

**Accord sur le traitement des données**  
**Basé sur les Clauses Contractuelles Types de la Commission Européenne**  
**entre les responsables du traitement et les sous-traitants au sein de l'UE / EEE**  
**en vertu de l'article 28 du règlement (UE) 2016/679 (RGPD)**

## **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.
- (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.
- (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.
- (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.

### **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, 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.
- (c) Les présentes clauses ne doivent pas être interprétées d'une manière contraire aux droits et obligations prévus par le règlement (UE) 2016/679 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 / Obligations 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 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 entraînant, 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. 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) Le sous-traitant dispose de l'autorisation générale du responsable du traitement pour engager un ou plusieurs sous-traitants ultérieurs à partir d'une liste convenue. Le sous-traitant informe expressément par écrit le responsable du traitement de tout changement concernant l'ajout ou le remplacement de sous-traitants ultérieurs qu'il est prévu d'apporter à cette liste au moins 30 jours à l'avance, donnant ainsi au responsable du traitement suffisamment de temps pour émettre des objections à l'encontre de ces changements avant le recrutement du ou des sous-traitants ultérieurs. Le sous-traitant fournit au responsable du traitement les informations nécessaires pour permettre à ce dernier d'exercer son droit d'émettre des objections.
- (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.
- (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.
- (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 violations de données à caractère personnel**

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, 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 ;
  - (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.
- (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.

**ANNEXE I / Liste des Parties**

**Responsable(s) du traitement :** [Identité et coordonnées du ou des responsables du traitement et, le cas échéant, du délégué à la protection des données du responsable du traitement]

<b>Nom :</b>	
<b>Adresse :</b>	
<b>Personne de contact (Nom, fonction et coordonnées) :</b>	
<b>Date d'adhésion :</b>	
<b>Signature :</b>	

**Sous-traitant(s) :** [Identité et coordonnées du ou des sous-traitants et, le cas échéant, du délégué à la protection des données du sous-traitant]

<b>Nom :</b>	<b>Bridgestone Mobility Solutions B.V.</b>
<b>Adresse :</b>	Beethovenstraat 503, 1083 HK Amsterdam, The Netherlands
<b>Personne de contact (Nom, fonction et coordonnées) :</b>	Mr. Civitas Hall Digital Trust Manager & DPO <a href="mailto:digitaltrust@webfleet.com">digitaltrust@webfleet.com</a>
<b>Date d'adhésion :</b>	
<b>Signature :</b>	

**ANNEXE II / Description du traitement**

<b>Catégories de personnes concernées dont les données à caractère personnel sont collectées</b>	<b>Personnes concernées:</b> <ul style="list-style-type: none"> <li>• Conducteurs</li> <li>• Les utilisateurs du Service WEBFLEET, accessible par internet à l'adresse <a href="http://www.webfleet.com">www.webfleet.com</a>.</li> </ul>																																					
<b>Catégories de données à caractère personnel traitées</b>	<b>Données gérées par l'utilisateur et contenu créé :</b> <table border="1" data-bbox="376 560 1469 1966"> <thead> <tr> <th data-bbox="376 560 571 636">Données</th> <th data-bbox="577 560 1118 636">Description</th> <th data-bbox="1125 560 1347 636">Temps de conservation</th> <th data-bbox="1353 560 1469 636">Produit</th> </tr> </thead> <tbody> <tr> <td data-bbox="376 645 571 757">Adresses</td> <td data-bbox="577 645 1118 757">Données de géolocalisation, adresses d'expédition, points de passage et emplacements des stations de recharge pour véhicules électriques utilisés par les gestionnaires de flotte</td> <td data-bbox="1125 645 1347 2020" rowspan="10">90 jours (France : 60 Jours)</td> <td data-bbox="1353 645 1469 757">1,4</td> </tr> <tr> <td data-bbox="376 766 571 837">Données de l'administrateur</td> <td data-bbox="577 766 1118 837">Nom, adresse électronique, adresse IP et numéro de téléphone de l'administrateur (s'ils ont été fournis).</td> <td data-bbox="1353 766 1469 837">1</td> </tr> <tr> <td data-bbox="376 846 571 913">Domaines</td> <td data-bbox="577 846 1118 913">Définitions des géo-zones pour déterminer les zones où les véhicules sont recherchés ou non.</td> <td data-bbox="1353 846 1469 913">1</td> </tr> <tr> <td data-bbox="376 922 571 994">Données sur le conducteur</td> <td data-bbox="577 922 1118 994">Le nom, l'adresse, l'adresse électronique, le permis de conduire et les coordonnées du conducteur.</td> <td data-bbox="1353 922 1469 994">1</td> </tr> <tr> <td data-bbox="376 1003 571 1093">Heure de départ de la flotte et des véhicules</td> <td data-bbox="577 1003 1118 1093">Heure de départ prévue au niveau de la flotte ou du véhicule</td> <td data-bbox="1353 1003 1469 1093">4</td> </tr> <tr> <td data-bbox="376 1102 571 1151">Ordres</td> <td data-bbox="577 1102 1118 1151">Données relatives à l'emploi des conducteurs</td> <td data-bbox="1353 1102 1469 1151">1</td> </tr> <tr> <td data-bbox="376 1160 571 1249">Routes</td> <td data-bbox="577 1160 1118 1249">Itinéraires de conduite prédéfinis, désactivations de commandes, itinéraires planifiés sur les terminaux des conducteurs.</td> <td data-bbox="1353 1160 1469 1249">1</td> </tr> <tr> <td data-bbox="376 1258 571 1352">Messages texte</td> <td data-bbox="577 1258 1118 1352">Messages échangés entre le gestionnaire de flotte et le conducteur par l'intermédiaire des terminaux du conducteur.</td> <td data-bbox="1353 1258 1469 1352">1</td> </tr> <tr> <td data-bbox="376 1361 571 1451">Étiquette de l'utilisateur</td> <td data-bbox="577 1361 1118 1451">Étiquette d'utilisateur/carte d'identification par radiofréquence (RFID) pour utiliser la station de recharge pour VE</td> <td data-bbox="1353 1361 1469 1451">4</td> </tr> <tr> <td data-bbox="376 1460 571 1966">Données sur le véhicule</td> <td data-bbox="577 1460 1118 1966">Spécifications du véhicule individuel, données de géolocalisation et de capteurs, données télématiques supplémentaires, y compris l'immatriculation, le numéro d'identification du véhicule ou la plaque d'immatriculation, la distance parcourue, le temps de conduite, l'heure de la journée, le régime du véhicule et du moteur, la charge et la température du moteur, les données relatives à la remorque, les séquences filmées par les caméras (vers l'intérieur et vers l'extérieur), la pression des pneus, le comportement de conduite, les manœuvres de freinage, de virage et d'accélération, la tension de la batterie, les protocoles de données relatives aux accidents pendant 45 secondes avant et 15 secondes après un accident ; les dispositifs du véhicule, les capteurs, les données de diagnostic liées au service, les données du tachygraphe. Le traitement de données supplémentaires dépend du fait que ces types de données ont été rendus accessibles par le responsable du traitement au sous-traitant, en fonction du type d'abonnement choisi.</td> <td data-bbox="1353 1460 1469 1966">1</td> </tr> </tbody> </table>			Données	Description	Temps de conservation	Produit	Adresses	Données de géolocalisation, adresses d'expédition, points de passage et emplacements des stations de recharge pour véhicules électriques utilisés par les gestionnaires de flotte	90 jours (France : 60 Jours)	1,4	Données de l'administrateur	Nom, adresse électronique, adresse IP et numéro de téléphone de l'administrateur (s'ils ont été fournis).	1	Domaines	Définitions des géo-zones pour déterminer les zones où les véhicules sont recherchés ou non.	1	Données sur le conducteur	Le nom, l'adresse, l'adresse électronique, le permis de conduire et les coordonnées du conducteur.	1	Heure de départ de la flotte et des véhicules	Heure de départ prévue au niveau de la flotte ou du véhicule	4	Ordres	Données relatives à l'emploi des conducteurs	1	Routes	Itinéraires de conduite prédéfinis, désactivations de commandes, itinéraires planifiés sur les terminaux des conducteurs.	1	Messages texte	Messages échangés entre le gestionnaire de flotte et le conducteur par l'intermédiaire des terminaux du conducteur.	1	Étiquette de l'utilisateur	Étiquette d'utilisateur/carte d'identification par radiofréquence (RFID) pour utiliser la station de recharge pour VE	4	Données sur le véhicule	Spécifications du véhicule individuel, données de géolocalisation et de capteurs, données télématiques supplémentaires, y compris l'immatriculation, le numéro d'identification du véhicule ou la plaque d'immatriculation, la distance parcourue, le temps de conduite, l'heure de la journée, le régime du véhicule et du moteur, la charge et la température du moteur, les données relatives à la remorque, les séquences filmées par les caméras (vers l'intérieur et vers l'extérieur), la pression des pneus, le comportement de conduite, les manœuvres de freinage, de virage et d'accélération, la tension de la batterie, les protocoles de données relatives aux accidents pendant 45 secondes avant et 15 secondes après un accident ; les dispositifs du véhicule, les capteurs, les données de diagnostic liées au service, les données du tachygraphe. Le traitement de données supplémentaires dépend du fait que ces types de données ont été rendus accessibles par le responsable du traitement au sous-traitant, en fonction du type d'abonnement choisi.	1
Données	Description	Temps de conservation	Produit																																			
Adresses	Données de géolocalisation, adresses d'expédition, points de passage et emplacements des stations de recharge pour véhicules électriques utilisés par les gestionnaires de flotte	90 jours (France : 60 Jours)	1,4																																			
Données de l'administrateur	Nom, adresse électronique, adresse IP et numéro de téléphone de l'administrateur (s'ils ont été fournis).		1																																			
Domaines	Définitions des géo-zones pour déterminer les zones où les véhicules sont recherchés ou non.		1																																			
Données sur le conducteur	Le nom, l'adresse, l'adresse électronique, le permis de conduire et les coordonnées du conducteur.		1																																			
Heure de départ de la flotte et des véhicules	Heure de départ prévue au niveau de la flotte ou du véhicule		4																																			
Ordres	Données relatives à l'emploi des conducteurs		1																																			
Routes	Itinéraires de conduite prédéfinis, désactivations de commandes, itinéraires planifiés sur les terminaux des conducteurs.		1																																			
Messages texte	Messages échangés entre le gestionnaire de flotte et le conducteur par l'intermédiaire des terminaux du conducteur.		1																																			
Étiquette de l'utilisateur	Étiquette d'utilisateur/carte d'identification par radiofréquence (RFID) pour utiliser la station de recharge pour VE		4																																			
Données sur le véhicule	Spécifications du véhicule individuel, données de géolocalisation et de capteurs, données télématiques supplémentaires, y compris l'immatriculation, le numéro d'identification du véhicule ou la plaque d'immatriculation, la distance parcourue, le temps de conduite, l'heure de la journée, le régime du véhicule et du moteur, la charge et la température du moteur, les données relatives à la remorque, les séquences filmées par les caméras (vers l'intérieur et vers l'extérieur), la pression des pneus, le comportement de conduite, les manœuvres de freinage, de virage et d'accélération, la tension de la batterie, les protocoles de données relatives aux accidents pendant 45 secondes avant et 15 secondes après un accident ; les dispositifs du véhicule, les capteurs, les données de diagnostic liées au service, les données du tachygraphe. Le traitement de données supplémentaires dépend du fait que ces types de données ont été rendus accessibles par le responsable du traitement au sous-traitant, en fonction du type d'abonnement choisi.		1																																			



**Données transactionnelles :**

Données	Description	Temps de conservation	Produit
Accélération (latérale)	Événements de freinage brutal, virages et départs en course	90 jours (France : 60 Jours)	1
Données CAN/OBD	Signaux provenant du réseau de contrôleurs (CAN) ou de l'interface de diagnostic embarquée (OBD) d'un véhicule, comme les indicateurs de dysfonctionnement, les prévisions d'entretien, la surveillance des portes, le niveau de carburant, etc.		1
Messages de position détaillés (pistes)	Localisation actuelle / historique d'un véhicule		1,2
Changements dans l'allumage	Si et quand le contact est mis et coupé		1,2
Odomètre et niveau de carburant momentanés	L'odomètre et le niveau de carburant actuels		1,2
Données du tachygraphe	Heures de travail des conducteurs de véhicules de transport de marchandises et de passagers recueillies par tachygraphe numérique	2 années complètes + année en cours	1
Données sur les trajets et la position des trajets, y compris l'horodatage	Enregistrement du lieu et de l'heure de début et de fin du voyage uniquement - pas d'itinéraire détaillé		1,2
Surveillance du dispositif de suivi	Déplacements de véhicules dont le contact est coupé (remorquage, vol), coupure de courant, protection du dispositif de suivi.	90 jours (France : 60 Jours)	1
Consommation de carburant et d'énergie	Consommation de carburant et/ou d'énergie au cours d'un voyage	2 années complètes + année en cours	1,2,5
Compteur kilométrique journalier	Distance parcourue pendant un voyage		1,2
Codes d'erreur	Indicateurs de dysfonctionnement provenant du bus FMS des poids lourds ou du système OBD.	90 jours (France : 60 Jours)	1
ID unique de la batterie du VE	L'identifiant unique du véhicule électrique pour la mise en correspondance avec les analyses de la batterie. Cet identifiant masque l'identité du véhicule à l'égard du tiers.	2 années complètes + année en cours	5
Données vidéo / caméra	<p>Séquence vidéo face à la route : ne peut pas être déconnectée.</p> <p>Séquence vidéo face au conducteur : peut être déconnectée via le menu de la caméra ou via Webfleet (ou via l'accessoire de couverture de l'objectif).</p> <p>Blocs vidéo de 2 minutes stockés sur la carte SD de la caméra depuis la vue frontale et la vue du conducteur, ainsi que depuis chaque objectif AUX connecté. Dans Webfleet, seules les séquences vidéo basées sur les déclencheurs d'événements suivants sont disponibles :</p> <ul style="list-style-type: none"> <li>- Événements de conduite (freinage brusque, braquage brusque) d'une gravité supérieure au niveau 3</li> <li>- Événements de collision</li> </ul>	<p>90 jours (France : 60 jours)</p> <p>Configurable sur la caméra de 4 minutes à illimité</p>	3

	- IA face au conducteur : conducteur distrait, téléphone portable, tabac, nourriture/boisson, ceinture de sécurité  - IA face à la route : distance de suivi de l'objet		
Numéro VIN	Identifiant unique à 17 caractères pour un véhicule, qui indique les caractéristiques uniques de la voiture, ses spécifications et le fabricant, et qui peut être utilisé pour suivre les rappels, les immatriculations, les demandes de garantie, les vols et la couverture d'assurance, ainsi que pour associer un véhicule à un propriétaire ou à une personne concernée.	2 années complètes + année en cours	1,2

**Données agrégées :**

Données	Description	Temps de conservation	Produit
Statistiques sur les conducteurs	Comportement des conducteurs agrégés dans le temps	2 années complètes + année en cours	1
Événements de conduite (le cas échéant)	Comportement de conduite dépassant le seuil de la conduite normale	90 jours (France : 60 Jours)	1,2
Cartes de carburant	Achats de carburant avec des cartes de paiement de carburant		1
KPIs	Indicateurs agrégés de conduite et de comportement utilisés dans le score OptiDrive	2 années complètes + année en cours	1
Livre de bord	Carnet de route du conducteur		1
Rapports	Des rapports configurables permettant de combiner toutes les données mentionnées ci-dessus, qui doivent être configurés par l'administrateur du compte.	30 jours à 36 mois, selon la configuration de l'administrateur du compte, mais des valeurs par défaut raisonnables s'appliquent.	1,2
Événements liés à la vitesse et aux excès de vitesse (le cas échéant)	Vitesse actuelle comparée à la limite de vitesse locale à partir de données cartographiques	90 Jours	1,2
Statistiques sur les véhicules	Événements de conduite et données sur l'empreinte carbone agrégés dans le temps	2 années complètes + année en cours	1
Statistiques sur le temps de travail	Enregistrement et sortie du chauffeur/co-pilote		1

**Liste des produits :**

1. Webfleet et dispositifs LINK
2. OEM.Connect
3. Dashcam
4. Chargement intelligent des VE
5. Analyse des batteries des VE

**Veillez noter** que le client peut demander la suppression des données qui ont été traitées en votre nom en contactant notre équipe d'assistance technique par téléphone et/ou par courriel.

Les données collectées aux fins de la déclaration des déplacements fiscaux ou de la déclaration du temps de travail, comme la gestion des tachygraphes, peuvent être soumises à d'autres législations pertinentes. Le

	<i>responsable du traitement des données a la responsabilité de déterminer si cette législation peut empêcher le responsable du traitement de procéder à l'effacement des données.</i>
<b>Données sensibles traitées</b>	Aucune
<b>Nature du traitement</b>	Dans le cadre de la fourniture du service et des produits WEBFLEET au client, conformément aux Conditions Générales de WEBFLEET.
<b>Finalité(s) pour lesquelles les données à caractère personnel sont collectées pour le compte du responsable du traitement</b>	Fournir le service WEBFLEET tel qu'il est décrit dans les Conditions Générales de WEBFLEET, y compris, mais sans s'y limiter, le traitement (i) du suivi des véhicules ; (ii) du comportement de conduite et des économies de carburant ; (iii) de la communication bidirectionnelle avec le conducteur ; (iv) du tachygraphe et des informations sur le temps de conduite restant ; (v) de rapports détaillés ; (vi) de l'intégration de solutions de tiers / de l'intégration commerciale ; (vii) des données de la caméra embarquée ; (viii) Emplacement de la station de recharge des VE ; (ix) Analyse de la batterie des VE
<b>Pour les transferts à des sous-traitants (ultérieurs), veuillez également préciser l'objet, la nature, et la durée du traitement</b>	Le traitement est décrit dans la liste des Sous-Traitants et est lié à la fourniture du Service et des Produits WEBFLEET. La Durée du traitement est la même que la durée du traitement par le Sous-traitant.

## ANNEXE III / Mesures Techniques et Organisationnelles, Y Compris Mesures Techniques et Organisationnelles Visant À Garantir La Sécurité des Données

Le sous-traitant maintient une certification ISO/IEC 27001 qui couvre les mesures techniques et organisationnelles ci-dessous et qui est disponible sur demande.

<b>Confidentialité</b>  <b>Art.32 (1) (b) RGPD</b>	<b>(i) Contrôle d'accès (bâtiment   bureaux   centre de données)</b> Empêcher tout accès non autorisé aux systèmes de traitement des données dans lesquels des données à caractère personnel sont traitées		
	<table border="0"> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Système d'alarme</li> <li><input checked="" type="checkbox"/> Système de contrôle d'accès automatique</li> <li><input checked="" type="checkbox"/> Détecteurs photoélectriques / Détecteurs de mouvement</li> <li><input checked="" type="checkbox"/> Gestion des clés (émission de clés, etc.)</li> <li><input checked="" type="checkbox"/> Enregistrement des visiteurs</li> <li><input checked="" type="checkbox"/> Sélection minutieuse des agents de sécurité</li> <li><input checked="" type="checkbox"/> Protection des puits de bâtiments</li> <li><input checked="" type="checkbox"/> Système de verrouillage par carte à puce / transpondeur</li> <li><input checked="" type="checkbox"/> Système de verrouillage manuel (usage limité aux employés clés à utiliser en cas de défaillance des systèmes de contrôle d'accès.</li> </ul> </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Vidéosurveillance aux points d'entrée (bureaux et centres de données).</li> <li><input checked="" type="checkbox"/> Serrures de sécurité</li> <li><input checked="" type="checkbox"/> Gestion des visiteurs aux bureaux d'accueil</li> <li><input checked="" type="checkbox"/> Sélection rigoureuse du personnel de nettoyage</li> <li><input checked="" type="checkbox"/> Port visible des badges d'accès obligatoire</li> <li><input checked="" type="checkbox"/> Un contrôle d'accès séparé, spécifique et documenté aux centres de données et aux salles de serveurs pour les personnes autorisées est mis en place. L'accès des personnes autorisées est documenté par le nom et le numéro de carte ou de jeton. Pour les centres de données, des systèmes de contrôle d'accès distincts sont mis en place</li> </ul> </td> </tr> </table>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Système d'alarme</li> <li><input checked="" type="checkbox"/> Système de contrôle d'accès automatique</li> <li><input checked="" type="checkbox"/> Détecteurs photoélectriques / Détecteurs de mouvement</li> <li><input checked="" type="checkbox"/> Gestion des clés (émission de clés, etc.)</li> <li><input checked="" type="checkbox"/> Enregistrement des visiteurs</li> <li><input checked="" type="checkbox"/> Sélection minutieuse des agents de sécurité</li> <li><input checked="" type="checkbox"/> Protection des puits de bâtiments</li> <li><input checked="" type="checkbox"/> Système de verrouillage par carte à puce / transpondeur</li> <li><input checked="" type="checkbox"/> Système de verrouillage manuel (usage limité aux employés clés à utiliser en cas de défaillance des systèmes de contrôle d'accès.</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Vidéosurveillance aux points d'entrée (bureaux et centres de données).</li> <li><input checked="" type="checkbox"/> Serrures de sécurité</li> <li><input checked="" type="checkbox"/> Gestion des visiteurs aux bureaux d'accueil</li> <li><input checked="" type="checkbox"/> Sélection rigoureuse du personnel de nettoyage</li> <li><input checked="" type="checkbox"/> Port visible des badges d'accès obligatoire</li> <li><input checked="" type="checkbox"/> Un contrôle d'accès séparé, spécifique et documenté aux centres de données et aux salles de serveurs pour les personnes autorisées est mis en place. L'accès des personnes autorisées est documenté par le nom et le numéro de carte ou de jeton. Pour les centres de données, des systèmes de contrôle d'accès distincts sont mis en place</li> </ul>
	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Système d'alarme</li> <li><input checked="" type="checkbox"/> Système de contrôle d'accès automatique</li> <li><input checked="" type="checkbox"/> Détecteurs photoélectriques / Détecteurs de mouvement</li> <li><input checked="" type="checkbox"/> Gestion des clés (émission de clés, etc.)</li> <li><input checked="" type="checkbox"/> Enregistrement des visiteurs</li> <li><input checked="" type="checkbox"/> Sélection minutieuse des agents de sécurité</li> <li><input checked="" type="checkbox"/> Protection des puits de bâtiments</li> <li><input checked="" type="checkbox"/> Système de verrouillage par carte à puce / transpondeur</li> <li><input checked="" type="checkbox"/> Système de verrouillage manuel (usage limité aux employés clés à utiliser en cas de défaillance des systèmes de contrôle d'accès.</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Vidéosurveillance aux points d'entrée (bureaux et centres de données).</li> <li><input checked="" type="checkbox"/> Serrures de sécurité</li> <li><input checked="" type="checkbox"/> Gestion des visiteurs aux bureaux d'accueil</li> <li><input checked="" type="checkbox"/> Sélection rigoureuse du personnel de nettoyage</li> <li><input checked="" type="checkbox"/> Port visible des badges d'accès obligatoire</li> <li><input checked="" type="checkbox"/> Un contrôle d'accès séparé, spécifique et documenté aux centres de données et aux salles de serveurs pour les personnes autorisées est mis en place. L'accès des personnes autorisées est documenté par le nom et le numéro de carte ou de jeton. Pour les centres de données, des systèmes de contrôle d'accès distincts sont mis en place</li> </ul>	
	<b>(ii) Contrôle d'accès (systèmes)</b> Empêcher l'utilisation non autorisée des systèmes de traitement des données		
<table border="0"> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Attribution des droits des utilisateurs</li> <li><input checked="" type="checkbox"/> Attribution de mots de passe</li> <li><input checked="" type="checkbox"/> Authentification avec nom d'utilisateur / mot de passe.</li> <li><input checked="" type="checkbox"/> Utilisation de systèmes de prévention des intrusions</li> <li><input checked="" type="checkbox"/> Utilisation de pare-feu matériels</li> <li><input checked="" type="checkbox"/> Définition des profils d'utilisateurs</li> <li><input checked="" type="checkbox"/> Mesures supplémentaires : pare-feu pour les applications web, analyses régulières de la vulnérabilité, tests de pénétration réguliers, gestion des correctifs, exigences minimales en matière de complexité des mots de passe et de changements forcés des mots de passe, utilisation de scanners de virus.</li> </ul> </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Attribution de profils d'utilisateurs aux systèmes informatiques.</li> <li><input checked="" type="checkbox"/> Utilisation de la technologie VPN</li> <li><input checked="" type="checkbox"/> Cryptage des supports de stockage mobiles</li> <li><input checked="" type="checkbox"/> Utilisation de l'administration centrale du smartphone (par exemple : effacement à distance du smartphone).</li> <li><input checked="" type="checkbox"/> Cryptage de disque sur les ordinateurs portables / notebooks.</li> <li><input checked="" type="checkbox"/> Utilisation d'un pare-feu logiciel (office clients).</li> </ul> </td> </tr> </table>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Attribution des droits des utilisateurs</li> <li><input checked="" type="checkbox"/> Attribution de mots de passe</li> <li><input checked="" type="checkbox"/> Authentification avec nom d'utilisateur / mot de passe.</li> <li><input checked="" type="checkbox"/> Utilisation de systèmes de prévention des intrusions</li> <li><input checked="" type="checkbox"/> Utilisation de pare-feu matériels</li> <li><input checked="" type="checkbox"/> Définition des profils d'utilisateurs</li> <li><input checked="" type="checkbox"/> Mesures supplémentaires : pare-feu pour les applications web, analyses régulières de la vulnérabilité, tests de pénétration réguliers, gestion des correctifs, exigences minimales en matière de complexité des mots de passe et de changements forcés des mots de passe, utilisation de scanners de virus.</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Attribution de profils d'utilisateurs aux systèmes informatiques.</li> <li><input checked="" type="checkbox"/> Utilisation de la technologie VPN</li> <li><input checked="" type="checkbox"/> Cryptage des supports de stockage mobiles</li> <li><input checked="" type="checkbox"/> Utilisation de l'administration centrale du smartphone (par exemple : effacement à distance du smartphone).</li> <li><input checked="" type="checkbox"/> Cryptage de disque sur les ordinateurs portables / notebooks.</li> <li><input checked="" type="checkbox"/> Utilisation d'un pare-feu logiciel (office clients).</li> </ul>	
<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Attribution des droits des utilisateurs</li> <li><input checked="" type="checkbox"/> Attribution de mots de passe</li> <li><input checked="" type="checkbox"/> Authentification avec nom d'utilisateur / mot de passe.</li> <li><input checked="" type="checkbox"/> Utilisation de systèmes de prévention des intrusions</li> <li><input checked="" type="checkbox"/> Utilisation de pare-feu matériels</li> <li><input checked="" type="checkbox"/> Définition des profils d'utilisateurs</li> <li><input checked="" type="checkbox"/> Mesures supplémentaires : pare-feu pour les applications web, analyses régulières de la vulnérabilité, tests de pénétration réguliers, gestion des correctifs, exigences minimales en matière de complexité des mots de passe et de changements forcés des mots de passe, utilisation de scanners de virus.</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Attribution de profils d'utilisateurs aux systèmes informatiques.</li> <li><input checked="" type="checkbox"/> Utilisation de la technologie VPN</li> <li><input checked="" type="checkbox"/> Cryptage des supports de stockage mobiles</li> <li><input checked="" type="checkbox"/> Utilisation de l'administration centrale du smartphone (par exemple : effacement à distance du smartphone).</li> <li><input checked="" type="checkbox"/> Cryptage de disque sur les ordinateurs portables / notebooks.</li> <li><input checked="" type="checkbox"/> Utilisation d'un pare-feu logiciel (office clients).</li> </ul>		
<b>(iii) Contrôle d'accès ( données )</b> Garantir que les utilisateurs autorisés d'un système de traitement des données ne puissent accéder qu'aux données pour lesquelles ils sont autorisés, et (ii) empêcher que les données à caractère personnel soient lues lorsque les données sont en cours d'utilisation, en mouvement ou au repos sans autorisation.			
<table border="0"> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Création d'un concept d'autorisation</li> <li><input checked="" type="checkbox"/> Nombre d'administrateurs réduit au « strict nécessaire ».</li> <li><input checked="" type="checkbox"/> Journalisation des accès aux applications, notamment lors de la saisie, de la modification et de la suppression des données.</li> <li><input checked="" type="checkbox"/> Assainissement sécurisé des médias avant leur réutilisation.</li> <li><input checked="" type="checkbox"/> Utilisation de broyeurs ou de services (si possible, avec un sceau de confidentialité).</li> </ul> </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Chiffrement des disques (bandes de sauvegarde pour le stockage hors site, ordinateurs portables).</li> <li><input checked="" type="checkbox"/> Gestion des droits par les administrateurs du système.</li> <li><input checked="" type="checkbox"/> Politique en matière de mots de passe, y compris la longueur des mots de passe, la gestion des changements de mots de passe.</li> <li><input checked="" type="checkbox"/> Stockage sécurisé des supports de données</li> <li><input checked="" type="checkbox"/> Journalisation de la destruction des supports sécurisés.</li> <li><input checked="" type="checkbox"/> Destruction conforme des supports de données (DIN 66399).</li> </ul> </td> </tr> </table>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Création d'un concept d'autorisation</li> <li><input checked="" type="checkbox"/> Nombre d'administrateurs réduit au « strict nécessaire ».</li> <li><input checked="" type="checkbox"/> Journalisation des accès aux applications, notamment lors de la saisie, de la modification et de la suppression des données.</li> <li><input checked="" type="checkbox"/> Assainissement sécurisé des médias avant leur réutilisation.</li> <li><input checked="" type="checkbox"/> Utilisation de broyeurs ou de services (si possible, avec un sceau de confidentialité).</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Chiffrement des disques (bandes de sauvegarde pour le stockage hors site, ordinateurs portables).</li> <li><input checked="" type="checkbox"/> Gestion des droits par les administrateurs du système.</li> <li><input checked="" type="checkbox"/> Politique en matière de mots de passe, y compris la longueur des mots de passe, la gestion des changements de mots de passe.</li> <li><input checked="" type="checkbox"/> Stockage sécurisé des supports de données</li> <li><input checked="" type="checkbox"/> Journalisation de la destruction des supports sécurisés.</li> <li><input checked="" type="checkbox"/> Destruction conforme des supports de données (DIN 66399).</li> </ul>	
<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Création d'un concept d'autorisation</li> <li><input checked="" type="checkbox"/> Nombre d'administrateurs réduit au « strict nécessaire ».</li> <li><input checked="" type="checkbox"/> Journalisation des accès aux applications, notamment lors de la saisie, de la modification et de la suppression des données.</li> <li><input checked="" type="checkbox"/> Assainissement sécurisé des médias avant leur réutilisation.</li> <li><input checked="" type="checkbox"/> Utilisation de broyeurs ou de services (si possible, avec un sceau de confidentialité).</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Chiffrement des disques (bandes de sauvegarde pour le stockage hors site, ordinateurs portables).</li> <li><input checked="" type="checkbox"/> Gestion des droits par les administrateurs du système.</li> <li><input checked="" type="checkbox"/> Politique en matière de mots de passe, y compris la longueur des mots de passe, la gestion des changements de mots de passe.</li> <li><input checked="" type="checkbox"/> Stockage sécurisé des supports de données</li> <li><input checked="" type="checkbox"/> Journalisation de la destruction des supports sécurisés.</li> <li><input checked="" type="checkbox"/> Destruction conforme des supports de données (DIN 66399).</li> </ul>		
<b>(iv) Traitement séparé</b> Veiller à ce que les données collectées à des fins différentes puissent être traitées séparément :			
<table border="0"> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Création d'un concept d'autorisation</li> <li><input checked="" type="checkbox"/> Mise à disposition d'enregistrements avec des attributs de finalité / champs de données.</li> </ul> </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Séparation logique des clients (dans les logiciels)</li> <li><input checked="" type="checkbox"/> Dans les données pseudonymisées : la séparation du fichier de cartographie et le stockage sur un système informatique sécurisé distinct.</li> </ul> </td> </tr> </table>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Création d'un concept d'autorisation</li> <li><input checked="" type="checkbox"/> Mise à disposition d'enregistrements avec des attributs de finalité / champs de données.</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Séparation logique des clients (dans les logiciels)</li> <li><input checked="" type="checkbox"/> Dans les données pseudonymisées : la séparation du fichier de cartographie et le stockage sur un système informatique sécurisé distinct.</li> </ul>	
<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Création d'un concept d'autorisation</li> <li><input checked="" type="checkbox"/> Mise à disposition d'enregistrements avec des attributs de finalité / champs de données.</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Séparation logique des clients (dans les logiciels)</li> <li><input checked="" type="checkbox"/> Dans les données pseudonymisées : la séparation du fichier de cartographie et le stockage sur un système informatique sécurisé distinct.</li> </ul>		

	<input checked="" type="checkbox"/> Droits de la base de données approuvés et documentés.	<input checked="" type="checkbox"/> Séparation des systèmes de production et d'essai
<b>Intégrité</b> <b>Art.32 (1) (b) RGPD</b>	<b>(i) Contrôle du transfert</b> <p>pour garantir que les données à caractère personnel ne puissent être lues, copiées ou modifiées pendant la transmission électronique ou pendant le transport ou le stockage sur disque. En outre, contrôler et déterminer à quels organismes le transfert des données à caractère personnel fournies par les équipements de communication de données est autorisé :</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Création de lignes dédiées ou de tunnels VPN</li> <li><input checked="" type="checkbox"/> Documentation des destinataires des données et des délais de mise à disposition des données, y compris les délais de suppression convenus.</li> <li><input checked="" type="checkbox"/> Pendant le transport physique, sélection minutieuse du personnel de transport et des véhicules (bande de stockage hors site).</li> <li><input checked="" type="checkbox"/> Cryptage des disques (bandes de sauvegarde pour le stockage hors site).</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Divulgaration de données sous forme anonyme ou pseudonyme.</li> <li><input checked="" type="checkbox"/> Création d'une vue d'ensemble des opérations régulières de demande et de livraison.</li> <li><input checked="" type="checkbox"/> Pendant le transport physique, sécuriser les conteneurs de transport / emballages (ruban adhésif de stockage hors site).</li> <li><input checked="" type="checkbox"/> Cryptage TLS de toutes les communications (client Web, API, applications mobiles).</li> </ul>
	<b>(ii) Contrôle des entrées</b> <p>assurer, contrôler ultérieurement et déterminer si et par qui des données personnelles ont été introduites, modifiées ou supprimées dans les systèmes de traitement des données :</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Journalisation de l'entrée, de la modification et de la suppression des données.</li> <li><input checked="" type="checkbox"/> Traçabilité de la saisie, de la modification et de la suppression des données par des noms d'utilisateurs individuels (et non par des groupes d'utilisateurs).</li> <li><input checked="" type="checkbox"/> Octroi de droits pour la saisie, la modification ou la suppression de données sur la base d'un concept d'autorisation.</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Création d'une vue d'ensemble de quelles applications sont autorisées à saisir, modifier ou supprimer quelles données.</li> <li><input checked="" type="checkbox"/> Conservation des formulaires, par lesquels les données ont été acquises lors d'un traitement automatisé.</li> </ul>
<b>Disponibilité et résilience</b> <b>Art.32 (1) (b) RGPD</b>	<b>(i) Contrôle des disponibilités</b> <p>pour s'assurer que les données personnelles sont protégées contre la destruction ou la perte accidentelle :</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Alimentation électrique ininterrompue ( ASI )</li> <li><input checked="" type="checkbox"/> Dispositifs de surveillance de la température et de l'humidité dans les salles de serveurs.</li> <li><input checked="" type="checkbox"/> Systèmes de détection d'incendie et de fumée</li> <li><input checked="" type="checkbox"/> Alarme en cas de détection d'une entrée non autorisée dans les salles de serveurs.</li> <li><input checked="" type="checkbox"/> Test de récupération des données</li> <li><input checked="" type="checkbox"/> Stockage hors site sécurisé des sauvegardes de données.</li> <li><input checked="" type="checkbox"/> En zone inondable : salles de serveurs au-dessus de la limite des eaux.</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Climatisation des salles de serveurs</li> <li><input checked="" type="checkbox"/> Blocs multiprises de protection dans les salles de serveurs.</li> <li><input checked="" type="checkbox"/> Extincteurs dans les salles de serveurs</li> <li><input checked="" type="checkbox"/> Création d'un concept de sauvegarde et de récupération.</li> <li><input checked="" type="checkbox"/> Préparer un plan d'intervention d'urgence</li> <li><input checked="" type="checkbox"/> Salles de serveurs non situées sous des installations sanitaires.</li> <li><input checked="" type="checkbox"/> Deux centres de données en Allemagne dans une configuration active/active pour soutenir la résilience.</li> </ul>
<b>Processus d'examen, d'analyse et d'évaluation réguliers</b> <b>Art.32 (1) (d) ; (Art.25 .du RGPD)</b>	<b>(i) Contrôle des instructions</b> <p>pour veiller à ce que les données à caractère personnel traitées pour le compte d'un Responsable du traitement ne soient traitées que conformément aux instructions de ce dernier :</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Sélection du contractant via l'examen de l'historique (en particulier la sécurité des données).</li> <li><input checked="" type="checkbox"/> Instructions écrites au contractant (par exemple, par le DPA) (RGPD)</li> <li><input checked="" type="checkbox"/> Dans la mesure où cela est requis : s'assurer que les contractants ont nommé des Délégués à la Protection des Données.</li> <li><input checked="" type="checkbox"/> Des droits de contrôle effectifs sur les sous-traitants ont été convenus.</li> <li><input checked="" type="checkbox"/> Système de Management de la Sécurité de l'Information (SMSI)</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Examen préalable de la documentation et des mesures de sécurité prises par le contractant.</li> <li><input checked="" type="checkbox"/> Obligation des employés du contractant de préserver la confidentialité des données (RGPD).</li> <li><input checked="" type="checkbox"/> Assurer la destruction sécurisée des données après la fin du contrat.</li> <li><input checked="" type="checkbox"/> Examen continu des contractants et de leurs activités.</li> <li><input checked="" type="checkbox"/> Gestion de la réponse aux incidents</li> <li><input checked="" type="checkbox"/> Protection des données par conception et par défaut (art.25 (2) RGPD).</li> </ul>

#### **ANNEXE IV / Dispositions complémentaires**

Le Responsable du traitement et le Sous-traitant conviennent de compléter les Clauses par les dispositions suivantes :

- (a) Si une disposition des présentes Clauses est à tout moment invalide ou inapplicable en vertu de la loi actuelle ou future, de la jurisprudence ou des directives et décisions d'application de l'autorité de surveillance compétente, elle sera inefficace dans la mesure, mais seulement dans la mesure, de cette invalidation ou inapplicabilité sans invalider les autres parties des présentes et les autres parties des présentes Clauses resteront pleinement en vigueur. Dans le cas où une disposition des présentes clauses serait jugée invalide ou inapplicable, les parties négocieront de bonne foi pour remplacer cette disposition par une autre disposition qui sera valide ou applicable et qui sera aussi proche que possible des dispositions jugées invalides ou inapplicables.
- (b) Toute modification des présentes clauses doit être faite par écrit sous peine de nullité, sauf indication contraire.
- (c) Toutes les dispositions des Clauses relatives au droit de résiliation s'appliquent également directement au contrat qui constitue la base de la coopération (par exemple, un accord de services sur la base duquel le Sous-traitant fournit des services qui impliquent le traitement de données à caractère personnel).
- (d) Les présentes clauses sont régies par le droit néerlandais.

## Annexe V / Liste de Sous-Traitants Ultérieurs

Le responsable du traitement a autorisé, par le biais d'une Autorisation Générale, le recours aux Sous-traitants ultérieurs suivants :

Société	Emplacement	Services	Produit ou service applicable *
<b>Bayerische Motoren Werke Aktiengesellschaft (BMW)</b>	Petuelring 130, 80788 Munich, Allemagne	Fourniture de données API concernant leurs véhicules du groupe BMW (BMW, MINI) à Bridgestone Mobility Solutions B.V. et ses filiales, afin de permettre la fourniture du service WEBFLEET à ses clients.	2
<b>BIA Power Grid, S.L.</b>	Paseo de Gracia 50, 08007 Barcelona, Espagne	Fourniture de données API concernant les stations de recharge de VE (appartenant au client ou privées) à Bridgestone Mobility Solutions B.V. et à ses filiales, dans le cadre de la fourniture du service de recharge de VE aux clients de WEBFLEET.	4
<b>DAKO Systemtechnik und Service GmbH &amp; Co. KG</b>	Brusseler Str. 7-11. 07747 Jena, Allemagne	Gestionnaire de tachygraphe WEBFLEET	1
<b>Ford Smart Mobility U.K. Limited</b>	Business Unit 2, Broadcast Centre, Here East, Queen Elizabeth Olympic Park, Stratford, Londres, Angleterre, E20 3BS	Fourniture de données API concernant les véhicules de marque Ford à Bridgestone Mobility Solutions B.V. et à ses filiales, afin de permettre la fourniture du service WEBFLEET à ses clients.	2
<b>Lytix, INC.</b>	170 Midsummer Blvd, Milton Keynes MK9 1BP, Royaume-Uni ; et HaMada Street 7, Yokne'am Illit, Israël	Services liés aux appareils photo (matériel et logiciels), y compris l'assistance à la clientèle  Lytix utilise les Sous-traitants ultérieurs suivants : <ul style="list-style-type: none"> <li>• Amazon Web Services EMEA SRL (Hosting)   38 Avenue John F. Kennedy, L-1855, Luxembourg</li> <li>• Logz.io UK Limited (data monitoring)   37 Broadhurst Gardens, Londres, Royaume-Uni, NW6 3QT</li> </ul>	3
<b>TomTom International B.V.</b>	De Ruijterkade 154 1011 AC Amsterdam Pays-Bas	Pour les clients qui ont souscrit au service WEBFLEET, ces services sous-traités par le Sous-traitant seront fournis par TomTom International en tant que partenaire stratégique. Les services comprennent la circulation, les caméras de sécurité, la recherche locale, les services d'état des routes, les informations météorologiques et les prix des carburants.	1
<b>Volytica Diagnostics GmbH</b>	Theresienstrasse 18, 01097 Dresden, Allemagne	Fourniture de données analytiques sur la batterie HV, y compris l'état de la batterie, l'état de santé, les prévisions et d'autres valeurs statistiques. Un identifiant unique est communiqué à ce fournisseur via l'API afin de masquer l'identité de la personne concernée ou du véhicule.	5
<b>Webfleet Solutions Development Germany GmbH</b>	Inselstrasse 22, 04103 Leipzig, Allemagne	Pôle technologique sécurisé certifié ISO 27001 qui comprend les technologies de l'information, le développement de logiciels sécurisés et les centres de données colocalisés en lien avec la plateforme de services télématiques WEBFLEET fournie à la société Bridgestone Mobility Solutions B.V..	1,2,3,4,5

**\* Liste de produits / Services :**

1. Webfleet et dispositifs LINK
2. OEM.Connect
3. Dashcam
4. Chargement intelligent des VE
5. Analyse des batteries des VE