Journal officiel
de l'Union européenne

FR
Série L

2026/699

3.6.2026

RÈGLEMENT DÉLÉGUÉ (UE) 2026/699 DE LA COMMISSION

du 23 mars 2026

modifiant le règlement (UE) 2018/858 du Parlement européen et du Conseil en ce qui concerne l'accès normalisé aux informations du système de diagnostic embarqué des véhicules et aux informations sur la réparation et l'entretien, et les prescriptions et procédures pour l'accès sécurisé aux informations du système de diagnostic embarqué

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2018/858 du Parlement européen et du Conseil du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, modifiant les règlements (CE) n° 715/2007 et (CE) n° 595/2009 et abrogeant la directive 2007/46/CE ([1]), et notamment son article 61, paragraphe 11,

considérant ce qui suit:

(1) Le règlement (UE) 2018/858 impose aux constructeurs de véhicules de fournir aux opérateurs indépendants un accès illimité, normalisé et non discriminatoire aux informations du système de diagnostic embarqué (OBD) des véhicules, aux équipements et outils de diagnostic ou autres, y compris les références complètes et les téléchargements disponibles du logiciel applicable, ainsi qu'aux informations sur la réparation et l'entretien des véhicules.

(2) L'article 4, paragraphe 5, point d), du règlement (UE) 2019/2144 du Parlement européen et du Conseil ([2]) (ci-après les «règles de l'Union en matière de cybersécurité») prévoit que les constructeurs doivent se conformer aux exigences applicables en matière de protection des véhicules contre les cyberattaques. Les prescriptions techniques et les procédures d'essai adoptées à cet effet s'appuient sur les prescriptions du règlement ONU n° 155 ([3]).

(3) Conformément au règlement ONU n° 155, les prescriptions techniques et les procédures d'essai qui y sont prévues s'entendent toutefois sans préjudice de la législation de l'Union régissant l'accès des parties autorisées au véhicule et à ses données, fonctions et ressources et les conditions de cet accès.

(4) Le règlement (UE) 2018/858 interdit à un constructeur de véhicules de subordonner l'accès des opérateurs indépendants aux informations sur la réparation et l'entretien des véhicules ainsi qu'à celles du système OBD, y compris l'accès en écriture à ces informations, à des conditions autres que celles qui y sont prévues, telles que celles motivées par la cybersécurité.

([1]) JO L 151 du 14.6.2018, p. 1, ELI: http://data.europa.eu/eli/reg/2018/858/oj.

([2]) Règlement (UE) 2019/2144 du Parlement européen et du Conseil du 27 novembre 2019 relatif aux prescriptions applicables à la réception par type des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, en ce qui concerne leur sécurité générale et la protection des occupants des véhicules et des usagers vulnérables de la route, modifiant le règlement (UE) 2018/858 du Parlement européen et du Conseil et abrogeant les règlements (CE) n° 78/2009, (CE) n° 79/2009 et (CE) n° 661/2009 du Parlement européen et du Conseil et les règlements (CE) n° 631/2009, (UE) n° 406/2010, (UE) n° 672/2010, (UE) n° 1003/2010, (UE) n° 1005/2010, (UE) n° 1008/2010, (UE) n° 1009/2010, (UE) n° 19/2011, (UE) n° 109/2011, (UE) n° 458/2011, (UE) n° 65/2012, (UE) n° 130/2012, (UE) n° 347/2012, (UE) n° 351/2012, (UE) n° 1230/2012 et (UE) 2015/166 de la Commission (JO L 325 du 16.12.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/2144/oj).

([3]) Règlement ONU n° 155 — Prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne la cybersécurité et de leurs systèmes de gestion de la cybersécurité [2021/387] (JO L 82 du 9.3.2021, p. 30, ELI: http://data.europa.eu/eli/reg/2021/387/oj).

(5) Le cadre juridique de l'Union régissant les mesures de cybersécurité à appliquer à l'accès aux informations du système OBD des véhicules n'est pas complet. Les règles de l'Union en matière de cybersécurité exigent des constructeurs qu'ils protègent les véhicules contre les cyberattaques, mais elles limitent l'effet des prescriptions techniques précisant les mesures applicables en ce qui concerne l'accès aux données des véhicules. Par ailleurs, les règles relatives à l'accès aux informations du système OBD des véhicules ne tiennent pas suffisamment compte de la cybersécurité. En conséquence, les constructeurs de véhicules se heurtent à d'importantes contraintes juridiques qui les empêchent d'appliquer des mesures efficaces de protection du véhicule contre les cyberattaques liées à l'accès aux informations du système OBD des véhicules.

(6) Il est donc nécessaire de veiller à ce que les constructeurs automobiles soient autorisés à appliquer des mesures de cybersécurité efficaces et proportionnées tout en accordant un accès aux informations du système OBD.

(7) L'augmentation des menaces pesant sur la cybersécurité et l'adoption, dans ce contexte, des règles de l'Union imposant aux constructeurs de véhicules de protéger les véhicules contre les cyberattaques constituent des évolutions techniques et réglementaires justifiant de modifier l'annexe X du règlement précité.

(8) Afin de permettre aux constructeurs de faire face à ces menaces tout en assurant l'accès effectif des opérateurs indépendants aux informations du système OBD des véhicules, le règlement (UE) 2018/858 devrait énoncer les conditions et décrire les procédures que les constructeurs de véhicules sont autorisés à appliquer pour garantir aux opérateurs indépendants un accès sécurisé aux informations du système OBD.

(9) En fonction de la nature et des conséquences de l'accès demandé, les constructeurs de véhicules devraient être autorisés à exiger des fabricants d'outils de diagnostic utilisés pour accéder aux informations du système OBD qu'ils authentifient l'outil et l'opérateur indépendant qui demande l'accès, ou son salarié, et qu'ils garantissent la traçabilité en consignant et en conservant les informations pertinentes relatives à cet accès. Ils devraient également être autorisés, dans des cas spécifiques, à exiger la connexion au serveur du constructeur du véhicule.

(10) Afin de protéger l'égalité des conditions de concurrence, il convient de pseudonymiser les informations relatives aux opérateurs indépendants qui demandent à accéder aux informations du système OBD des véhicules.

(11) Pour que les constructeurs de véhicules puissent gérer les dépendances, comme l'exigent les règles applicables en matière de cybersécurité des véhicules, ils devraient être autorisés à vérifier que les outils de diagnostic et leurs fabricants respectent les normes de cybersécurité applicables et les mises en œuvre pertinentes en matière de sécurité.

(12) En cas d'incidents de cybersécurité, d'abus graves ou d'incidents impliquant la responsabilité du constructeur de véhicules, les constructeurs de véhicules devraient pouvoir obtenir des informations sur des cas spécifiques d'accès et suspendre temporairement, s'il y a lieu et sous le contrôle de l'autorité compétente en matière de réception, l'accès d'un outil, ainsi que de l'opérateur indépendant ou de son salarié.

(13) Les constructeurs de véhicules devraient fournir toutes les informations techniques nécessaires aux fabricants d'outils de diagnostic génériques suffisamment longtemps avant la mise sur le marché d'un véhicule pour leur permettre de fournir un service adéquat aux réparateurs indépendants.

(14) Outre qu'il prévoit les conditions et procédures d'un accès sécurisé aux informations du système OBD, le présent règlement devrait faciliter l'accès aux informations du système OBD des véhicules et aux informations sur la réparation et l'entretien, en tenant compte des progrès techniques.

(15) Le catalogue d'informations à mettre à disposition par les constructeurs de véhicules devrait être clarifié et mis à jour, notamment en tenant compte des besoins liés à la réparation et à l'entretien des batteries de véhicules et des nouveaux systèmes d'aide à la conduite.

(16) Lorsque les constructeurs de véhicules, aux fins de l'accès aux informations du système OBD, du diagnostic, de la réparation et de l'entretien, du suivi et de l'inspection des véhicules, permettent l'accès au flux de données embarqué par d'autres moyens que l'utilisation du port de données sériel du connecteur de liaison de données normalisé, le même accès et les mêmes informations devraient être mis à la disposition de tous les opérateurs indépendants dans des conditions non discriminatoires.

(17) Eu égard au rôle des éditeurs de données dans la facilitation de la réparation et de l'entretien des véhicules, il convient de clarifier les exigences en matière de partage d'informations des constructeurs automobiles.

(18) Afin de permettre aux réparateurs indépendants de reprogrammer les unités de contrôle des véhicules dans des conditions identiques à celles des constructeurs automobiles et des réparateurs agréés, il est nécessaire de prévoir des exigences supplémentaires pour que les constructeurs mettent des logiciels ou des informations spécifiques à la disposition des fabricants d'outils de diagnostic indépendants.

(19) Toutefois, pour se conformer à ces exigences, les constructeurs de véhicules doivent mettre en œuvre des mesures préparatoires importantes, c'est pourquoi il convient de reporter l'application de ces exigences en prévoyant un délai d'exécution approprié.

(20) Le présent règlement s'applique sans préjudice du règlement (UE) 2016/679 du Parlement européen et du Conseil ([4]) et de la directive 2002/58/CE du Parlement européen et du Conseil ([5]). En particulier, les dispositions du présent règlement imposant aux constructeurs de fournir aux opérateurs indépendants l'accès aux informations du système OBD des véhicules s'entendent sans préjudice des droits des personnes concernées et des obligations des constructeurs de véhicules, des fabricants d'outils de diagnostic et des opérateurs indépendants prévus par ces actes.

(21) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([6]) et a rendu un avis le 20 février 2026 ([7]).

(22) Il convient dès lors de modifier le règlement (UE) 2018/858 en conséquence,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

L'annexe X du règlement (UE) 2018/858 est modifiée conformément à l'annexe du présent règlement.

Article 2

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 23 mars 2026.

Par la Commission
La présidente
Ursula VON DER LEYEN

([4]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE) (JO L 119 du 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) https://www.edps.europa.eu/data-protection/our-work/our-work-by-type/opinions_fr.

ANNEXE

L'annexe X du règlement (UE) 2018/858 est modifiée comme suit:

1) Le point 1 est remplacé par le texte suivant:

«1. Introduction

La présente annexe établit les prescriptions techniques relatives à l'accès aux informations du système OBD des véhicules et aux informations sur la réparation et l'entretien des véhicules, quel que soit le type de groupe motopropulseur du véhicule.».

2) Au point 2.1, la deuxième phrase est remplacée par le texte suivant:

«Le respect de l'obligation faite au constructeur de fournir les informations relatives au système OBD du véhicule et les informations sur la réparation et l'entretien des véhicules sur leurs sites internet dans un format normalisé est présumé conforme à la partie 1 "Informations générales et définition de cas d'utilisation", à la partie 2 "Exigences techniques", à la partie 3 "Exigences fonctionnelles relatives à l'interface utilisateur" et à la partie 4 "Test de conformité" de la norme EN ISO 18541 — 2021 et à la partie 5 "Dispositions particulières pour les véhicules utilitaires lourds" "Véhicules routiers — Normalisation de l'accès aux informations relatives à la réparation et à la maintenance pour l'automobile (RMI)" de la norme EN ISO 18541 — 2018.».

3) Au point 2.5, la partie introductive est remplacée par le texte suivant:

«2.5. Les informations sur la réparation et l'entretien des véhicules comprennent:».

4) Le point 2.5.1 est remplacé par le texte suivant:

«2.5.1. l'identification non équivoque du véhicule et la liste des options installées en usine qui en résulte, ainsi que des systèmes, composants, entités techniques distinctes, pièces ou équipements dont le constructeur est responsable;».

5) Le point 2.5.4 est remplacé par le texte suivant:

«2.5.4. les informations concernant les systèmes, les composants, les entités techniques distinctes, les pièces, les équipements et le diagnostic (telles que les valeurs théoriques minimales et maximales pour les mesures), y compris les informations sur les fonctions et les capacités nécessaires à l'étalonnage et à la réparation des systèmes avancés d'aide à la conduite (ADAS) ou des systèmes d'aide au contrôle de la conduite (DCAS) et des composants connexes);».

6) Le point 2.5.7 est remplacé par le texte suivant:

«2.5.7. les informations nécessaires pour déterminer si une mise à jour logicielle ou un codage de variantes est nécessaire pour une opération spécifique de réparation et d'entretien;».

7) Le point 2.5.7 *bis* suivant est inséré:

«2.5.7 *bis*. les informations nécessaires à l'identification de la mise à jour logicielle correcte ou du codage de variantes correct pour chaque système, composant, entité technique distincte, pièce ou équipement nécessitant une mise à jour logicielle;

par dérogation au point 2.1, si la détermination de la version correcte du logiciel ou du codage de variantes correct nécessite une connexion d'arrière-plan, le constructeur n'est pas tenu de publier sur le site web les informations nécessaires à l'identification de la mise à jour logicielle correcte ou du codage de variantes correct pour chaque système, composant, entité technique distincte, pièce ou équipement nécessitant une mise à jour logicielle;».

8) Le point 2.5.8 est modifié comme suit:

«2.5.8. les informations fournies concernant les outils et équipements exclusifs et les renseignements obtenus au moyen de ceux-ci, y compris les informations relatives à tous outillage, équipement et notice d'utilisation supplémentaires qui sont nécessaires pour effectuer l'étalonnage d'un composant ou d'un système;».

9) Les points 2.5.12 et 2.5.13 suivants sont ajoutés:

«2.5.12. les informations que le constructeur fournit à ses partenaires, concessionnaires et réparateurs agréés ou qu'il utilise à des fins de réparation ou d'entretien, qui sont requises pour le diagnostic et, le cas échéant, pour la réparation des systèmes de batteries de traction ainsi que de leurs unités remplaçables, y compris les modules de batteries;

2.5.13. les informations propres au type de véhicule nécessaires à la manipulation en toute sécurité des pièces et composants, en particulier les informations nécessaires à la protection contre les risques électriques, thermiques et chimiques liés aux batteries de traction, qui sont à la disposition du constructeur du véhicule ou de ses partenaires.».

10) Le point 2.6.2 est remplacé par le texte suivant:

«2.6.2. les informations suivantes:

a) les données de diagnostic descriptives visées au point 3 de l'appendice 2. Le constructeur veille à ce que ces données répondent aux exigences suivantes:

i) elles sont mises à disposition sous la forme d'ensembles de données électroniques directement exploitables,

ii) elles présentent le même degré de détail que celui utilisé par les outils de diagnostic exclusifs du constructeur du véhicule,

iii) elles sont documentées de manière exhaustive;

b) les descriptions des interactions à l'extérieur et à bord nécessaires à l'accomplissement de tout travail de réparation et d'entretien.

Le constructeur de véhicules ne met à disposition les informations visées au point a) que pour les types de véhicules pour lesquels la fiche de réception par type a été délivrée pour la première fois après le 1er septembre 2020.».

11) Le point 2.6.3 suivant est inséré:

«2.6.3. des informations sur la manière d'acquérir des outils et équipements exclusifs.».

12) Les points 2.6 *bis* et 2.6 *ter* suivants sont insérés:

«2.6 *bis*. Le constructeur met à la disposition des fabricants d'équipements de réparation et d'outils de diagnostic génériques toutes les informations, spécifications techniques et instructions d'utilisation pour la réparation, l'entretien et le diagnostic des systèmes ADAS/DCAS au moyen d'outils de diagnostic.

2.6 *ter*. Les informations visées aux points 2.6 et 2.6 *bis* sont mises à disposition conformément aux modalités et conditions fixées par le constructeur en vertu du présent règlement, y compris les modalités et conditions de paiement ou les limitations d'utilisation et les frais exigés conformément à l'article 63, paragraphe 1.».

13) Le point 2.9 est remplacé par le texte suivant:

«2.9. Aux fins de l'accès aux informations du système OBD, du diagnostic, de la réparation et de l'entretien, du suivi et de l'inspection des véhicules, le constructeur doit permettre un accès bidirectionnel au flux de données embarqué, par tous les moyens suivants:

a) le port de données sériel du connecteur de liaison de données normalisé, visé à l'appendice 1, paragraphe 6.5.3, de l'annexe C5 du règlement ONU no 154 (*), conformément au paragraphe 4.7.3 de l'annexe 9B et aux normes de référence figurant à l'appendice 6 de ladite annexe du règlement ONU no 49 (**);

b) tout autre moyen d'accès embarqué fourni par le constructeur à ses partenaires, concessionnaires et réparateurs agréés ou utilisé par le constructeur à des fins de réparation et d'entretien, y compris les connecteurs Ethernet, les broches non normalisées sur le port OBD normalisé, les interfaces de programmation d'applications utilisées pour l'intégration du service après-vente et les réseaux locaux sans fil;

c) toute installation fournie par le constructeur à ses partenaires, concessionnaires et réparateurs agréés ou utilisée par le constructeur pour permettre l'accès à distance aux informations du système OBD des véhicules à des fins de réparation et d'entretien, y compris le suivi et l'inspection (lorsque le suivi et l'inspection sont effectués pour la réparation et l'entretien) ou les services de réparation et de diagnostic à distance.

Lorsque le véhicule est en mouvement, le constructeur peut choisir de mettre le flux de données à disposition uniquement pour des fonctions en lecture seule, à condition d'appliquer la même restriction à ses propres partenaires, concessionnaires et réparateurs agréés.

Le constructeur peut appliquer des conditions d'accès au flux de données du véhicule, dans la mesure où cela est nécessaire et proportionné au respect de l'article 4, paragraphe 5, point d), et de la ligne D4 de l'annexe II du règlement (UE) 2019/2144, ainsi que de l'article 4, paragraphes 7 et 8, et de l'article 6, paragraphe 3, du règlement (UE) 2024/1257. Pour l'accès par les moyens décrits au point 2.9, a) et b), ces conditions ne doivent pas aller au-delà des conditions que le constructeur est autorisé à appliquer en vertu de l'appendice 4 de la présente annexe.

(*) Règlement nº 154 de la Commission économique pour l'Europe des Nations unies (CEE-ONU) — Prescriptions uniformes relatives à l'homologation des voitures particulières et des véhicules utilitaires légers en ce qui concerne les émissions de référence, les émissions de dioxyde de carbone et la consommation de carburant et/ou la mesure de la consommation d'énergie électrique et de l'autonomie électrique (WLTP) [2021/2039] (JO L 423 du 26.11.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/2039/oj).

(**) Règlement nº 49 de la Commission économique pour l'Europe des Nations unies (CEE-ONU) — Prescriptions uniformes concernant les mesures à prendre pour réduire les émissions de gaz polluants et de particules des moteurs à allumage par compression et des moteurs à allumage commandé utilisés pour la propulsion des véhicules [2023/64] (JO L 14 du 16.1.2023, p. 1, ELI: http://data.europa.eu/eli/reg/2023/64/oj).».

14) Le point 6.1 est remplacé par le texte suivant:

«6.1. L'obligation faite au constructeur de fournir les informations sur la réparation et l'entretien des véhicules sur son site web dans un format normalisé est présumée respectée s'il se conforme aux parties de la norme ISO 18541-1:2021 à ISO 18541-4:2021 et ISO 18541-5:2018 visées au point 2.1.

Quiconque souhaite copier ou republier ces informations doit négocier directement avec le constructeur concerné. Des informations relatives au matériel de formation doivent également être disponibles et elles peuvent être fournies sur des supports autres que les sites web.

6.1.1. Aux fins de la publication des informations sur la réparation et l'entretien, le constructeur met ces informations à disposition sous la forme de fichiers dans le format servant au traitement électronique direct des ensembles de données contenus dans ces fichiers. Les informations présentent le même degré de détail que celles utilisées par le constructeur à des fins de réparation et d'entretien. Elles sont documentées aux fins de leur interprétation et mises à jour à la fréquence convenue avec l'opérateur indépendant. Les mises à jour sont disponibles à la même fréquence et dans les mêmes délais que lorsqu'elles sont mises à la disposition des concessionnaires et réparateurs agréés. Les informations sont communiquées dans des dossiers constitués sur la base des informations techniques classées par cas d'utilisation, telles qu'elles sont à la disposition du constructeur. Les informations visées à la première phrase du présent point sont fournies conformément aux modalités et conditions fixées par le constructeur en vertu du présent règlement; c'est le cas, par exemple, pour les modalités de paiement et toute condition ou limitation de l'utilisation compatible, ainsi que pour les frais exigés conformément à l'article 63, paragraphe 1, du présent règlement. Les dossiers de réception définis sur la base de critères correspondant aux exigences en matière d'informations nécessaires pour le cas d'utilisation 5.1.1, le cas d'utilisation 5.1.2, le cas d'utilisation 5.2, le cas d'utilisation 5.3, le cas d'utilisation 5.4, le cas d'utilisation 5.5, le cas d'utilisation 5.7, le cas d'utilisation 5.8, le cas d'utilisation 5.9, le cas d'utilisation 8 et le cas d'utilisation 11 de la norme ISO 18541-1:2021 sont présumés conformes.

Le constructeur ne fournit, à partir du 23 juin 2027, des dossiers de réception définis sur la base de critères correspondant aux exigences en matière d'informations nécessaires pour le cas d'utilisation 5.3 et le cas d'utilisation 5.4 de la norme ISO 18541-1:2021, disponibles uniquement sur la base du numéro d'identification du véhicule (VIN), que lorsqu'un réparateur indépendant en fait la demande par l'intermédiaire d'une interface de programmation d'applications [API (*)]. Dans ce cas, le réparateur indépendant transmet au constructeur une demande propre au VIN par l'intermédiaire d'un tiers agissant sur la base d'un accord avec le constructeur.

Lorsque les dossiers de réception sont définis sur la base de critères correspondant aux exigences en matière d'informations nécessaires pour le cas d'utilisation 8 de la norme ISO 18541-1:2021, le constructeur fournit à ce tiers, à partir du 23 juin 2027 une API qui permet au réparateur indépendant de visualiser et de mettre à jour l'historique d'entretien électronique sous réserve des conditions supplémentaires spécifiées dans la norme ISO et, le cas échéant, des conditions et procédures du constructeur utilisées pour obtenir l'accord du client. Le constructeur doit le faire sous réserve des

procédures et informations requises identiques ou équivalentes à celles spécifiées sur son site web consacré aux informations sur la réparation et l'entretien. En pareil cas, le réparateur indépendant peut, avec l'accord du client, transmettre une demande de mise à jour des dossiers de réparation ou d'entretien au constructeur par l'intermédiaire d'un tiers agissant sur la base d'un accord avec le constructeur. Un certificat conforme à la recommandation ITU-T X.509 de l'Union internationale des télécommunications peut être utilisé pour vérifier l'identité du réparateur indépendant.

L'accès à ces API, y compris pour la mise à jour de l'historique d'entretien électronique, est soumis à l'article 63, paragraphe 1.

Les informations sont structurées de manière qu'il soit plus tard possible de rechercher et de filtrer les informations contenues dans le dossier sur la base de critères de classification du type de modèle et d'autres critères de classification utilisés par le propre réseau du constructeur du véhicule.

6.1.2. Des informations sur toutes les pièces dont est équipé d'origine le véhicule, tel qu'identifié par le VIN du véhicule et par tout critère supplémentaire comme l'empattement, la puissance du moteur, le type de finition ou les options, et qui peuvent être remplacées par des pièces détachées proposées par le constructeur du véhicule à ses concessionnaires ou réparateurs agréés ou à des tiers au moyen d'une référence au numéro des pièces d'origine, doivent être mises à disposition, sous la forme d'ensembles de données lisibles par machine et électroniquement exploitables, dans une base de données accessible pour les opérateurs indépendants.

Dans cette base de données doivent figurer le numéro VIN, le numéro de la pièce d'origine, la dénomination de la pièce d'origine, les indications de validité (dates de début et de fin de validité), les indications de montage et, le cas échéant, les caractéristiques de structure.

Les informations de la base de données doivent être régulièrement mises à jour. Si ces informations sont mises à la disposition des concessionnaires, les mises à jour doivent inclure toutes les modifications apportées à des véhicules individuels après leur production.

_____

(*) Au sens de l'article 2 du règlement d'exécution (UE) 2023/138 de la Commission du 21 décembre 2022 établissant une liste d'ensembles de données de forte valeur spécifiques et les modalités de leur publication et de leur réutilisation (JO L 19 du 20.1.2023, p. 43, ELI: http://data.europa.eu/eli/reg_impl/2023/138/oj).».

15) Le point 6.2.2 est remplacé par le texte suivant:

«6.2.2. la norme https//ssl-tls (RFC5246), ou toute norme lui succédant, est utilisée;».

16) Le point 6.2.3 est remplacé par le texte suivant:

«6.2.3. des certificats de sécurité établis conformément à la norme internationale ISO/IEC 9594-8:2020 sont utilisés pour l'authentification mutuelle des opérateurs indépendants et des constructeurs;».

17) Le point 6.4 est remplacé par le texte suivant:

«6.4. La reprogrammation des unités de contrôle, le codage des variantes et l'activation des pièces de rechange sont effectués en utilisant matériel non propriétaire, sans aucune dépendance à l'égard du matériel du constructeur, conformément à l'une des normes suivantes:

a) norme internationale ISO 22900-2;

b) SAE J2534-1;

c) SAE J2534-2;

d) TMC RP1210B;

e) norme ISO/DIS 17978-1 — Diagnostic véhicule orienté services (SOVD).

En cas d'utilisation d'Ethernet, la reprogrammation des unités de contrôle, le codage des variantes et l'activation des pièces de rechange doivent être effectués conformément à la norme ISO 22900-2 ou à la norme J2534-2.

Afin de valider la compatibilité de l'application propre au constructeur et des interfaces de communication du véhicule (VCI) conformes à la norme internationale ISO 22900-2 ou aux normes SAE J2534-1, SAE J2534-2 ou TMC RP1210B, le constructeur propose une validation des VCI résultant d'un développement indépendant ou fournit les informations nécessaires au fabricant de VCI pour effectuer cette validation et lui prête tout matériel spécial requis à cet effet.

Le constructeur peut facturer des frais raisonnables et proportionnés pour cette validation ou la mise à disposition de ces informations et de ce matériel. Ces frais ne doivent pas décourager le recours à cette validation ou l'utilisation de ces informations et de ce matériel.»;

18) Le point 6.4 *bis* suivant est inséré:

«6.4 *bis.* À compter du …, le constructeur de véhicules met à la disposition du fabricant d'outils de diagnostic indépendants l'un quelconque des logiciels ou informations suivants pour le type de véhicule pour lequel la fiche de réception par type a été délivrée pour la première fois après le 1er septembre 2020:

a) les interfaces de logiciels ou de services web destinées aux fabricants d'outils de diagnostic indépendants pour leur intégration, qui permettent le codage de variantes, le couplage avec un véhicule d'une pièce de rechange d'origine [y compris un logiciel et un matériel compatibles (tels que définis par le constructeur du véhicule) remanufacturés ou réutilisés] ou d'une pièce de rechange autorisée par le constructeur du véhicule, ainsi que la reprogrammation des unités de contrôle avec le logiciel d'équipement d'origine d'un véhicule conformément aux instructions du constructeur du véhicule; ou

b) les informations, processus et ressources nécessaires pour mettre en œuvre la reprogrammation et le codage de variantes dans l'outil de diagnostic indépendant du fabricant d'outils de diagnostic indépendants.

Toutefois, par dérogation au délai indiqué dans la première phrase du présent point, le constructeur du véhicule met à disposition le logiciel ou les informations visés aux points a) et b) ci-dessus à partir des dates suivantes:

i) …, en ce qui concerne les véhicules pour lesquels la réception par type a été accordée pour la première fois après le 1er septembre 2020, mais avant le 6 juillet 2022;

ii) … pour toute opération supposant la réalisation de mises à jour logicielles ou dépendant de celle-ci.».

19) Le point 6.4 *ter* suivant est inséré:

«6.4. *ter.* Jusqu'à ce que le constructeur du véhicule mette à disposition le logiciel ou les informations pour le type de véhicule visé au point 6.4 *bis* et pendant la période de deux ans suivant cette date, l'utilisation du matériel de diagnostic et du logiciel de diagnostic du constructeur du véhicule par les prestataires de services à distance visés au point 1.2 de l'appendice 4, aux fins de la reprogrammation et du codage des variantes ou de l'activation des pièces, est soumise aux mêmes frais et conditions de paiement que celles applicables aux réparateurs indépendants, que les outils de diagnostic soient ou non utilisés à distance.

En outre, le constructeur de véhicules partage avec tous les fabricants d'outils de diagnostic intéressés, dès qu'elles sont disponibles:

a) les informations nécessaires à la mise en œuvre de l'API entre les systèmes du constructeur de véhicules et des fabricants d'outils de diagnostic concernés,

i) au plus tard le … pour toute opération supposant la réalisation de mises à jour logicielles ou dépendant de celle-ci; et

ii) pour les autres opérations, au plus tard le …; ou

iii) en ce qui concerne les véhicules pour lesquels la réception par type a été accordée pour la première fois avant le 6 juillet 2022, au plus tard le …;

b) les informations nécessaires pour tester la fonctionnalité de mise à jour et l'interaction pour le matériel, au plus tard le … pour toute opération supposant la réalisation de mises à jour logicielles ou dépendant de celle-ci.».

20) Le point 6.4 *quater* suivant est inséré:

«6.4 *quater*. Le découplage des composants, entités techniques distinctes, pièces et équipements, à l'exception de ceux qui ont été initialement conçus pour ne pas être découplés, est effectué conformément au processus décrit au présent point. Il n'est soumis à aucune autre condition que celles visées au présent point.

Le fabricant met en place un processus de découplage des composants, entités techniques distinctes, pièces et équipements. Aux fins de l'installation d'un composant, d'une entité technique distincte, d'une pièce ou d'un équipement réutilisé, les processus définis par le constructeur de véhicules peuvent inclure l'obligation de fournir l'identifiant unique (y compris, le cas échéant, le numéro de série d'une entité) de ce composant, de cette entité technique distincte, de cette pièce ou de cet équipement et le VIN du véhicule, ainsi que l'obligation d'obtenir un accord du propriétaire du véhicule ou du preneur du véhicule en leasing, lorsqu'ils sont identifiables. Lorsqu'un accord est requis, il peut être fourni de manière asynchrone par rapport à la désinstallation de la pièce.

Aux fins du processus industriel de remanufacturage, par lequel les spécifications initiales d'un composant, d'une entité technique distincte, d'une pièce ou d'un équipement usagé ou défaillant sont rétablies, le VIN du véhicule d'origine ne sera pas requis pour le découplage du véhicule d'origine. Dans ce cas, l'identifiant unique du composant et l'accord du propriétaire du véhicule ou du preneur du véhicule en leasing, lorsqu'ils sont identifiables, peuvent être exigés.

Tous les opérateurs indépendants, y compris les remanufacturers et les reconditionneurs, authentifiés conformément aux exigences spécifiées à l'appendice 4, ont un accès égal à ces processus.

Aux fins de l'authentification d'un tel opérateur, lorsque le processus de découplage du constructeur de véhicules doit être effectué sur ses plateformes extérieures, les identifiants d'authentification délivrés conformément au point 9.2 de l'appendice 4, ou ceux utilisés pour accéder au site internet RMI du constructeur de véhicules, sont acceptés.».

21) Les points 7.2 et 7.3 sont supprimés.

22) Le point 7.4 est remplacé par le texte suivant.

«7.4. Sur la base d'un certificat dûment rempli relatif à l'accès aux informations du système OBD du véhicule et aux informations sur la réparation et l'entretien du véhicule, l'autorité compétente en matière de réception peut présumer que le constructeur a pris des mesures et mis en place des procédures satisfaisantes concernant l'accès auxdites informations, à condition qu'aucune plainte n'ait été déposée.».

23) Le point 7.5 suivant est ajouté:

«7.5. Les informations du système OBD des véhicules et les informations sur la réparation et l'entretien des véhicules sont fournies aux opérateurs indépendants au plus tard à la date à laquelle le véhicule est mis sur le marché.».

24) À l'appendice 2, le point 3 est remplacé par le texte suivant:

«3. Informations requises pour la fabrication d'outils de diagnostic

Afin de faciliter la fourniture d'outils de diagnostic génériques aux réparateurs multimarques, le constructeur de véhicules communique les informations visées aux points 3.1, 3.2 et 3.3. Ces informations incluent toutes les fonctions des outils de diagnostic et tous les liens vers des instructions de dépannage et des informations en matière de réparation. Des frais raisonnables peuvent être facturés pour l'accès à ces informations.».

25) L'appendice 3 est modifié comme suit:

a) au point 2, les points 2.1.14 et 2.1.15, suivants sont ajoutés:

«2.1.14. "fournisseur de services à distance (FSD)",

un prestataire de services agissant à distance pour la fourniture d'un service à l'OI dans le cadre de ses activités liées au SERMI, la programmation, l'installation ou l'activation de pièces et d'équipements sur un véhicule;

2.1.15. "salarié de FSD",

le salarié d'un FSD agréé qui, sur autorisation du CAB, aura accès aux informations sur la réparation et l'entretien (RMI) liées à la sécurité.»;

b) au point 3, les troisième et quatrième alinéas sont remplacés par le texte suivant:

«Les OI souhaitant recevoir des informations sur la réparation et l'entretien liées à la sécurité doivent obtenir un certificat d'inspection d'agrément auprès d'un CAB accrédité.

Les salariés d'OI qui sont appelés à traiter des informations sur la réparation et l'entretien liées à la sécurité doivent obtenir un certificat d'inspection d'autorisation auprès d'un CAB accrédité.»;

c) au point 4.1.1, le point f) suivant est ajouté:

«f) Le SERMI gère une liste d'interprétations approuvées, à utiliser exclusivement aux fins de l'interprétation du système.»;

d) le point 4.4.2 suivant est ajouté:

«4.4.2. Les FSD doivent assumer les responsabilités et remplir les obligations énoncées au point 4.4.1.»;

e) le point 4.5.2 suivant est ajouté:

«4.5.2. Les salariés des FSD doivent assumer les responsabilités et remplir les obligations énoncées au point 4.5.1.».

26) L'appendice 4 suivant est ajouté:

«*Appendice 4*

Conditions et procédure d'accès aux informations du système OBD des véhicules

1. Champ d'application

1.1. Le présent appendice contient les seules conditions d'accès que le constructeur est autorisé à définir et les procédures que le constructeur du véhicule applique ou qu'il est autorisé, à titre exclusif, à exiger d'autres parties qu'elles les appliquent, tout en mettant en œuvre les mesures de sécurité requises pour l'accès aux informations du système OBD visées au point 2.9, a) et b), de la présente annexe.

1.2. Toute référence dans le présent appendice à des opérateurs indépendants ou à des partenaires, concessionnaires et réparateurs agréés du constructeur, ainsi qu'à un constructeur de véhicules agissant à des fins de réparation et d'entretien, inclut toute personne ou tout opérateur agissant pour leur compte, tel qu'un prestataire de services agissant à distance pour la fourniture d'un service à l'opérateur indépendant, la programmation, l'installation ou l'activation de pièces et d'équipements sur un véhicule (fournisseurs de services à distance).

2. Obligations du constructeur

2.1. Il incombe au constructeur de véhicules de veiller à ce que toutes les conditions techniques préalables à l'application des procédures visées au présent appendice soient en place, y compris les identifiants d'accès tels que les certificats ou les jetons logiciels, et les dispositions nécessaires prises avec les fabricants d'outils de diagnostic.

2.2. Le constructeur de véhicules démontre à l'autorité compétente en matière de réception que le véhicule est conçu pour permettre l'accès aux informations du système OBD, conformément aux prescriptions du présent appendice, à l'aide d'outils de diagnostic multimarques.

2.3. Le constructeur de véhicules fournit aux fabricants d'outils de diagnostic les informations visées au point 11 du présent appendice.

2.4. Le constructeur de véhicules veille à ce que son serveur utilisé pour permettre l'accès prévu au point 2.9 de la présente annexe offre aux opérateurs indépendants, sans discrimination, la même disponibilité et les mêmes performances du système d'information que celles qu'il offre aux partenaires, concessionnaires et réparateurs officiels du constructeur de véhicules ou au constructeur de véhicules qui l'utilisent à cette fin.

Le constructeur de véhicules veille à ce que tout serveur utilisé pour permettre l'accès prévu au point 2.9 de la présente annexe soit accessible sans interruption, sauf circonstances exceptionnelles et imprévisibles indépendantes de sa volonté et non imputables à une négligence de sa part, ou nécessaires à des fins d'entretien du système d'information. En cas de maintenance, la période d'indisponibilité ne doit pas dépasser la période de maintenance de tout autre serveur utilisé par le constructeur pour permettre l'accès aux fins visées au point 2.9 de la présente annexe. Les informations relatives à l'entretien planifié doivent être mises à la disposition des fabricants d'outils de diagnostic suffisamment à l'avance.

Le constructeur de véhicules met les informations statistiques annuelles sur la disponibilité de ses serveurs à la disposition de l'autorité compétente en matière de réception, lorsque celle-ci le demande. Les cas d'indisponibilité du serveur doivent être rapidement signalés par le constructeur du véhicule au forum OBD défini au point 12.

2.5. Le constructeur de véhicules ne restreint pas l'accès aux informations du système OBD au-delà des restrictions énoncées au présent appendice, sauf disposition contraire spécifiquement énoncée par le présent règlement. En outre, le constructeur de véhicules ne restreint pas l'accès des opérateurs indépendants aux informations du système OBD au-delà des restrictions qui s'appliquent à ses partenaires, concessionnaires et réparateurs agréés ou à lui-même lorsqu'il accède aux informations du système OBD à des fins de réparation et d'entretien.

2.6. Le constructeur du véhicule veille à ce que les mesures de cybersécurité qu'il met en œuvre, y compris les exigences de compatibilité visées au point 6.2, n'aient pas pour effet de restreindre ou d'entraver l'accès aux informations du système OBD au titre du présent appendice au-delà de ce qui est nécessaire et proportionné pour se conformer à l'article 4, paragraphe 5, point d), et à la ligne D4 de l'annexe II du règlement (UE) 2019/2144. Ces mesures peuvent anticiper des risques et menaces futurs si le constructeur du véhicule peut démontrer leur incidence et leur probabilité.

2.7. Toute mesure mise en œuvre par le constructeur du véhicule pour empêcher la manipulation des émissions et la fraude au compteur kilométrique ne doit pas restreindre ou entraver l'accès aux informations du système OBD au-delà de ce qui est nécessaire et proportionné pour se conformer à l'article 4, paragraphes 7 et 8, du règlement (UE) 2024/1257 du Parlement européen et du Conseil (*).

3. Authentification

3.1. Le constructeur de véhicules peut, pour la délivrance des identifiants d'accès, exiger l'authentification du fabricant de l'outil de diagnostic et de l'outil de diagnostic utilisé, sauf pour les opérations de réparation et d'entretien suivantes:

a) la lecture des codes d'anomalie de diagnostic;

b) la lecture du VIN du véhicule;

c) la lecture des données et l'effacement des codes d'anomalie de diagnostic lorsque l'accès sans restriction au moyen d'un outil de détection générique ou OBD est requis en vertu du règlement (UE) 2017/1151 ou du règlement (UE) 2024/1257, ou prévu dans le règlement ONU n° 49, le règlement ONU n° 83 (**), le règlement ONU n° 168 (***) ou le règlement ONU n° 154.

3.2. Lorsque l'accès aux informations du système OBD suppose des modifications du véhicule, le constructeur du véhicule peut, pour délivrer les identifiants d'accès, exiger l'authentification de l'opérateur. Dans le cas de dispositifs utilisés à des fins de suivi, lorsque les données sont en lecture seule et communiquées de manière autonome au serveur des fabricants d'outils de diagnostic sans interaction humaine, le constructeur du véhicule n'exige pas l'authentification de l'opérateur.

3.3. Lorsque l'accès aux informations du système OBD suppose une modification du logiciel du véhicule ou de sa configuration/de ses paramètres consistant en une reprogrammation du code logiciel du véhicule, entraînant une modification du comportement prévu du véhicule et persistant au-delà de l'opération de réparation et d'entretien, de sorte qu'elle ne peut être inversée ou écrasée que par l'exécution d'une opération équivalente, le constructeur du véhicule peut exiger l'authentification du salarié de l'opérateur qui cherche à accéder aux informations du système OBD, à moins que le constructeur de l'outil de diagnostic n'atteste au constructeur du véhicule que, sur la base du résultat d'un audit indépendant effectué au plus tôt trois ans avant la demande, l'opérateur dispose d'un système permettant d'identifier sans ambiguïté le salarié qui le demande.

3.4. Les cas d'accès visés au point 3.2 comprennent les opérations de réparation et d'entretien telles que l'activation des actionneurs et des procédures d'essai fonctionnelles, l'effacement des codes de diagnostic d'anomalie, la remise en position initiale des voyants de service, la remise à l'état initial des paramètres d'apprentissage adaptatif et le remplacement de pièces, y compris l'initialisation des composants non intelligents et les données de lecture par identificateur, sauf lorsqu'ils sont utilisés aux fins de l'inspection technique périodique avec des valeurs comparables aux valeurs définies à l'annexe B de la norme ISO20730-3, à condition que ces valeurs soient disponibles dans le véhicule.

3.5. Les cas d'accès visés au point 3.2 comprennent l'étalonnage, entendu comme un processus d'ajustement ou d'alignement des paramètres logiciels et matériels du véhicule, tel que prescrit par le constructeur du véhicule et sans codage de variante ni modification du logiciel du véhicule.

3.6. Aux fins de l'authentification visée aux points 3.1 à 3.3, le constructeur du véhicule peut exiger du fabricant de l'outil utilisé pour accéder aux informations du système OBD qu'il atteste:

a) l'identité de l'outil de diagnostic;

b) lorsque l'accès aux informations du système OBD suppose des modifications du véhicule visées au point 3.2, l'identité de l'outil de diagnostic et l'identité pseudonymisée de l'opérateur, et l'observation par l'opérateur des exigences en matière d'autorisation visées au point 8.1;

c) lorsque l'accès aux informations du système OBD suppose une modification du logiciel du véhicule ou de sa configuration/de ses paramètres consistant en une reprogrammation du code logiciel du véhicule, entraînant une modification du comportement prévu du véhicule et persistant au-delà de l'opération de réparation et d'entretien, de sorte qu'elle ne puisse être annulée ou écrasée que par l'exécution d'une opération équivalente visée au point 3.3, l'identité pseudonymisée du salarié de l'opérateur et l'observation par ce salarié des exigences en matière d'autorisation visées au point 8.2.

3.7. Dans les cas visés aux point 3.6, b) et c), l'identité de l'opérateur et, le cas échéant, de son salarié ainsi que leur observation des exigences en matière d'autorisation visées aux points 8.1 et 8.2 doivent être vérifiés par le fabricant de l'outil de diagnostic utilisé pour accéder aux informations du système OBD ou établis sur la base d'un certificat d'autorisation visé au point 9.2.

3.8. Le constructeur de véhicules n'exige pas de redevance pour assurer l'accès prévu au point 2.9 de l'annexe X. Toutefois, le constructeur de véhicules peut facturer des frais justifiés et proportionnés pour l'utilisation de l'installation à distance visée au point 2.9, c).

4. Exigences de connexion

4.1. Sauf dans les cas d'accès visés au point 3.1, a) à c), le constructeur du véhicule peut avoir besoin d'établir une connexion en ligne unique entre l'outil de diagnostic et le serveur du constructeur de véhicules, via le serveur du fabricant de l'outil de diagnostic, pour recevoir les identifiants d'accès. Après la fourniture de ces identifiants, l'accès ne nécessite pas de connexion en ligne.

4.2. Lorsque l'accès aux informations du système OBD suppose une modification du logiciel du véhicule, de sa configuration ou de ses paramètres entraînant une modification du comportement prévu du véhicule qui persiste au-delà de l'opération de réparation et d'entretien et qui ne peut être inversée ou écrasée que par l'exécution d'une opération équivalente, le constructeur du véhicule peut exiger une connexion en ligne continue au moment de la réparation, de l'outil de diagnostic au serveur du fabricant de l'outil de diagnostic ainsi qu'au serveur du constructeur de véhicules.

4.3. Les cas d'accès visés au point 4.2 comprennent les situations suivantes:

a) les opérations de réparation et d'entretien consistant à mettre en place un composant de rechange et à paramétrer les préférences du client, à identifier une unité de contrôle électronique (UCE) et à procéder au codage de variantes, à initialiser une UCE et un composant, à coder les variantes lors du remplacement de composants existants et à coder les variantes lors de l'ajout d'un nouveau composant;

b) les opérations de réparation et d'entretien visées au point 5.5.

4.4. Les cas d'accès visés au point 4.2 ne comprennent pas les opérations de réparation et d'entretien énumérées aux points 3.4 et 3.5.

4.5. Toutefois, par dérogation au point 4.4, les cas d'accès visés au point 4.2 comprennent les opérations de réparation et d'entretien visées au point 3.5 lorsqu'il est nécessaire de valider des valeurs d'étalonnage qui sont soumises à des exigences réglementaires ou lorsque l'étalonnage ne peut pas être achevé sans que des données spécifiques d'un composant ou d'une entité technique distincte soient nécessaires pour achever le processus de réparation et extraites du serveur du constructeur dans le cadre d'un processus de codage de variantes.

5. Exigences en matière de traçabilité

5.1. Sauf dans les cas d'accès visés au point 3.1, a) à c), le constructeur de véhicules peut exiger du constructeur de l'outil de diagnostic qu'il collecte et stocke le VIN du véhicule et l'identifiant unique de l'outil de diagnostic.

5.2. Lorsque l'accès aux informations du système OBD suppose des modifications du véhicule, le constructeur du véhicule peut demander au fabricant de l'outil de diagnostic de recueillir et de consigner les informations sur tous les travaux de diagnostic exécutés (par exemple, l'ID de service et la sous-fonction) ainsi que la date et l'heure UTC d'utilisation de paramètres/attributs pour chaque interaction avec le véhicule.

5.3. Les cas d'accès visés au point 5.2 comprennent les opérations de réparation et d'entretien visées aux points 3.4, 3.5, 4.3 et 4.5.

5.4. Lorsque l'accès aux informations du système OBD suppose une modification du logiciel du véhicule ou de sa configuration/de ses paramètres consistant en une reprogrammation du code logiciel du véhicule, entraînant une modification du comportement prévu du véhicule et persistant au-delà de l'opération de réparation et d'entretien, de sorte qu'elle ne puisse être inversée ou écrasée que par l'exécution d'une opération équivalente, le constructeur du véhicule peut exiger du fabricant de l'outil de diagnostic qu'il recueille et fournisse les résultats de l'inspection topologique du réseau du véhicule, l'état initial du véhicule lors de la connexion, y compris les versions matérielles/logicielles de toutes les unités de contrôle électronique installées dans le véhicule, les résultats de toutes les interactions et routines du module (par exemple, les paramètres de retour) et les résultats de la lecture du contrôle de santé final du véhicule après réparation.

5.5. Les cas d'accès visés au point 5.4 comprennent les opérations de réparation et d'entretien telles que le couplage d'une pièce de rechange d'origine [y compris le logiciel et le matériel compatibles (tels que définis par le constructeur du véhicule) remanufacturés ou réutilisés] ou d'une pièce de rechange autorisée par le constructeur du véhicule à l'aide d'un outil de diagnostic indépendant et la reprogrammation d'un module à l'aide du logiciel d'équipement d'origine du véhicule et du logiciel de programmation de l'équipement d'origine conformément aux instructions du constructeur du véhicule. Ils comprennent aussi les cas de découplage ou de radiation d'une pièce d'un véhicule.

5.6. Les cas d'accès visés au point 5.4 ne comprennent pas les opérations de réparation et d'entretien énumérées aux points 3.4, 3.5, 4.3 et 4.5.

6. Exigences en matière de cybersécurité applicables à l'outil de diagnostic

6.1. Sauf dans les cas d'accès visés au point 3.1, a) à c), le constructeur du véhicule peut exiger que l'outil de diagnostic utilisé pour accéder aux informations du système OBD soit conforme aux exigences pertinentes du règlement (UE) 2024/2847 du Parlement européen et du Conseil (****) et que le fabricant de l'outil de diagnostic observe soit la norme TISAX (Trusted Information Security Assessment Exchange), au niveau spécifié par le constructeur du véhicule conformément au point 2.5, soit la norme ISO 27001.

6.2. Lorsque l'accès aux informations du système OBD suppose des modifications du véhicule visées au point 3.2, le constructeur du véhicule peut exiger que l'outil de diagnostic utilisé pour accéder aux informations du système OBD et le fabricant de l'outil de diagnostic respectent les prescriptions du constructeur du véhicule relatives à la mise en œuvre de la sécurité.

6.3. Les prescriptions pour la mise en œuvre de la sécurité élaborées par le constructeur du véhicule ne vont pas au-delà des prescriptions imposées à l'outil de diagnostic, aux fournisseurs d'outils et à l'organisation du constructeur du véhicule et sont appliquées de manière non discriminatoire.

6.4. Le constructeur du véhicule peut exiger du fabricant de l'outil de diagnostic qu'il réalise des essais pour vérifier la conformité de l'outil de diagnostic avec les prescriptions spécifiées. Un accord sur le niveau de service doit prévoir que toute vérification des résultats de ces essais réalisés par le constructeur du véhicule est effectuée en temps utile. Si la conformité d'un fabricant d'outils de diagnostic avec les prescriptions de la présente section n'est pas confirmée, le constructeur du véhicule doit fournir une déclaration claire des raisons de la non-conformité, ainsi que les mesures à mettre en œuvre par le fabricant de l'outil de diagnostic.

6.5. Les cas d'accès visés au point 6.2 comprennent les opérations de réparation et d'entretien visées aux points 3.4 et 3.5.

6.6. Lorsque l'accès aux informations du système OBD suppose une modification du logiciel du véhicule ou de sa configuration/de ses paramètres entraînant une modification du comportement prévu du véhicule qui persiste au-delà de l'opération de réparation et d'entretien, de sorte qu'elle ne peut être inversée ou écrasée que par l'exécution d'une opération équivalente, le constructeur du véhicule peut exiger que l'outil de diagnostic utilisé pour accéder aux informations du système OBD et le fabricant de l'outil de diagnostic respectent les prescriptions pertinentes du constructeur du véhicule relatives à la mise en œuvre du système de gestion des mises à jour logicielles [telles que définies dans le règlement ONU n° 156 (*****)]. Ces prescriptions ne vont pas au-delà des prescriptions imposées à l'outil de diagnostic, aux fournisseurs d'outils et à l'organisation du constructeur du véhicule et sont appliquées sur une base non discriminatoire.

6.7. Les cas d'accès visés au point 6.6 comprennent les opérations de réparation et d'entretien visées aux points 4.3, 4.5 et 5.5 et n'incluent pas ceux visés aux points 3.4 et 3.5.

7. Identifiants d'accès

7.1. Lorsque toutes les conditions visées aux points 3, 4 et 6 sont remplies, le constructeur du véhicule fournit sans délai au fabricant de l'outil de diagnostic des identifiants d'accès suffisants pour lui permettre d'accéder aux informations requises du système OBD.

7.2. Les identifiants d'accès peuvent être spécifiques au VIN.

7.3. Les identifiants d'accès sont valables pendant au moins 30 jours à compter de la date où ils ont été communiqués.

7.4. Toutefois, lorsque l'accès aux informations du système OBD suppose une modification du véhicule, le constructeur du véhicule peut limiter la validité des identifiants d'accès à 24 heures.

7.5. Les cas d'accès visés au point 7.4 comprennent les opérations de réparation et d'entretien visées aux points 3.4, 3.5, 4.3, 4.5 et 5.5.

8. Critères d'autorisation et certificats d'autorisation

8.1. Dans les cas visés au point 3.2, le constructeur du véhicule peut refuser de délivrer des identifiants d'accès si le fabricant de l'outil de diagnostic utilisé pour accéder aux informations du système OBD n'atteste pas que l'opérateur qui demande à accéder aux informations du système OBD:

a) a contracté une assurance responsabilité civile valable d'un montant de couverture minimal de 1 000 000 EUR pour les dommages corporels et de 500 000 EUR pour les dommages matériels;

b) exerce une activité commerciale légitime dans le secteur automobile visée au point 6.3 de la présente annexe.

Aucune condition de délivrance des identifiants d'accès autre que celles spécifiées aux points a) et b) n'est imposée par le constructeur du véhicule.

8.2. Dans les cas visés au point 5.4, lorsque le constructeur du véhicule exige l'authentification du salarié de l'opérateur et à moins que le fabricant de l'outil de diagnostic n'atteste au constructeur du véhicule, dans le respect des conditions énoncées au point 3.3, que l'opérateur dispose d'un système permettant d'identifier sans ambiguïté le salarié qui demande l'accès, le constructeur du véhicule peut refuser de délivrer des identifiants d'accès si le fabricant de l'outil de diagnostic utilisé pour accéder aux informations du système OBD n'atteste pas, outre le respect des conditions visées au point 8.1, que le salarié demandant à accéder aux informations du système OBD a conclu un contrat de travail avec l'opérateur demandant à accéder aux informations du système OBD et que le salarié concerné dispose d'une carte d'identité spécifique du pays ou d'un document équivalent en cours de validité.

8.3. Pour pouvoir bénéficier de la procédure d'authentification au titre du présent appendice, le fabricant de l'outil de diagnostic s'est engagé, dans les conditions générales des contrats conclus avec les opérateurs, à accepter, à la demande de l'opérateur indépendant, aux fins d'attester le respect des prescriptions visées aux points 8.1 et 8.2, un certificat visé au point 9.2 du présent appendice et délivré au plus tôt 60 mois avant la demande d'accès. Toutefois, lorsque l'opérateur ne demande pas à être authentifié sur la base d'un tel certificat, le fabricant de l'outil de diagnostic peut, aux fins de l'authentification, choisir de vérifier l'identité de l'opérateur ou de son salarié et le respect des critères d'autorisation au moyen de ses propres processus.

9. Organisme d'évaluation de la conformité et centre de confiance

9.1. Les certificats visés aux points 3.7 et 8.3 sont délivrés par un centre de confiance visé au point 2.1.6 de l'appendice 3 sur la base des constatations d'un organisme d'évaluation de la conformité au sens du point 4.2.2 de l'appendice 3 en ce qui concerne les circonstances visées au point 9.2.

9.2. Aux fins de la délivrance des certificats d'autorisation par un centre de confiance, l'organisme d'évaluation de la conformité:

a) satisfait aux prescriptions visées au point 4.3.1, a), b), d), e), f), g), h), i), k), l), n) et p), de l'appendice 3 de l'annexe X;

b) inspecte et confirme les circonstances visées au point 4.3.3, d) et g), de l'appendice 3 de l'annexe X. Dans les cas visés au point 5.4, lorsque le constructeur du véhicule exige l'authentification du salarié de l'opérateur, l'inspection et la confirmation de ces circonstances se rapportent au salarié de l'opérateur.

9.3. Aux fins de la délivrance des certificats d'autorisation dans les cas visés au point 9.1, le centre de confiance:

a) satisfait aux prescriptions du point 4.6 de l'appendice 3;

b) fournit toutes les informations requises au fabricant de l'outil de diagnostic afin qu'il intègre les certificats dans ses outils de diagnostic.

10. Accès du constructeur du véhicule aux informations concernant l'opérateur

10.1. Le constructeur du véhicule n'obtient, sur demande du fabricant de l'outil de diagnostic, l'accès aux informations relatives à une opération individuelle de réparation ou d'entretien enregistrée conformément au point 5 que lorsque cela est nécessaire pour des travaux de réparation ou d'entretien effectués sur un véhicule individuel pour:

a) réagir à un soupçon raisonnable d'utilisation abusive grave de l'accès au véhicule;

b) mener des enquêtes en cas de recours en responsabilité du fait des produits ou en garantie;

c) enquêter sur les incidents de cybersécurité ou de manipulation illicite, répondre aux questions du propriétaire du véhicule ou d'une autorité publique.

Dans les cas visés aux points b) et c), ces informations comprennent, le cas échéant, les informations concernant l'opérateur et/ou son personnel. Dans les cas où le fabricant de l'outil de diagnostic s'est appuyé pour l'authentification sur un certificat fourni par le centre de confiance, le CAB concerné fournit les informations requises sur la base de son évaluation d'une demande documentée du constructeur du véhicule.

Le constructeur du véhicule veille à ce que les informations relatives à une opération individuelle de réparation ou d'entretien auxquelles il a accès aux fins visées aux points a) à c) ne soient pas utilisées à d'autres fins.

10.2. Dans les cas visés au point 10.1, le fabricant de l'outil de diagnostic informe sans délai l'opérateur indépendant et, le cas échéant, son salarié, de l'accès aux informations relatives à une opération de réparation ou d'entretien individuelle ou aux informations concernant l'opérateur et/ou son personnel.

10.3. Dans les cas visés au point 10.1, a) et c), et lorsque cela est nécessaire et proportionné pour prévenir de nouvelles utilisations abusives ou faire face à des risques de cybersécurité, le constructeur du véhicule peut temporairement suspendre ou restreindre l'accès de l'outil de diagnostic concerné ou demander au fabricant de l'outil de diagnostic concerné de prendre des mesures immédiates pour restreindre temporairement l'accès de l'opérateur, de l'outil de diagnostic ou du salarié concerné aux informations du système OBD concernant les véhicules de ce constructeur.

10.4. Dans des cas exceptionnels, en réponse à un incident de cybersécurité important présent ou imminent, un constructeur de véhicules peut suspendre l'accès aux informations du système OBD, au niveau le plus fin possible, lorsque cela est nécessaire et proportionné pour réagir à l'incident concerné.

10.5. Dans les cas visés aux points 10.3 et 10.4, le constructeur du véhicule doit, dans le même temps, signaler la suspension à l'autorité compétente en matière de réception, en indiquant les motifs de la suspension et tous les éléments de preuve pertinents. La suspension est levée lorsque l'incident est réglé ou si l'autorité compétente en matière de réception demande au constructeur du véhicule de le faire.

Dans un délai de dix jours à compter du jour de la notification, l'autorité compétente en matière de réception réexamine les motifs de la suspension et, si la suspension est manifestement injustifiée ou disproportionnée, demande au constructeur du véhicule ou au fabricant de l'outil de diagnostic concerné de rétablir l'accès.

L'autorité compétente en matière de réception peut, à tout moment, demander au constructeur du véhicule et au fabricant de l'outil de diagnostic concerné de rétablir l'accès lorsqu'elle estime que les motifs de suspension ont cessé d'exister.

11. Informations à fournir aux fabricants d'outils de diagnostic

11.1. Le système RMI du constructeur du véhicule doit afficher les coordonnées et des informations sur la procédure à suivre pour obtenir les informations demandées, conformément aux points a), b), c) et d), concernant l'intégration de l'outil de diagnostic, au moment de la réception par type:

a) coordonnées pour les demandes d'informations techniques et commerciales;

b) description du processus d'intégration, avec calendrier indicatif;

c) conditions générales d'intégration des outils de diagnostic par le fabricant de l'outil de diagnostic;

d) barème des honoraires pour les services liés à l'intégration.

11.2. Sous réserve de la conclusion d'un accord de non-divulgation, le constructeur du véhicule met, sur demande, les informations suivantes à la disposition de tout opérateur indépendant se conformant à la norme TISAX, au niveau spécifié par le constructeur du véhicule conformément au point 2.5, ou à la norme ISO 27001:

a) à titre de référence, un modèle d'accord sur l'intégration de la sécurité, indiquant clairement les conditions qu'il est prévu d'inclure dans tous les accords du constructeur de véhicules avec les fabricants d'outils de diagnostic en la matière;

b) une description des exigences et des processus d'intégration sécurisée de l'outil de diagnostic, accompagnée d'un calendrier indicatif.

11.3. Le constructeur de véhicules fournit les informations suivantes et met les services suivants à la disposition du fabricant de l'outil de diagnostic, au moment de la conclusion d'un accord sur l'intégration de l'outil de diagnostic:

a) les exigences, processus et spécifications techniques détaillés et actualisés en temps utile pour l'intégration sécurisée de l'outil de diagnostic, y compris les exigences de mise en œuvre en matière de sécurité;

b) moyennant une rémunération raisonnable, comme indiqué au point 2.3, une assistance technique avec réponse instantanée pour l'intégration de la sécurité et la vérification des outils de diagnostic.

11.4. Les prescriptions de mise en œuvre en matière de sécurité visées au point 11.3 sont accompagnées d'une explication des raisons de cette exigence. Dans des cas exceptionnels, le constructeur de véhicules peut ne fournir que les prescriptions nécessaires sans explication détaillée lorsque:

a) la divulgation des objectifs spécifiques qui sous-tendent une exigence pourrait compromettre des informations exclusives ou des secrets d'affaires; ou

b) la divulgation du raisonnement révélerait une stratégie de cybersécurité plus large qui doit rester confidentielle afin de préserver l'intégrité du système.

11.5. Les informations visées aux points 11.1 à 11.3 doivent être fournies en même temps que la demande de réception par type.

12. Forum OBD

12.1. Le forum sur l'accès aux informations concernant les véhicules («forum OBD») est chargé de coordonner et de contrôler la mise en œuvre des procédures pour:

a) l'authentification et l'autorisation des opérateurs indépendants comme décrit aux points 3 et 8 du présent appendice, y compris les processus utilisés par les fabricants d'outils de diagnostic pour la vérification des critères d'autorisation, comme décrit au point 3 du présent appendice;

b) la délivrance des identifiants d'accès décrits au point 7 du présent appendice, y compris le respect des exigences en matière de traçabilité et de connectivité;

c) la divulgation des informations relatives à l'accès et à la suspension ou à la restriction de l'accès, comme décrit au point 10 du présent appendice.

12.2. Le forum

a) conseille la Commission sur la mise en œuvre du présent appendice;

b) conseille les autorités compétentes en matière de réception sur les litiges relatifs à l'interprétation et à la mise en œuvre du présent appendice;

c) conseille les constructeurs dé véhicules, les fabricants d'outils de diagnostic et les opérateurs indépendants sur:

i) l'interprétation à donner au présent appendice;

ii) les aspects pratiques des procédures visées au point 12.1;

iii) les orientations concernant la résolution des litiges relatifs à la mise en œuvre des procédures visées au point 12.1.

12.3. Les membres du forum OBD sont représentés par les constructeurs de véhicules et les opérateurs indépendants participant à la mise en œuvre et à l'utilisation des procédures et processus décrits au point 12.1.

12.4. Le forum OBD fonctionne selon la structure juridique et organisationnelle commune en tant que "forum pour l'accès aux informations sur la réparation et l'entretien (RMI) des véhicules liées à la sécurité", au sens du point 2.1.12 de l'appendice 3.

_____

(*) Règlement (UE) 2024/1257 du Parlement européen et du Conseil du 24 avril 2024 relatif à la réception par type des véhicules à moteur et des moteurs, ainsi que des systèmes, des composants et des entités techniques distinctes destinés à ces véhicules, en ce qui concerne leurs émissions et la durabilité de leurs batteries (Euro 7), modifiant le règlement (UE) 2018/858 du Parlement européen et du Conseil, et abrogeant les règlements (CE) nº 715/2007 et (CE) nº 595/2009 du Parlement européen et du Conseil, le règlement (UE) nº 582/2011 de la Commission, le règlement (UE) 2017/1151 de la Commission, le règlement (UE) 2017/2400 de la Commission et le règlement d'exécution (UE) 2022/1362 de la Commission (JO L, 2024/1257, 8.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1257/oj).

(**) Règlement nº 83 de la Commission économique pour l'Europe des Nations unies (CEE-ONU) — Prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne les émissions de polluants selon les exigences du moteur en matière de carburant (JO L 42 du 15.2.2012, p. 1, ELI: http://data.europa.eu/eli/reg/2012/83/oj).

(***) Règlement nº 168 de la Commission économique pour l'Europe des Nations unies (CEE-ONU) — Prescriptions uniformes relatives à l'homologation des voitures particulières et des véhicules utilitaires légers en ce qui concerne les émissions en conditions réelles de conduite (RDE) [2024/211] (JO L, 2024/211, 12.1.2024, ELI: http://data.europa.eu/eli/reg/2024/211/oj).

(****) Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) nº 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience) (JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(*****) Règlement nº 156 de la Commission économique pour l'Europe des Nations unies (CEE-ONU) — Prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne les mises à jour logicielles et le système de gestion des mises à jour logicielles [2021/388] (JO L 82 du 9.3.2021, p. 60, ELI: http://data.europa.eu/eli/reg/2021/388/oj).».