caractère personnel sont traitées pour le compte du responsable du traitement, sont précisés à l'annexe II.

Clause 7
Obligation des parties

7.1. Instructions

a) Le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis. Dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si la loi le lui interdit pour des motifs importants d'intérêt public. Des instructions peuvent également être données ultérieurement par le responsable du traitement pendant toute la durée du traitement des données à caractère personnel. Ces instructions doivent toujours être documentées.
b) Le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction donnée par le responsable du traitement constitue une violation du règlement (UE) 2016/679 / du règlement (UE) 2018/1725 ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

7.2. Limitation de la finalité

Le sous-traitant traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du traitement, telles que définies à l'annexe II, sauf instruction complémentaire du responsable du traitement.

7.3. Durée du traitement des données à caractère personnel

Le traitement par le sous-traitant n'a lieu que pendant la durée précisée à l'annexe II.

7.4. Sécurité du traitement

a) Le sous-traitant met au moins en œuvre les mesures techniques et organisationnelles précisées à l'annexe III pour assurer la sécurité des données à caractère personnel. Figure parmi ces mesures la protection des données contre toute violation de la sécurité entraînante, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données (violation de données à caractère personnel). Lors de l'évaluation du niveau de sécurité approprié, les Parties tiennent dûment compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques pour les personnes concernées.
b) Le sous-traitant n'accorde aux membres de son personnel l'accès aux données à caractère personnel faisant l'objet du traitement que dans la mesure strictement nécessaire à l'exécution, à la gestion et au suivi du contrat. Le sous-traitant veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

7.5. Données sensibles

Si le traitement porte sur des données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, ou des données relatives aux condamnations pénales et aux infractions («données sensibles»), le sous-traitant applique des limitations spécifiques et/ou des garanties supplémentaires.

7.6 Documentation et conformité

a) Les Parties doivent pouvoir démontrer la conformité avec les présentes clauses.
b) Le sous-traitant traite de manière rapide et adéquate les demandes du responsable du traitement concernant le traitement des données conformément aux présentes clauses.
c) Le sous-traitant met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les présentes clauses et découlant directement du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725. À la demande du responsable du traitement, le sous-traitant permet également la réalisation d'audits des activités de traitement couvertes par les présentes clauses et y contribue, à intervalles raisonnables ou en présence d'indices de non-conformité. Lorsqu'il décide d'un examen ou d'un audit, le responsable du traitement peut tenir compte des certifications pertinentes en possession du sous-traitant.
d) Le responsable du traitement peut décider de procéder lui-même à l'audit ou de mandater un auditeur indépendant. Les audits peuvent également comprendre des inspections dans les locaux ou les installations physiques du sous-traitant et sont, le cas échéant, effectués moyennant un préavis raisonnable.
e) Les Parties mettent à la disposition de l'autorité de contrôle compétente/des autorités de contrôle compétentes, dès que celles-ci en font la demande, les informations énoncées dans la présente clause, y compris les résultats de tout audit.

7.7. Recours à des sous-traitants ultérieurs

a) **AUTORISATION ÉCRITE GÉNÉRALE :** le sous-traitant dispose de l'autorisation générale du responsable du traitement pour ce qui est du recrutement de sous-traitants ultérieurs sur la base d'une liste convenue. Le sous-traitant informe spécifiquement par écrit le responsable du traitement de tout projet de modification de cette liste par l'ajout ou le remplacement de sous-traitants ultérieurs au moins 30 (trente) jours à l'avance, donnant ainsi au responsable du traitement suffisamment de temps pour pouvoir s'opposer à ces changements avant le recrutement du ou des sous-traitants ultérieurs concernés. Le sous-traitant fournit au responsable du traitement les informations nécessaires pour lui permettre d'exercer son droit d'opposition.
b) Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement), il le fait au moyen d'un contrat qui impose au sous-traitant ultérieur, en substance, les mêmes obligations en matière de protection des données que celles imposées au sous-traitant en vertu des présentes clauses. Le sous-traitant veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses et du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.
c) À la demande du responsable du traitement, le sous-traitant lui fournit une copie de ce contrat conclu avec le sous-traitant ultérieur et de toute modification qui y est apportée ultérieurement. Dans la mesure nécessaire à la protection des secrets d'affaires ou d'autres informations confidentielles, y compris les données à caractère personnel, le sous-traitant peut expurger le texte du contrat avant d'en diffuser une copie.
d) Le sous-traitant demeure pleinement responsable, à l'égard du responsable du traitement, de l'exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur. Le sous-traitant informe le responsable du traitement de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.
e) Le sous-traitant convient avec le sous-traitant ultérieur d'une clause du tiers bénéficiaire selon laquelle — dans le cas où le sous-traitant a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable — le responsable du traitement a le droit de résilier le contrat conclu avec le sous-traitant ultérieur et de donner instruction au sous-traitant ultérieur d'effacer ou de renvoyer les données à caractère personnel.

7.8. Transferts internationaux

a) Tout transfert de données vers un pays tiers ou une organisation internationale par le sous-traitant n'est effectué que sur la base d'instructions documentées du responsable du traitement ou afin de satisfaire à une exigence spécifique du droit de l'Union ou du droit de l'État membre à laquelle le sous-traitant est soumis et s'effectue conformément au chapitre V du règlement (UE) 2016/679 ou du règlement (UE) 2018/1725.
b) Le responsable du traitement convient que lorsque le sous-traitant recrute un sous-traitant ultérieur conformément à la clause 7.7 pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement) et que ces activités de traitement impliquent un transfert de données à caractère personnel au sens du chapitre V du règlement (UE) 2016/679, le sous-traitant et le sous-traitant ultérieur peuvent garantir le respect du chapitre V du règlement (UE) 2016/679 en utilisant les clauses contractuelles types adoptées par la Commission sur la base de

l'article 46, paragraphe 2, du règlement (UE) 2016/679, pour autant que les conditions d'utilisation de ces clauses contractuelles types soient remplies.

Clause 8

Assistance au responsable du traitement

a) Le sous-traitant informe sans délai le responsable du traitement de toute demande qu'il a reçue de la part de la personne concernée. Il ne donne pas lui-même suite à cette demande, à moins que le responsable du traitement des données ne l'y ait autorisé.
b) Le sous-traitant prête assistance au responsable du traitement pour ce qui est de remplir l'obligation qui lui incombe de répondre aux demandes des personnes concernées d'exercer leurs droits, en tenant compte de la nature du traitement. Dans l'exécution de ses obligations conformément aux points a) et b), le sous-traitant se conforme aux instructions du responsable du traitement.
c) Outre l'obligation incombant au sous-traitant d'assister le responsable du traitement en vertu de la clause 8, point b), le sous-traitant aide en outre le responsable du traitement à garantir le respect des obligations suivantes, compte tenu de la nature du traitement et des informations dont dispose le sous-traitant :

1) l'obligation de procéder à une évaluation de l'incidence des opérations de traitement envisagées sur la protection des données à caractère personnel (« analyse d'impact relative à la protection des données ») lorsqu'un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques ;
2) l'obligation de consulter l'autorité de contrôle compétente/les autorités de contrôle compétentes préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ;
3) l'obligation de veiller à ce que les données à caractère personnel soient exactes et à jour, en informant sans délai le responsable du traitement si le sous-traitant apprend que les données à caractère personnel qu'il traite sont inexactes ou sont devenues obsolètes ;
4) les obligations prévues à l'article 32 du règlement (UE) 2016/679.

d) Les Parties définissent à l'annexe III les mesures techniques et organisationnelles appropriées par lesquelles le sous-traitant est tenu de prêter assistance au responsable du traitement dans l'application de la présente clause, ainsi que la portée et l'étendue de l'assistance requise.

Clause 9

Notification de violation de données personnelles

En cas de violation de données à caractère personnel, le sous-traitant coopère avec le responsable du traitement et lui prête assistance aux fins de la mise en conformité avec les obligations qui lui incombent en vertu des articles 33 et 34 du règlement (UE) 2016/679 ou des articles 34 et 35 du règlement (UE) 2018/1725, selon celui qui est applicable, en tenant compte de la nature du traitement et des informations dont dispose le sous-traitant.

9.1. Violation de données en rapport avec des données traitées par le responsable du traitement

En cas de violation de données à caractère personnel en rapport avec des données traitées par le responsable du traitement, le sous-traitant prête assistance au responsable du traitement :

a) aux fins de la notification de la violation de données à caractère personnel à l'autorité de contrôle compétente/aux autorités de contrôle compétentes, dans les meilleurs délais après que le responsable du traitement en a eu connaissance, le cas échéant (sauf si la violation de données à caractère personnel est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques);
b) aux fins de l'obtention des informations suivantes qui, conformément à l'article 33, paragraphe 3, du règlement (UE) 2016/679, doivent figurer dans la notification du responsable du traitement, et inclure, au moins :

1) la nature des données à caractère personnel, y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
2) les conséquences probables de la violation de données à caractère personnel;
3) les mesures prises ou les mesures que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.
   Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais ;

c) aux fins de la satisfaction, conformément à l'article 34 du règlement (UE) 2016/679, de l'obligation de communiquer dans les meilleurs délais la violation de données à caractère personnel à la personne concernée, lorsque la violation

de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

9.2. Violation de données en rapport avec des données traitées par le sous-traitant

En cas de violation de données à caractère personnel en rapport avec des données traitées par le sous-traitant, celui-ci en informe le responsable du traitement dans les meilleurs délais après en avoir pris connaissance. Cette notification contient au moins :

a) une description de la nature de la violation constatée (y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et d'enregistrements de données à caractère personnel concernés) ;
b) les coordonnées d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la violation de données à caractère personnel ;
c) ses conséquences probables et les mesures prises ou les mesures qu'il est proposé de prendre pour remédier à la violation, y compris pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.

Les Parties définissent à l'annexe III tous les autres éléments que le sous-traitant doit communiquer lorsqu'il prête assistance au responsable du traitement aux fins de la satisfaction des obligations incombant à ce dernier en vertu des articles 33 et 34 du règlement (UE) 2016/679.

SECTION III - DISPOSITIONS FINALES

Clause 10
Non-respect des Clauses et résiliation

a) Sans préjudice des dispositions du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725, en cas de manquement du sous-traitant aux obligations qui lui incombent en vertu des présentes clauses, le responsable du traitement peut donner instruction au sous-traitant de suspendre le traitement des données à caractère personnel jusqu'à ce que ce dernier se soit conformé aux présentes clauses ou jusqu'à ce que le contrat soit résilié. Le sous-traitant informe rapidement le responsable du traitement s'il n'est pas en mesure de se conformer aux présentes clauses, pour quelque raison que ce soit.
b) Le responsable du traitement est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel conformément aux présentes clauses si :
1) le traitement de données à caractère personnel par le sous-traitant a été suspendu par le responsable du traitement conformément au point a) et le respect des présentes clauses n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension ;
2) le sous-traitant est en violation grave ou persistante des présentes clauses ou des obligations qui lui incombent en vertu du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725 ;
3) le sous-traitant ne se conforme pas à une décision contraignante d'une juridiction compétente ou de l'autorité de contrôle compétente/des autorités de contrôle compétentes concernant les obligations qui lui incombent en vertu des présentes clauses ou du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.
c) Le sous-traitant est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel en vertu des présentes clauses lorsque, après avoir informé le responsable du traitement que ses instructions enfreignent les exigences juridiques applicables conformément à la clause 7.1, point b), le responsable du traitement insiste pour que ses instructions soient suivies.
d) À la suite de la résiliation du contrat, le sous-traitant supprime, selon le choix du responsable du traitement, toutes les données à caractère personnel traitées pour le compte du responsable du traitement et certifie auprès de celui-ci qu'il a procédé à cette suppression, ou renvoie toutes les données à caractère personnel au responsable du traitement et détruit les copies existantes, à moins que le droit de l'Union ou le droit national n'impose de les conserver plus longtemps. Le sous-traitant continue de veiller à la conformité aux présentes clauses jusqu'à la suppression ou à la restitution des données.

APPENDICE 1 - DÉTAILS DU TRAITEMENT

1. *Catégories de personnes concernées dont les données à caractère personnel sont traitées :*

■ Clients
□ Participants aux évènements
■ Participants à la communication
□ Parties intéressées
□ Fournisseur et/ou prestataire de services (contacts individuels chez ces fournisseurs)
■ Salariés
□ Anciens salariés
□ Proches de salariés
■ Représentants commerciaux
■ Relations d'affaires
■ Partenaires commerciaux
□ Visiteurs
■ Utilisateurs du service
■ Abonnés
□ Candidats
□ Apprentis/stagiaires
□ Consultants
□ Actionnaires/organismes
□ Fournisseurs et prestataires de services
■ Autres, veuillez préciser : ceux qui sont employés par les clients, c'est-à-dire les conducteurs et les utilisateurs des SERVICES VDO FLEET

2. Catégories de données à caractère personnel traitées :

Données à caractère général/coordonnées personnelles :
■ Noms Profils personnels
■ Données d'adresse personnelle
■ Données de pièce d'identité (par exemple, passeport, carte de Sécurité sociale, permis de conduire)
□ Image
■ Date de naissance
□ Autre, veuillez préciser : _____

Données relatives à un contrat :
■ Données de règlement et de paiement
■ Situation financière/solvabilité
□ Autre, veuillez préciser : _____
■ Coordonnées bancaires/données de carte de crédit
■ Historiques des contrats

Données professionnelles
■ Données relatives à la personne
■ Données relatives à la gestion des performances
■ Données relatives au salaire ou à la Sécurité sociale
■ Autre, veuillez préciser :
□ Données relatives au poste et à l'emploi
□ Données relatives aux qualifications et à la formation
■ Données relatives aux absences

- données d'admission du client et de ses opérateurs/utilisateurs
- données du conducteur (par exemple, nom, adresse (adresse de l'entreprise ou adresse privée le cas échéant), genre, date de naissance, numéro de permis, numéro de carte, etc.)
- données sur le véhicule et profils du véhicule
- données de communication (par exemple, téléphone, e-mail)
- données de mouvement, données GPS
- activités des conducteurs et profils de déploiement des véhicules, y compris les temps de conduite et les temps de repos conformément à l'annexe 1B du règlement (UE) n° 561/2006, du règlement (UE) n° 2020/1054, du règlement (CE) n° 1360/2002, du règlement n° 165/2014 et du règlement d'exécution (UE) n° 2016/799.
- données relatives à l'utilisation du service par les utilisateurs, données de téléchargement pour la carte de conducteur et le tachygraphe

Données relatives aux services et à l'utilisation des outils informatiques :
□ Identifiants d'appareil
□ Données image/vidéo
□ Données audio/voix
■ Données d'accès
□ Métadonnées
□ Autre, veuillez préciser : _____
■ Données relatives à l'utilisation et aux connexions
■ Données de télécommunication/contenus de messages
□ Données d'identification
□ Autorisation

3. <u>Les données sensibles traitées (le cas échéant) et les limitations ou garanties appliquées qui tiennent pleinement</u>

compte de la nature des données et des risques encourus, tels que, par exemple, la limitation stricte de la finalité, les restrictions des accès (y compris l'accès réservé uniquement au personnel ayant suivi une formation spécialisée), la tenue d'un registre de l'accès aux données, les restrictions applicables aux transferts ultérieurs ou les mesures de sécurité supplémentaires.

Catégories particulières de données personnelles

□ Origine raciale ou ethnique
□ Santé physique ou mentale
□ Données biométriques
□ Appartenance syndicale
□ Infractions pénales, condamnations ou jugements
□ Convictions religieuses ou philosophiques
□ Opinions politiques
□ Données génétiques
□ Vie sexuelle
□ Autre, veuillez préciser : _____

4. Nature du traitement :

CONTINENTAL a le droit de collecter, de traiter et d'utiliser les données à caractère personnel uniquement en conformité avec le contrat des SERVICES VDO FLEET et les instructions du CLIENT (voir Clause 7.1 ci-dessus).
Les détails sur l'étendue, la nature et la finalité de la collecte, du traitement et/ou de l'utilisation des données personnelles font l'objet des Conditions générales du Contrat, de sa Description de service ainsi que des aperçus fonctionnels des produits.

5. Finalités pour lesquelles les données personnelles sont traitées pour le compte du responsable du traitement

CONTINENTAL a été chargé d'agir en tant que processeur de données, afin de traiter pour le compte du CLIENT (le responsable du traitement) les données personnelles qui sont nécessaires pour rendre les SERVICES VDO FLEET.

6. Durée du traitement

La durée du traitement des données dépend de la durée du Contrat ou des éventuels contrats individuels ou commandes basés sur un accord-cadre.
Jusqu'à la fin du traitement et sous réserve de toute autre instruction documentée du responsable du traitement, le sous-traitant renvoie au responsable du traitement ou à un tiers désigné par le responsable du traitement, tous les documents, supports de données, résultats du traitement et données qui sont entrés en sa possession, et qui sont liés à la relation contractuelle ou ont été générés au cours de l'exécution du contrat et/ou du présent DPA.
Cette obligation s'étend aux copies et/ou reproductions des supports de données et/ou des stocks de données. Il n'existe pas de droit de conservation des données et des supports de données susmentionnés. Sauf disposition contraire du contrat, le sous-traitant restitue gratuitement au responsable du traitement toutes les données et tous les supports de données. Le responsable du traitement prend en charge tous les coûts et autres dépenses liés à la restitution des données.
Le responsable du traitement ne peut pas exiger l'effacement des données stockées par le sous-traitant, si et dans la mesure où le sous-traitant est soumis à des obligations légales de conservation. Au lieu de la suppression, le traitement des données peut être restreint, dans la mesure où cela est autorisé par les lois d'application locales ou nationales sur la protection des données. Cela s'applique en particulier si, en raison de la méthode de stockage spécifique, l'effacement n'est pas possible ou n'est possible qu'au prix de dépenses disproportionnées.

APPENDICE 2 - MESURES TECHNIQUES ET ORGANISATIONNELLES

La politique d'entreprise Directive sur la sécurité de l'information de Continental (CISG) définit les **exigences minimales** des mesures techniques et organisationnelles de CONTINENTAL en matière de traitement de l'information. En fonction de la classification des informations, des mesures sont mises en œuvre qui vont au-delà des exigences minimales.

Les exigences de la CISG sont mises en œuvre dans l'entreprise sur la base du Cadre standard de sécurité de l'information de l'entreprise et du Système de gestion de la sécurité de l'information (ISMS) correspondant.

La politique d'entreprise Directive sur la sécurité de l'information de Continental (CISG)
Cadre standard de sécurité de l'information de l'entreprise
Annexe 1 - Système de gestion de la sécurité de l'information (ISMS)
Annexe 2 - Rôles et responsabilités en matière de sécurité de l'information - tableau RACI

1. Contrôle de l'accès physique

Sécurisation de l'accès physique/de l'accès aux systèmes de traitement par lesquels le traitement a lieu, consistant à interdire cet accès aux personnes non autorisées (par exemple, grâce à des protections physiques : clôture, personnel de sécurité, verrouillage de porte, tourniquet, porte dotée d'un lecteur de cartes, caméra de surveillance, protection organisationnelle d'objets, autorisation d'accès, enregistrement d'accès).
Le Prestataire a mis en œuvre les Mesures Techniques et Organisationnelles suivantes aux fins du traitement des données à caractère personnel détaillé dans le présent DPA :

Classification standard des zones de sécurité de l'entreprise
Annexe 1 - Exigences d'aménagement et de sécurité
Annexe 2 - Enregistrement audio/visuel sur les lieux de travail
Badge Continental standards de l'entreprise

■	Système d'alarme
■	Système de contrôle d'accès automatique
☐	Système de verrouillage par code
☐	Barrières d'accès biométriques
☐	Barrières lumineuses/capteurs de mouvements
■	Système de verrouillage manuel à clé (registre des clés, délivrance de clés)
■	Enregistrement des visiteurs
■	Sélection prudente du personnel de sécurité
■	Cartes à puce/systèmes de verrouillage à transpondeur
■	Contrôle vidéo des portes d'accès
■	Verrous de sécurité
■	Contrôle du personnel par gardien/réception
■	Sélection prudente du personnel de nettoyage
■	Obligations de porter des badges de salarié/visiteur
☐	Divers :

2. Contrôle de l'accès aux données/contrôle des utilisateurs

Prévention de l'utilisation des systèmes de traitement automatisé par des personnes non autorisées, au moyen d'équipements de transmission des données (authentification nécessitant un identifiant et un mot de passe).
Le Prestataire a mis en œuvre les Mesures Techniques et Organisationnelles suivantes aux fins du traitement des données à caractère personnel détaillé dans le présent DPA :

Règlement sur les mots de passe du Manuel d'entreprise (M60.02.01)
Procédure standard de l'entreprise pour l'identification et l'autorisation des utilisateurs des systèmes informatiques
Règlement sur la sécurité des CLIENTS de l'entreprise (remplace le M60.02.10)
Gouvernance de l'environnement mobile de l'entreprise (remplace le M60.05.01)

■	Authentification avec nom d'utilisateur/mot de passe (mots de passe attribués selon les règlements en vigueur)
☐	Utilisation de systèmes de détection des intrusions
■	Utilisation de logiciels antivirus
■	Utilisation de logiciels pare-feu
■	Création de profils d'utilisateurs
■	Attribution de profils d'utilisateurs pour les systèmes informatiques
■	Utilisation de la technologie VPN
■	Chiffrement des supports de stockage de données mobiles
☐	Chiffrement des supports de stockage de données sur ordinateurs portables
☐	Utilisation de logiciels d'administration centrale des smartphones (par exemple, pour l'effacement externe des données)
☐	Divers :

3. Contrôle de l'utilisation des données/contrôle des supports de stockage des données/contrôle de la mémoire

Mesures destinées à empêcher la lecture, la copie, la modification ou l'effacement non autorisé(e) de supports de données (contrôle des supports de stockage de données), à empêcher la saisie non autorisée de données à caractère personnel ainsi que leur accès non autorisé, la modification et l'effacement non autorisé(e) des données à caractère personnel sauvegardées (contrôle de mémoire). Mesures destinées à garantir que les personnes autorisées à utiliser un système de traitement automatisé n'aient accès aux données à caractère personnel qu'en fonction de leur autorisation d'accès (par exemple, au moyen de concepts d'autorisation, de mots de passe, de règles régissant la démission et la réaffectation de salariés au sein d'autres départements) (contrôle de l'utilisation des données).
Le Prestataire a mis en œuvre les Mesures Techniques et Organisationnelles suivantes aux fins du traitement des données à caractère personnel détaillé dans le présent DPA :

Règlement sur les mots de passe du Manuel d'entreprise (M60.02.01)
Procédure standard de l'entreprise pour l'identification et l'autorisation des utilisateurs des systèmes informatiques
Classification et contrôle de l'information de l'entreprise
Manuel de l'entreprise, Directives de sécurité pour les bases de données - 3.4.6 Intégrité des données

■	Rôles et autorisations fondés sur le principe de « stricte nécessité »
■	Nombre d'administrateurs réduit à l'« essentiel »
■	Enregistrement des accès aux applications, en particulier de la saisie, de la modification et de l'effacement de données
■	Effacement physique des supports de stockage de données avant réutilisation
■	Utilisation de destructeurs de documents offrant un niveau de sécurité approprié ou recours à des prestataires de services
■	Administration des droits par des administrateurs de systèmes déterminés
■	Règles relatives aux mots de passe, définissant, entre autres, la longueur des mots de passe et imposant leur modification
■	Conservation sécurisée des supports de stockage de données
■	Destruction appropriée des supports de stockage de données (DIN 66399)
☐	Enregistrement des destructions
☐	Divers :

4. Contrôle des transferts/du transport

Mesures visant à assurer la confidentialité et l'intégrité des données au cours du transfert de données à caractère personnel et du transport des supports de stockage de données (par exemple, grâce à un chiffrement renforcé des transmissions de données, à l'utilisation d'enveloppes scellées pour les envois par la poste, à une sauvegarde cryptée sur des supports de stockage de données).
Le Prestataire a mis en œuvre les Mesures Techniques et Organisationnelles suivantes aux fins du traitement des données à caractère personnel détaillé dans le présent DPA :

■	Mise en place de lignes dédiées ou de tunnels VPN
■	Chiffrement des transmissions de données sur internet (HTTPS, SFTP, etc.)
■	Chiffrement des courriers électroniques

■	Enregistrement des destinataires des données et des périodes de transmission planifiée ou détermination d'un commun accord d'échéances d'effacement
☐	En cas de transport physique, sélection minutieuse du personnel et des véhicules
☐	Transmission des données sous forme anonymisée ou pseudonymisée
☐	En cas de transport physique, sélection de conteneurs/emballages sécurisés
☐	Divers :

5. Contrôle de la saisie/de la transmission

Mesures visant à assurer un examen a posteriori de façon à déterminer quelles données à caractère personnel ont été saisies ou modifiées, quand et par qui dans le cadre de systèmes de traitement automatisé, par exemple au moyen d'un dispositif de journalisation (contrôle des saisies).
Selon le système, mesures visant à assurer qu'il soit possible de vérifier et de déterminer quels établissements/locaux ont reçu ou transmis des données à caractère personnel au moyen d'équipements permettant la transmission de données, ou à quels établissements/locaux de telles données pourraient être transmises (contrôle des transmissions).
Le Prestataire a mis en œuvre les Mesures Techniques et Organisationnelles suivantes aux fins du traitement des données à caractère personnel détaillé dans le présent DPA :

Directive sur la sécurité de l'information de Continental (CISG) – 3.5.10.1 Enregistrement de l'audit
Procédure standard de l'entreprise pour l'identification et l'autorisation des utilisateurs des systèmes informatiques
Classification et contrôle de l'information de l'entreprise
Manuel de l'entreprise, Directives de sécurité pour les bases de données - 3.4.6 Intégrité des données

■	Enregistrement de la saisie, de la modification et de l'effacement des données
■	Traçabilité de la saisie, de la modification et de l'effacement des données, assurée par l'emploi de noms d'utilisateurs uniques (et non de groupes d'utilisateurs)
■	Attribution de droits de saisie, de modification et d'effacement de données, selon un concept d'autorisation
☐	Création d'une synthèse indiquant quelles données peuvent être saisies, modifiées et effacées, avec quelles applications
☐	Gestion de formulaires à partir desquels les données font l'objet d'un traitement automatisé
☐	Divers :

6. Contrôle de la disponibilité/restauration/fiabilité/intégrité des données

Mesures destinées à garantir que les systèmes utilisés peuvent être restaurés en cas de dysfonctionnement (possibilité de rétablissement). Mesures visant à faire en sorte que toutes les fonctions d'un système soient disponibles et que tout dysfonctionnement soit signalé (fiabilité). Mesures destinées à garantir que les données à caractère personnel stockées ne peuvent être endommagées par les dysfonctionnements d'un système (intégrité des données). Mesures destinées à garantir la protection des données à caractère personnel contre les risques de destruction ou de perte accidentelle (contrôle de disponibilité), par exemple, en mettant en œuvre des sauvegardes adaptées et des concepts de rétablissement après sinistre.
Le Prestataire a mis en œuvre les Mesures Techniques et Organisationnelles suivantes aux fins du traitement des données à caractère personnel détaillé dans le présent DPA :

Règlement sur la sécurité des sauvegardes et des restaurations du Manuel de l'entreprise (M60.02.08)

■	Alimentation électrique continue (UPS)
■	Appareils permettant de contrôler la température et l'humidité dans les salles de serveurs
■	Systèmes de détection des incendies et de la fumée
☐	Alarmes en cas d'accès non autorisé aux salles de serveurs
■	Tests de la restauration des données
■	Conservation des sauvegardes de données en un lieu sûr et séparé
☐	Dans les zones inondables, le serveur est situé au-dessus du niveau d'inondation
■	Appareils de climatisation dans les salles de serveurs
☐	Blocs d'alimentation électrique protégés dans les salles de serveurs
■	Extincteurs d'incendie dans les salles de serveurs
■	Élaboration d'un concept de sauvegarde et de restauration
☐	Élaboration d'un plan d'urgence
☐	Divers :

7. Contrôle de la séparation/séparabilité

Mesures visant à faire en sorte que les données collectées pour des finalités différentes puissent être traitées séparément (par exemple, séparation logique des données clients, contrôles d'accès spécifiques (concept d'autorisation), séparation des données de tests et de production).
Le Prestataire a mis en œuvre les Mesures Techniques et Organisationnelles suivantes aux fins du traitement des données à caractère personnel détaillé dans le présent DPA :

Directive sur la sécurité de l'information de Continental (CISG) – 3.5.1.4 Séparation des installations de développement, de test et d'exploitation

■	Stockage physiquement séparé dans des systèmes ou sur des supports de stockage de données distinctes
☐	Intégration d'attributions/de champs de données de finalité(s) dans les ensembles de données
■	Création de droits d'accès aux bases de données
☐	Séparation logique des clients (fondée sur les logiciels)
☐	Pour les données pseudonymisées : séparation du fichier de cartographie et conservation dans un système informatique séparé et sécurisé
■	Séparation des systèmes de production et de tests
☐	Divers :

ANNEXE III : LISTE DE SOUS-TRAITANTS ULTERIEURS

CONTINENTAL assure un niveau approprié de mesures de sécurité techniques et organisationnelles chez les sous-traitants secondaires impliqués afin de traiter les données personnelles dans un cadre approprié et sécurisé (Adéquation du sous-traitant supérieur).

Si des sous-traitants secondaires sont impliqués dans le traitement des données personnelles (par exemple, l'hébergement, la fourniture d'espace de centre de données, les services de cloud, les logiciels d'exploitation, etc.), la mise en œuvre de mesures techniques et organisationnelles par le sous-traitant secondaire respectif sera assurée par des accords de traitement des données correspondants. Les sous-traitants secondaires doivent – avec une garantie suffisante – assurer au moins les mêmes mesures techniques et organisationnelles que celles convenues entre le Client et CONTINENTAL.

Afin de prévenir et/ou d'éviter tout accès non autorisé et/ou toute tentative d'accès non autorisée aux systèmes informatiques et aux installations de stockage de CONTINENTAL, y compris aux données qui y sont stockées - que ce soit de l'extérieur ou de l'intérieur ou par des Sup-Processeurs - CONTINENTAL a mis en place des mesures permanentes de contrôle et de surveillance de ses systèmes informatiques, y compris un contrôle d'accès / surveillance d'accès (24/7, 365 jours) en mettant en œuvre des systèmes de détection d'intrusion / pare-feu / contrôle d'accès de pointe, etc. Si un accès non autorisé ou une tentative d'accès non autorisée est détecté, il y sera automatiquement mis fin sans délai. L'équipe de service de Continental Automotive Technologies GmbH en Europe a le contrôle exclusif de ces systèmes de sécurité ; l'accès à ces systèmes par les Processeurs ou autres est exclu.

Les sous-traitants/sous-traitants secondaires suivants sont impliqués par CONTINENTAL :

Applicable uniquement si Continental Automotive Technologies GmbH n'est pas la partie contractante **:**	
■	**Continental Automotive Technologies GmbH et sociétés affiliées du Groupe**, Vahrenwalder Straße 9, 30165 Hanovre, Allemagne (Développement et assistance)

SOUS-TRAITANTS SECONDAIRES APPLICABLES A TOUS LES PAYS/CLIENTS :	
■	**Eviden Germany GmbH**, Otto-Hahn Ring 6, 81739 München (Assistance et Maintenance)
■	**Com-a-tec GmbH,** Am Krebsgraben 15, 78048 Villingen-Schwenningen, Germany (Support niveau 2)
■	**Continental AG**, Hauptverwaltung, Vahrenwalder Straße 9, D-30165 Hannover Continental AG est le titulaire du contrat concernant la fourniture de services par le sous-traitant de Continental AG envers Continental Automotive Technologies GmbH, comme indiqué ci-dessous séparément.
■	**Google Ireland Limited,** Gordon House, Barrow Street, Dublin 4, Irlande (Fournisseur de services Cloud, par exemple la plateforme Google Cloud) **Veuillez noter :** Google sera utilisé en tant que « sous-traitant secondaire » pour la fourniture de services cloud. À cet égard, CONTINENTAL a veillé à ce que les données provenant de l'Espace économique européen (EEE) ne soient traitées que dans l'EEE, sauf accord contraire avec le CLIENT. En complément des mesures précitées viennent s'ajouter les mesures suivantes : les clauses contractuelles types de la Commission européenne ont été convenues avec OKTA (voir la décision d'exécution (UE) 2021/914 de la Commission du 04.06.2021) et la nouvelle décision d'adéquation adoptée par la Commission européenne le 10.07.2023 concernant le niveau de protection des données personnelles transférées de l'UE vers les organisations situées aux États-Unis s'applique. Continental a également mis en place des mesures de sécurité techniques

	spécifiques pour empêcher l'accès non autorisé aux données, en particulier depuis l'extérieur de l'espace économique européen (EEE).
■	**kernel concepts GmbH**, Hauptstraße 16, 57074 Siegen (fournisseur de services de noyau, d'amélioration, de maintenance, etc., les données seront traitées uniquement dans l'EEE)
■	**pendo.io Inc.,** 150 Fayetteville St., Raleigh, NC 27601, États-Unis ; Représentant européen (art. 27 RGPD) : DP-Dock GmbH, Ballindamm 39, 20095 Hambourg (Services d'assistance et de développement) **Veuillez noter :** pendo.io ne traite que des données anonymisées et agrégées ; En complément des mesures précitées viennent s'ajouter les mesures suivantes : les clauses contractuelles types de la Commission européenne en place (voir la décision d'exécution (UE) 2021/914 de la Commission du 04.06.2021). Continental a également mis en place des mesures de sécurité techniques spécifiques pour empêcher l'accès non autorisé aux données, en particulier depuis l'extérieur de l'espace économique européen (EEE), ainsi qu'à la nouvelle décision d'adéquation adoptée par la Commission européenne le 10.07.2023 concernant le niveau de protection des données personnelles transférées de l'UE vers les organisations situées aux États-Unis.
■	**Zonar Sytems, Inc.**, 18200 Cascade Ave S, Seattle, WA 98188, États-Unis, filiale à 100 % de Continental Group. Zonar Systems fournit des services d'assistance, de maintenance et de développement pour les Services VDO Fleet de CONTINENTAL. **Veuillez noter :** Tout accès par Zonar Systems aux données (personnelles) du Client – VDO Fleet au sein de l'EEE est à la fois soumis aux règles d'entreprise contraignantes de Continental Group qui garantissent un niveau adéquat de protection des données au sens de l'art 45 et suivants du RGPD, ainsi qu'à la nouvelle décision d'adéquation adoptée par la Commission européenne le 10.07.2023 concernant le niveau de protection des données personnelles transférées de l'UE vers les organisations situées aux États-Unis.
■	**Continental Digital Services France SAS**, 1 avenue Paul Ourliac B.P.13704 31037 Toulouse, France Continental Digital Services France est une société du groupe Continental qui fournit des activités de développement, suivi et support pour les services.
■	**Continental Automotive Components (India) Private Limited,** Technical Center India, South Gate Tech Park, Plot No. 1, Veerasandra Industrial Area, Hosur Main Road, Bangalore - 560 100, India Continental Automotive Components (India) est une société du groupe Continental qui fournit des activités de développement, suivi et support pour les services. **Veuillez noter :** Tout accès par Continental Automotive Components (India) aux données (personnelles) du Client – VDO Fleet au sein de l'EEE est à la fois soumis aux règles d'entreprise contraignantes de Continental Group qui garantissent un niveau adéquat de protection des données au sens de l'art 45 et suivants du RGPD, ainsi qu'à la nouvelle décision d'adéquation adoptée par la Commission européenne le 10.07.2023 concernant le niveau de protection des données personnelles transférées de l'UE vers les organisations situées aux États-Unis.

	SOUS-TRAITANTS SUPPLEMENTAIRES UNIQUEMENT APPLICABLES POUR LA FRANCE / LES CLIENTS FRANÇAIS :
■	**IMA TECHNOLOGIES**, 31 Route de Gachet 44300 Nantes, France (Hotline)

	SOUS-TRAITANTS DE CONTINENTAL AG APPLICABLES A TOUS LES PAYS/CLIENTS :
■	**SYZYGY Deutschland GmbH**, Im Atzelnest 3, 61352 Bad Homburg, Allemagne (Services d'hébergement)
■	**MongoDB Limited, Ireland,** 3 Shelbourne Buildings, Ballsbridge, Dublin 4, Irlande (Fournisseur de services Cloud ; les services Cloud sont restreints à l'EEE.)

	SOUS-TRAITANTS DE ZONAR SYSTEMS, INC APPLICABLES A TOUS LES PAYS/CLIENTS :
■	**Clearblade Inc., 1701 Directors BLVD STE 250, Austin, TX 78744, USA**

	(Solution de gestion des connexions d'appareils télématiques, assistance / maintenance) **Veuillez noter :** Continental s'est assuré que les services et les données provenant de l'Espace économique européen (EEE) ne seront traités que sur des serveurs situés dans l'Espace économique européen (EEE). En complément des mesures précitées viennent s'ajouter les mesures suivantes : les clauses contractuelles types de la Commission européenne ont été convenues avec Clearblade (voir la décision d'exécution (UE) 2021/914 de la Commission du 04.06.2021). Continental a également mis en place des mesures de sécurité techniques spécifiques pour empêcher l'accès non autorisé aux données, en particulier depuis l'extérieur de l'espace économique européen (EEE), ainsi qu'à la nouvelle décision d'adéquation adoptée par la Commission européenne le 10.07.2023 concernant le niveau de protection des données personnelles transférées de l'UE vers les organisations situées aux États-Unis.
■	**DataDog Inc.,** New York Times Bldg, 620 8 th Ave 45th Floor, New York, MA, États-Unis (Services d'assistance et de disponibilité) **Veuillez noter :** Data Dog Inc. ne traite que des données anonymisées et agrégées ; En complément des mesures précitées viennent s'ajouter les mesures suivantes : les clauses contractuelles types de la Commission européenne en place (voir la décision d'exécution (UE) 2021/914 de la Commission du 04.06.2021). Continental a également mis en place des mesures de sécurité techniques spécifiques pour empêcher l'accès non autorisé aux données, en particulier depuis l'extérieur de l'espace économique européen (EEE).
■	**OKTA Inc.,** 100 First Street, 6th Floor, San Francisco, CA 94105, USA (Service Provider Customer Identity & Access Management (CIAM)) Veuillez noter : Continental s'est assuré que les services et les données provenant de l'Espace économique européen (EEE) ne seront traités que sur des serveurs situés dans l'Espace économique européen (EEE). En complément des mesures précitées viennent s'ajouter les mesures suivantes : les clauses contractuelles types de la Commission européenne ont été convenues avec OKTA (voir la décision d'exécution (UE) 2021/914 de la Commission du 04.06.2021) et la nouvelle décision d'adéquation adoptée par la Commission européenne le 10.07.2023 concernant le niveau de protection des données personnelles transférées de l'UE vers les organisations situées aux États-Unis s'applique. Continental a également mis en place des mesures de sécurité techniques spécifiques pour empêcher l'accès non autorisé aux données, en particulier depuis l'extérieur de l'espace économique européen (EEE).
■	**MongoDB Limited, Ireland,** 3 Shelbourne Buildings, Ballsbridge, Dublin 4, Irlande (Fournisseur de services Cloud ; les services Cloud sont restreints à l'EEE.)
■	**pendo.io Inc.,** 150 Fayetteville St., Raleigh, NC 27601, États-Unis ; Représentant européen (art. 27 RGPD) : DP-Dock GmbH, Ballindamm 39, 20095 Hambourg (Services d'assistance et de développement) **Veuillez noter :** pendo.io ne traite que des données anonymisées et agrégées ; En complément des mesures précitées viennent s'ajouter les mesures suivantes : les clauses contractuelles types de la Commission européenne en place (voir la décision d'exécution (UE) 2021/914 de la Commission du 04.06.2021). Continental a également mis en place des mesures de sécurité techniques spécifiques pour empêcher l'accès non autorisé aux données, en particulier depuis l'extérieur de l'espace économique européen (EEE), ainsi qu'à la nouvelle décision d'adéquation adoptée par la Commission européenne le 10.07.2023 concernant le niveau de protection des données personnelles transférées de l'UE vers les organisations situées aux États-Unis.

Informations générales : Vos droits dans le cadre du Règlement général européen sur la protection des données restent inchangés. CONTINENTAL confirme en outre que vos données seront stockées dans des centres de données situés dans l'Union européenne. CONTINENTAL utilise les normes de sécurité les plus élevées (par exemple, ISO/DIN/https/cryptage) et protège les données personnelles pendant leur transmission et leur stockage.

* * *