



DIAG'ASSIST



Contrat de sous-traitance

conclu entre

.....Numéro de client

.....Raison sociale

..... Rue / n°

.....Code postal, ville

..... Pays

– ci-après « **le Client** » –

et

HELLA Gutmann Solutions GmbH
Am Krebsbach 2
79241 Ihringen
Allemagne

– ci-après « **le Fournisseur** » –

- Le Client et le Fournisseur sont appelés conjointement les « **Parties** » ou séparément la « **Partie** »

Préambule

Le Fournisseur développe et distribue des solutions de diagnostic électroniques pour véhicules automobiles. Par l'intermédiaire d'une interface électronique, il reçoit des données sur les véhicules provenant de l'exploitation du Client. Ces données comprennent également des données définies par le règlement général sur la protection des données (« **RGPD** ») comme des données à caractère personnel, par exemple l'immatriculation et le numéro d'identification du véhicule. Les Parties conviennent du contrat suivant pour régler l'utilisation de ces données à caractère personnel.



1. Objet, étendue et durée du contrat

- 1.1. Le Client confie au Fournisseur le traitement et l'utilisation des données décrites à l'article 1.2, conformément aux droits et obligations prévus par le présent contrat.
- 1.2. Les données prévues par le présent contrat sont les données à caractère personnel transmises par le Fournisseur à l'occasion des réparations / de l'entretien de véhicules automobiles provenant de l'exploitation du Client, notamment les informations concernant les clients du Client, les numéros d'identification des véhicules (FIN/VIN) et les immatriculations. Ces données sont appelées ci-après « **données contractuelles** ».
- 1.3. En l'état actuel des choses, les données contractuelles comprennent les types de données suivantes :
 - FIN/VIN
 - Immatriculation
 - Nom, adresse, adresse électronique et numéro de téléphone du détenteur du véhicule

À l'occasion de l'utilisation de Remote-Service, les données contractuelles contiennent en outre :

- Nom du client final du Client

À l'occasion de l'utilisation de Techview, les données contractuelles contiennent en outre :

- Information par image
- Vidéo en direct et flux audio
- Historique des discussions avec images et fichiers
- Numéro de téléphone de l'employé du garage automobile
- Adresse électronique de l'employé du garage automobile

En outre, les données contractuelles comprennent, pour l'utilisation de Cyber Security management :

- Nom et prénom de l'employé du Client
- Adresse électronique de l'employé du Client
- Référence aux fins de vérification d'identité (IDnow-Token)

- 1.4. Le Fournisseur saisit, stocke et traite les données contractuelles. Ce traitement des données contractuelles s'effectue exclusivement pour préparer et soutenir les travaux de maintenance et de réparation du Client dans le cadre de son activité professionnelle.



1.5. Le Fournisseur stocke les données contractuelles jusqu'au terme du contrat (article 12) ou jusqu'à tout ordre d'effacement antérieur du Client. Les données sont stockées plus longtemps si des règles de conservation légales l'exigent.

1.6. Sont concernés par la transmission et le traitement des données contractuelles

- les clients du Client (dont les consommateurs),
- le détenteur du véhicule,
- les employés du Client

2. Mesures d'ordre technique et organisationnel visant à garantir la sécurité des données

2.1. Le Fournisseur s'engage à protéger efficacement les données contractuelles selon l'état de la technique contre tout accès non autorisé, toute modification, destruction ou perte, transmission non autorisée, tout autre traitement non autorisé et tout autre abus. Il s'engage également à prendre toutes les mesures d'ordre technique et organisationnel (« MTO ») requises, conformément à l'article 32 du RGPD. Les MTO permettent de garantir que les données contractuelles soient protégées dans les limites nécessaires contre les abus, la perte et l'accès non autorisé par des tiers.

2.2. L'état actuel des MTO prises par le Fournisseur est présenté dans **l'annexe 1**. Le Fournisseur adaptera ses MTO au cours du contrat si les mesures prises ne correspondent plus à l'état actuel de la technique et/ou si des adaptations sont nécessaires en raison des évolutions organisationnelles, dans la mesure où les frais d'implémentation sont proportionnels au risque affectant les droits et les libertés des personnes concernées. Les MTO présentées dans **l'annexe 1** ne peuvent pas être inférieures au niveau de sécurité. Le Fournisseur documente les modifications des MTO.

2.3. Dans les cas des articles 6.3 et 6.4 (problèmes de protection des données), le Fournisseur adapte ses MTO conformément à l'article 2.2 du présent contrat, dans la mesure où ceci est utile et nécessaire à éviter toute violation future du même type. En outre, les Parties prendront les mesures appropriées pour atténuer les conséquences négatives possibles pour les personnes concernées.

3. Droits et devoirs du Client, mesures de contrôle

3.1. Seul le Client répond de l'appréciation de la légitimité du traitement conformément à l'art. 6, paragraphe 1, du RGPD, et de la préservation des droits des personnes concernées en vertu des art. 12 à 22 du RGPD.

3.2. Le Client peut s'assurer du respect des MTO prises en vertu de l'alinéa 2 du présent contrat par des inspections sur place et avant le début du traitement des données conformément à l'article 3.3, puis régulièrement sur rendez-vous à une fréquence appropriée. À cet égard, le Client ne peut pas effectuer lui-même les inspections. Pour les inspections, il doit mandater des experts qui doivent assurer au Fournisseur qu'ils contrôlent exclusivement le respect des obligations prévues par l'art. 28 du



RGPD, qu'ils remettent ces résultats exclusivement au Client et qu'ils ne dévoilent notamment aucun secret commercial du Fournisseur au Client.

- 3.3. En outre, le Client peut demander au Fournisseur des renseignements et des informations sur la mise en œuvre des MTO conformément à l'alinéa 2, ainsi que sur le respect de toutes les autres obligations prévues par l'art. 28 du RGPD. Le Fournisseur peut répondre à cette exigence soit lui-même, soit par l'intermédiaire d'un tiers, par exemple :
 - 3.3.1. en donnant des renseignements personnels sur la mise en œuvre des MTO ;
 - 3.3.2. en présentant une attestation, un rapport ou un extrait de rapport d'une instance indépendante (par exemple d'un expert).
- 3.4. Les frais engagés le cas échéant dans le cadre des examens en vertu des articles 3.2 à 3.3 du présent contrat, notamment en raison du mandat confié à un tiers, sont à la charge du Client, dans la mesure où le Client a mandaté lui-même le tiers ou s'il exige que le Fournisseur mandate le tiers.
- 3.5. Le Client informe le Fournisseur sans délai s'il constate des erreurs ou des irrégularités lors de l'examen des MTO.

4. Droits et devoirs du Fournisseur

- 4.1. Le Fournisseur, ainsi que toute personne placée sous son autorité ayant accès aux données contractuelles, traitent les données contractuelles exclusivement pour le compte du Client, suivant ses consignes et dans les limites de l'objectif du présent contrat, dans la mesure où le Fournisseur n'est pas tenu à un autre contrat par le droit de l'Union européenne ou des États membres auquel le contractant est soumis. Dans ce cas, le Fournisseur fait part de ces exigences légales au Client avant le traitement, dans la mesure où le droit concerné n'interdit pas une telle communication en raison d'un motif d'intérêt public important.
- 4.2. Outre les directives du Client, le Fournisseur ne peut pas saisir, traiter ou utiliser les données contractuelles pour répondre à ses propres besoins ou aux besoins d'un tiers.
- 4.3. Le Fournisseur peut uniquement rectifier, effacer ou bloquer les données contractuelles sur instruction du Client, sauf si des intérêts légitimes du Fournisseur s'y opposent.
- 4.4. Le Fournisseur n'établit aucune copie ou aucun duplicata des données contractuelles sans l'autorisation du Client. En sont exclues les sauvegardes si elles sont nécessaires pour assurer un traitement des données en bonne et due forme, ainsi que les données nécessaires au regard du respect des obligations légales de conservation.
- 4.5. Le Fournisseur est tenu de transmettre sans délai au Client toutes les questions de tiers relatives aux données contractuelles. Il ne peut pas, sans autorisation sous forme écrite du Client, donner des renseignements aux personnes concernées ou à d'autres tiers sur les données contractuelles.



- 4.6. Si le Fournisseur a la possibilité de recourir à des dispositifs de traitement de données du Client, il peut uniquement utiliser cet accès pour satisfaire à ses obligations résultant du présent contrat.
- 4.7. Au regard de la nature du traitement, le Fournisseur aide le Client, selon ses possibilités, par des MTO appropriées, à satisfaire à son obligation de répondre aux demandes d'exercice des droits des personnes concernées, mentionnés au chapitre III du RGPD. En outre, il aide le Client à satisfaire aux obligations prévues par les articles 32 à 36 du RGPD, compte tenu de la nature du traitement et des informations dont il dispose. Le Client doit rembourser au Fournisseur les frais engagés à cet égard. Les Parties en fixent le montant à 50,00 € / heure, ainsi que la TVA le cas échéant.

5. Délégué à la protection des données

- 5.1. Le délégué à la protection des données du Fournisseur est Monsieur Eike Westermann (dataprivacy@hella.com).
- 5.2. Il convient de communiquer au Client sans délai tout changement de délégué à la protection des données.

6. Obligations de déclaration

- 6.1. Le Fournisseur informe le Client sans délai s'il estime que l'une de ses instructions porte atteinte au RGPD ou à toute autre règle relative à la protection des données de l'Union européenne ou des États membres. Le Fournisseur peut suspendre l'exécution de l'instruction concernée jusqu'à ce qu'il soit informé de l'examen par le Client et de ses résultats. Si l'examen du Client révèle la présence d'une violation des règles relatives à la protection des données, le Fournisseur n'exécute pas l'instruction donnée. En l'absence de consensus entre les Parties, après l'examen effectué par le Client, sur l'adéquation de la consigne avec le RGPD ou toute autre règle de l'Union européenne ou des États membres sur la protection des données, les Parties informent l'autorité de contrôle compétente et lui demandent de prendre une décision conformément à l'art. 58, alinéa 2, point a) du RGPD.
- 6.2. Si le Fournisseur a connaissance d'une violation des données contractuelles, il doit en informer le responsable sans délai. Le Fournisseur a connaissance d'une violation des données contractuelles si les informations dont il dispose sont suffisantes pour permettre une notification au sens du RGPD.
- 6.3. L'article 6.2 s'applique en conséquence si le Fournisseur a connaissance de perturbations dans le traitement ou dans le fonctionnement de l'entreprise ou de toute autre violation des règles de protection des données contractuelles.
- 6.4. Le Fournisseur doit informer le Client sans délai de toute mesure de contrôle et de toute mesure engagée par l'autorité de contrôle concernant les données contractuelles. Il en va de même en cas d'enquête d'une autorité compétente chez le Fournisseur. Le Fournisseur observe les décisions administratives relatives aux données contractuelles.

7. Pouvoir de donner des instructions / Étendue



- 7.1. Il convient de donner les instructions par écrit (notamment écrit ou e-mail).
- 7.2. Le Fournisseur documente les instructions du responsable dans la forme adéquate.

8. Obligation au secret des données

- 8.1. Le Fournisseur s'engage à préserver le secret des données dans le cadre du traitement des données contractuelles.
- 8.2. Le Fournisseur doit obliger ses employés chargés de l'exécution des travaux à respecter la confidentialité des données. En outre, le Fournisseur doit informer ces employés qu'ils sont tenus aux instructions et à la finalité.
- 8.3. Le secret des données persiste au terme du contrat.

9. Traitement transfrontalier

Le traitement des données convenu par contrat s'effectue exclusivement dans un État membre de l'Union européenne ou dans un autre État partie à l'accord sur l'Espace économique européen. Le lieu de stockage des données contractuelles doit être situé au sein de l'Union européenne ou de l'Espace économique européen. Tout traitement de données contractuelles dans un pays tiers, y compris la consultation de données dans un pays tiers (par exemple par le service clientèle, le centre d'assistance, etc.) nécessite l'autorisation écrite du Client et la réunion des conditions spéciales prévues par les art. 44 et suivants du RGPD. Le Client donne son consentement si les conditions légales sont réunies. Il en va de même en cas de contrat confié à des sous-traitants dans des pays tiers. Pour assurer un niveau de protection adéquat des données, les Parties sont tenues d'utiliser les clauses contractuelles standard de la Commission européenne dès qu'elles sont disponibles. Si ces clauses sont convenues entre le Fournisseur et le sous-traitant, le consentement du Client n'est pas nécessaire.

10. Sous-traitants

- 10.1. Le Fournisseur peut confier le traitement des données à des sous-traitants. À cet égard, les accords contractuels avec le / les sous-traitant(s) doivent être conformes aux règles relatives à la protection des données dans le rapport contractuel régissant les relations entre le Client et le Fournisseur. Une liste des sous-traitants actuellement mandatés est jointe au présent contrat en **annexe 2**.
- 10.2. Le Fournisseur informera le Client en temps utile par écrit (notamment écrit ou e-mail) de toute modification concernant le recours à des sous-traitants ou leur remplacement. Le Client peut contester ces modifications par écrit (notamment écrit ou e-mail) dans un délai de deux semaines à compter de la réception de l'information.
- 10.3. Le Fournisseur s'assure que son sous-traitant lui accorde les droits de contrôle prévus aux art. 3.2 et 3.3 du présent contrat. À l'aide de ces droits, il s'assure notamment que le sous-traitant offre des garanties suffisantes de mise en œuvre des mesures d'ordre technique et organisationnel appropriées, de manière que le traitement soit conforme aux prescriptions du RGPD. Le Fournisseur doit documenter les résultats des examens et les remettre au Client à sa demande.



10.4. Il convient de consigner par écrit les contrats conclus avec les sous-traitants (notamment écrit ou e-mail).

11. Propriété des supports de données, restitution de données et de supports de données, effacement

11.1. Les supports de données remis par le Client sur lesquels sont stockées des données contractuelles sont la propriété du Client.

11.2. Au terme de la période contractuelle (ou plus tôt à la demande du Client), le Fournisseur doit effacer entièrement les données contractuelles en sa possession, si aucune obligation légale de conservation ne s'y oppose.

11.3. Il convient de consigner l'effacement des données en indiquant la date et de le confirmer au Client par écrit (notamment écrit ou e-mail) à sa demande.

12. Durée

12.1. Le présent contrat entre en vigueur dès sa signature par les parties. Il est conclu pour une durée indéterminée.

12.2. Le contrat peut être résilié par les deux Parties avec un préavis de deux semaines. Il en va autrement si le Fournisseur est tenu par un autre contrat à traiter les données contractuelles pour le Client. Dans ce cas, le délai de préavis de deux semaines commence seulement au terme de l'autre contrat.

12.3. Chacune des Parties peut mettre fin au contrat sans préavis pour juste motif. Il y a juste motif si, compte tenu de toutes les circonstances de l'espèce et des intérêts réciproques des Parties, la poursuite de la relation contractuelle ne peut être raisonnablement exigée de la partie résiliante jusqu'au terme convenu ou jusqu'au terme du délai de préavis. Il en va notamment ainsi en présence d'une infraction grave de l'autre partie aux dispositions du présent contrat ou aux dispositions du RGPD.

12.4. Les résiliations s'effectuent par écrit en vertu de l'art. 126 du BGB.

13. Droit applicable / tribunal compétent / nullité partielle

13.1. Les Parties conviennent de l'application du droit allemand, à l'exclusion des règles de conflits de lois. Les tribunaux compétents pour connaître de tous les litiges en rapport avec le présent contrat sont les tribunaux du ressort du siège social du Fournisseur.

13.2. La caducité ou l'inapplicabilité de l'une des dispositions du présent contrat n'affecte pas la validité du contrat dans ses autres dispositions. La disposition caduque ou inapplicable est remplacée par une règle économiquement équivalente qui aurait été convenue par les Parties au contrat dans le sens correspondant à la matière du contrat.



DIAG'ASSIST

Lieu, date



Ihringen, le 17 novembre 2020

.....
.....

Signature Client
(Représentant habilité 1)

(Managing Director)

.....

Rolf Kunold

Nom en caractères d'imprimerie

- Annexe 1 -

Mesures d'ordre technique et organisationnel

Il convient de définir ci-après chacune des mesures d'ordre technique et organisationnel et de les qualifier concrètement.

Si le contrat concerne des données sensibles ou des types particuliers de données à caractère personnel (par ex. informations sur l'appartenance à un syndicat ou sur la santé), il convient de convenir de mesures de protection spécifiques. Il convient de les mentionner et de les définir.

Les mesures suivantes sont des exigences minimales. Le Fournisseur doit les garantir à tout moment :

1. Contrôle des entrées

Il convient d'interdire aux personnes non autorisées l'accès (physique) aux dispositifs de traitement de données avec lesquels les données à caractère personnel sont traitées et utilisées.

Mesures d'ordre technique et organisationnel visant à garantir le contrôle des entrées :

- lecteur de cartes ID, carte à puce ;
- mesures de protection contre le vol, la manipulation et les dommages, des appareils utilisés pour le traitement des données ;
par ex. concept d'autorisation d'accès aux serveurs, ASI et climatisation des locaux des serveurs
- plusieurs zones de sécurité sur le site de l'entreprise;
- enregistrement du personnel sur place;
- remise contrôlée des clés (y compris zones d'accès);
- système de sécurité des portes (ouverture électrique des portes, etc.) ;
- service de sécurité, portier ;
- règles pour l'accès de personnes externes ;
- portillons à sens unique (par ex. tourniquet) ;
- systèmes de surveillance, par ex. système d'alarme

2. Contrôle de l'utilisation

Il convient d'empêcher que des personnes non autorisées puissent utiliser les systèmes de traitement de données.

Mesures d'ordre technique (protection par mot de passe) et organisationnel (fiche utilisateur) pour l'identification et l'authentification des utilisateurs :

- concept d'autorisation et introduction de niveaux d'accès différenciés (système) ;
- ID d'utilisateur individuel ;
- règles relatives au mot de passe (notamment caractères spéciaux, longueur minimale, il convient de changer régulièrement de mot de passe) ;
- concevoir et implémenter un processus garantissant que tous les droits d'accès soient immédiatement révoqués si un employé quitte l'entreprise du Fournisseur ;
- pare-feu ;

- cryptage des supports de données conformément aux règles applicables à la politique d'utilisation acceptable pour l'utilisation / l'élimination de supports de données (par ex. USB, disques durs externes) ;
- règles applicables à l'accès de personnes externes.

3. Contrôle de l'accès

Il convient de s'assurer que les personnes habilitées à utiliser un système de traitement de données puissent exclusivement accéder aux données relevant de leur autorisation d'accès et que les données à caractère personnel ne puissent pas être lues, copiées, modifiées ou effacées par des personnes non autorisées, lors de leur traitement et après leur stockage.

Mesures de développement du concept des autorisations et des droits d'accès, ainsi que leur contrôle et leur consignation :

- concept d'autorisation et mise en œuvre de niveaux d'accès différenciés (données);
- tous les serveurs sont hébergés dans des centres de calcul sûrs dont la sécurité est régulièrement testée ;
- il n'est pas possible d'installer des / logiciels inconnus non autorisés sur le matériel du Fournisseur ;

4. Contrôle de la transmission

Il convient de s'assurer que les données à caractère personnel ne puissent pas être lues, copiées, modifiées ou effacées par des personnes non autorisées, lors de leur transmission électronique ou pendant leur transport ou leur stockage sur un support de données.

Mesures prises lors de la transmission, du transport ou du stockage sur des supports de données (manuel ou électronique), ainsi qu'à l'occasion de la vérification ultérieure :

- cryptage, tunnel (VPN = Virtual Private Network) ;
- enregistrement du type de transmission / des données transmises / des destinataires sécurité des transports.

5. Contrôle de l'introduction

Il convient de s'assurer qu'il est possible de vérifier et de déterminer a posteriori si des données à caractère personnel ont été saisies, modifiées ou effacées, et par qui.

Mesures permettant de vérifier a posteriori si des données ont été saisies, modifiées ou supprimées, et par qui :

- enregistrement des activités du système (lire, modifier, tentatives d'accès non autorisées, analyse régulière des protocoles / analyse spécifique, si nécessaire) ;
- exploitation régulière et systématique de l'enregistrement ;

6. Contrôle des ordres

Il convient de s'assurer que les données à caractère personnel traitées pour le compte d'autrui soient uniquement traitées conformément aux instructions du Client.

Mesures relatives à la délimitation des compétences entre le Client et le Fournisseur :

- les employés sont particulièrement tenus au secret des données clients transmises ;
- les données clients doivent au moins être traitées avec la même diligence que les données « confidentielles » du Fournisseur ;
- gestion de l'exécution du contrat (contrôle / audit de sous-traitants par le Fournisseur, le Client reçoit les résultats de l'auto-évaluation du Fournisseur).

7. Contrôle de disponibilité

Le Fournisseur doit s'assurer que les données à caractère personnel sont protégées contre la destruction ou la perte fortuites.

Mesures garantissant la sécurité des données (destruction / perte) :

- processus de back-up ;
- conservation distincte ;
- duplication des disques durs (par ex. processus RAID) ;
- alimentation sans interruption (ASI) ;
- concept d'archivage des données ;
- contrôle régulier du statut du système (monitoring) ;
- protection contre les virus ;

8. Contrôle de dissociation

Il convient de s'assurer que les données saisies à des fins différentes puissent être traitées séparément.

Mesures relatives au traitement distinct (stockage, modification, effacement, transmission) de données à des fins différentes :

- dissociation du système en temps réel et du système test ;
- séparation fonctionnelle documentée.

- Annexe 2 -

N°	Raison sociale	Adresse	Objectif de la sous-traitance
1	Asanetwork GmbH	Vennhauser Allee 265 40627 Düsseldorf Allemagne	Pour la connexion d'autres logiciels avec les dispositifs de diagnostic dans l'atelier
2	Hella Gutmann Solutions A/S	Lundborgvej 10, 8800 Viborg, Danemark	Pour le bon choix des véhicules
3	TecAlliance GmbH	Steinheilstraße 10 85737 Ismaning Allemagne	Pour l'identification correcte des véhicules en Autriche, en Suisse, en Allemagne, en France et aux Pays-Bas
4	Bisnode Danmark a/s	Gyngemose Parkvej 50, 8 2860 Søborg Danemark	Pour l'identification correcte des véhicules en Finlande, en Norvège et en Suède
5	AUTIG	Skagensgade 1 2630 Taastrup Denmark	Pour l'identification correcte des véhicules au Danemark

6	Jifeline BV	De Hoogjens 11, 4254 XV Sleeuwijk, Pays-Bas	Pour effectuer les diagnostics/les codages par internet.
7	APIZEE	11 rue Blaise Pascal 22300 Lannion FRANCE	Pour effectuer les sessions d'assistance à distance par vidéo/audio/chat
8	AWS	Amazon Web Services Inc. 410 Terry Avenue North, Seattle, WA 98109-5210, USA	Pour fournir des services en ligne
9	TecMotive GmbH	Wilmerdorfer Str. 115-116 10627 Berlin Allemagne	Pour fournir les prestations de services
10	IDnow GmbH	Auenstr. 100 80469 München Allemagne	Vérification d'identité/Vérification de l'employé dans l'atelier
11	FCA Italy S.p.A.	C.so G. Agnelli 200 10135 Turin Italie	Accès authentifié au diagnostic (Security Gateway)

12	Mercedes-Benz AG	Mercedesstraße 120 70372 Stuttgart Allemagne	Diagnostic basé sur un certificat (CeBAS)
13	VOLKSWAGEN AG	Berliner Ring 2 38440 Wolfsburg Deutschlan	Protection du diagnostic des véhicules (SFD)
14	WM SE	Pagenstecherstraße 121, 49090 Osnabrück	Transmission de données pour la facturation de services à distance aux clients de WM
15	OE Service GmbH	Dr. Franz-Palla-Gasse 22 9020 Klagenfurt Österreich	Saisie et récupération de données dans/depuis les portails des constructeurs automobiles
16	Microsoft Ireland Operations Limited	70 Sir John Rogerson's Quay Dublin 2 Irland	Hébergement de l'application
17	WESP	Zuidwal 4-B 5211 JK 's-Hertogenbosch Niederlande	Pilotage de la collecte de données pour les analyses de performance des ateliers. Sur la base des données relatives à l'atelier, des indicateurs et des rapports sont générés pour l'atelier.

18	WERBAS GmbH – Werkstatt-Software	Max-Eyth-Straße 42, 71088 Holzgerlingen	Traitement des données clients & véhicules pour la création et la documentation de la commande
19	Ingenieurbüro Bücher	Zu den Alpen 12, 48301 Nottuln	Traitement des données clients & véhicules pour la création et la documentation de la commande
20	Limex Computer GmbH	Holsten-Mündruper Straße 80 49086 Osnabrück	Traitement des données clients & véhicules pour la création et la documentation de la commande
21	PRM Software AG	Dieselstraße 4, 71277 Rutesheim	Traitement des données clients & véhicules pour la création et la documentation de la commande
22	DVSE Gesellschaft für Datenverar- beitung, Service und Entwicklung mbH	Lise-Meitner-Straße 4, 22941 Bargteheide	Traitement des données clients & véhicules pour la création et la documentation de la commande
23	n-Systems GmbH & Co. KG	Kaiserstraße 95-101a 66133 Saarbrücken	Transfert des données clients & véhicules pour la commande de pièces de rechange

24	drivelog - Der Werkstattpartner für KFZ Ersatzteile und Werkstattzubehör	Robert-Bosch-Straße 8, 73760 Ostfildern	Transfert des données clients & véhicules pour la commande de pièces de rechange
25	auteon GmbH	Körtestraße 2, 10967 Berlin	Transfert des données clients & véhicules pour la commande de pièces de rechange
26	RENAULT s.a.s.	13-15 quai Le Gallo 92100 Boulogne-Billancourt FRANCE	CAN Gateway Unlocking Solution
27	Kia Europe GmbH	Theodor-Heuss-Allee 11 60486 Frankfurt am Main	Secure Diagnostic Access