Lignes directrices 01/2020 sur le traitement des données à caractère personnel dans le contexte des véhicules connectés et des applications liées à la mobilité

Version 2.0

Adoptées le 9 mars 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Historique des versions

Version 2.0	9 mars 2021	Adoption des lignes directrices après consultation publique
Version 1.0	28 janvier 2020	Adoption des lignes directrices pour consultation publique

Table des matières

1 INTRODUCTION 4

1.1 Travaux connexes 5

1.2 Législation applicable 6

1.3 Champ d'application 8

1.4 Définitions 12

1.5 Risques liés à la protection des données et de la vie privée 14

2 RECOMMANDATIONS GÉNÉRALES 16

2.1 Catégories de données 16

2.2 Finalités 18

2.3 Pertinence et minimisation des données 19

2.4 Protection des données dès la conception et protection des données par défaut 19

2.5 Informations 23

2.6 Droits de la personne concernée 25

2.7 Sécurité 25

2.8 Transmission de données à caractère personnel à des tiers 26

2.9 Transfert de données à caractère personnel en dehors de l'UE/EEE 27

2.10 Utilisation de technologies Wi-Fi embarquées 28

3 ÉTUDES DE CAS 28

3.1 Prestation de services par des tiers 28

3.2 eCall 32

3.3 Études d'accidentologie 35

3.4 Lutte contre le vol de véhicules 37

vu l'article 70, paragraphe 1, point e), du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après le «RGPD»),

vu l'accord sur l'Espace économique européen (EEE) et, en particulier, son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018[1],

vu les articles 12 et 22 de son règlement intérieur,

A ADOPTÉ LES LIGNES DIRECTRICES SUIVANTES

1 INTRODUCTION

1. Symbole de l'économie du XX[e] siècle, la voiture est un produit de consommation de masse qui a des répercussions sur l'ensemble de la société. Généralement associée à la notion de liberté, la voiture est souvent considérée comme plus qu'un simple moyen de transport. Elle constitue, en effet, un espace privé permettant de jouir d'une forme d'autonomie de décision, sans subir d'interférences extérieures. À l'heure où les véhicules connectés sont de plus en plus présents, cette vision ne correspond plus à la réalité. La connectivité embarquée se répand rapidement, allant des modèles de luxe et des marques haut de gamme aux modèles milieu de gamme de grande taille, et les véhicules se transforment en des centres de données importants. Les véhicules ne sont pas les seuls à être connectés; les conducteurs et les passagers le sont aussi de plus en plus. En fait, un grand nombre de modèles lancés sur le marché ces dernières années sont équipés de capteurs et d'équipements embarqués connectés, pouvant notamment recueillir et enregistrer les performances du moteur, les habitudes de conduite, les endroits fréquentés et parfois même les mouvements oculaires du conducteur, son pouls ou des données biométriques utilisées pour identifier une personne physique de façon unique[2].

2. Le traitement de ces données s'effectue dans un écosystème complexe qui ne se limite pas aux acteurs traditionnels de l'industrie automobile, mais qui est également façonné par l'émergence de nouveaux acteurs de l'économie numérique. Ces nouveaux acteurs peuvent proposer des services d'infodivertissement, comme de la musique en ligne, des informations sur l'état des routes et sur la circulation, ou fournir des systèmes et services d'aide à la conduite, tels que des logiciels de pilotage automatique, des mises à jour sur l'état du véhicule, des assurances basées sur l'utilisation ou une cartographie dynamique. En outre, les véhicules étant connectés par l'intermédiaire de réseaux de communications électroniques, les gestionnaires des infrastructures routières et les opérateurs de télécommunications intervenant dans ce processus jouent aussi un rôle important en ce qui concerne les éventuelles opérations de traitement appliquées aux données à caractère personnel des conducteurs et des passagers.

3. Par ailleurs, les véhicules connectés génèrent de plus en plus de données, dont la plupart peuvent être considérées comme des données à caractère personnel puisqu'elles

[1] Dans le présent document, on entend par «États membres» les «États membres de l'EEE».
[2] Document infographique «Data and the connected car» (Données et voitures connectées) du Future of Privacy Forum; https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf

concernent les conducteurs ou les passagers. Même si elles ne sont pas directement associées à un nom, mais bien à des aspects et caractéristiques techniques du véhicule, les données collectées par un véhicule connecté concernent le conducteur ou les passagers du véhicule. À titre d'exemple, les données relatives au style de conduite ou à la distance parcourue, les données relatives à l'usure des pièces du véhicule, les données de localisation ou les données recueillies par les caméras peuvent concerner le comportement du conducteur et donner des informations sur d'autres personnes susceptibles de se trouver à l'intérieur du véhicule ou sur des personnes concernées passant à proximité du véhicule. Ces données techniques sont produites par une personne physique et permettent au responsable du traitement ou à toute autre personne de l'identifier, directement ou indirectement. Le véhicule peut être considéré comme un terminal susceptible d'être utilisé par différents utilisateurs. Ainsi, comme pour un ordinateur personnel, cette pluralité potentielle d'utilisateurs n'influence pas le caractère personnel des données.

4. En 2016, la Fédération internationale de l'automobile (FIA) a lancé la campagne «My Car My Data» («Ma voiture mes données») dans toute l'Europe pour avoir une idée de ce que les Européens pensent des véhicules connectés[3]. Cette campagne a mis en lumière le vif intérêt des conducteurs pour la connectivité, mais elle a également mis en évidence la vigilance dont il convient de faire preuve en ce qui concerne l'utilisation des données générées par les véhicules, ainsi que l'importance du respect de la législation en matière de protection des données à caractère personnel. L'enjeu est donc, pour chaque partie prenante, d'intégrer la dimension relative à la «protection des données à caractère personnel» dès la phase de conception des produits et de faire en sorte que les utilisateurs de véhicules bénéficient d'une transparence et d'un contrôle en ce qui concerne leurs données, conformément au considérant 78 du RGPD. Cette approche contribue à renforcer la confiance des utilisateurs et, partant, le développement à long terme de ces technologies.

1.1 Travaux connexes

5. Les véhicules connectés sont devenus un sujet important pour les régulateurs au cours de la décennie passée, et surtout ces deux dernières années. Différents travaux ont ainsi été publiés aux niveaux national et international sur la sécurité et le respect de la vie privée dans le contexte des véhicules connectés. Ces règlements et initiatives visent à compléter les cadres existants en matière de protection des données et de respect de la vie privée au moyen de règles sectorielles spécifiques ainsi qu'à fournir des orientations aux professionnels du secteur.

1.1.1 Initiatives aux niveaux européen et international

6. Depuis le 31 mars 2018, eCall, le système embarqué fondé sur le numéro 112, est obligatoire pour tous les nouveaux types de véhicules des catégories M1 et N1 (voitures particulières et véhicules utilitaires légers)[4,5]. En 2006, le groupe de travail «article 29» avait déjà adopté un document de travail sur la protection des données et le respect de la vie privée dans l'initiative «eCall»[6]. En outre, comme indiqué précédemment, le groupe de travail «article 29» a également adopté un avis en octobre 2017 sur le traitement des données à caractère personnel dans le cadre des systèmes de transport intelligents coopératifs (STI-C).

---

[3] Campagne «My Car My Data» («Ma voiture mes données»); http://www.mycarmydata.eu/.

[4] Le service eCall interopérable dans toute l'UE; https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en.

[5] Décision nº 585/2014/UE du Parlement européen et du Conseil du 15 mai 2014 concernant le déploiement du service eCall interopérable dans toute l'Union européenne (Texte présentant de l'intérêt pour l'EEE); https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014D0585.

[6] Document de travail sur la protection des données et le respect de la vie privée dans l'initiative «eCall»; http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_fr.pdf.

7. En janvier 2017, l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) a publié une étude axée sur la cybersécurité et la résilience des voitures intelligentes, dans laquelle elle a recensé les ressources sensibles ainsi que les menaces correspondantes, les risques, les facteurs d'atténuation et les mesures de sécurité envisageables à mettre en œuvre[7]. En septembre 2017, la Conférence internationale des commissaires à la protection des données et de la vie privée (ICDPPC) a adopté une résolution sur les véhicules connectés[8]. Enfin, en avril 2018, le groupe de travail international sur la protection des données dans les télécommunications (IWGDPT) a également adopté un document de travail sur les véhicules connectés[9].

1.1.2 Initiatives nationales des membres du comité européen de la protection des données (EDPB)

8. En janvier 2016, la conférence des autorités fédérales et régionales allemandes chargées de la protection des données et l'association allemande de l'industrie automobile (VDA) ont publié une déclaration commune sur les principes en matière de protection des données dans les véhicules connectés et non connectés[10]. En août 2017, le centre britannique pour les véhicules connectés et autonomes (Centre for Connected and Autonomous Vehicles - CCAV) a publié un guide sur les principes de cybersécurité relatifs aux véhicules connectés et automatisés afin de sensibiliser le secteur automobile à cette question[11]. En octobre 2017, l'autorité française chargée de la protection des données, la Commission nationale de l'informatique et des libertés (CNIL), a publié un pack de conformité sur les véhicules connectés afin d'aider les parties prenantes à intégrer la protection des données dès la phase de conception et par défaut, dans le but de permettre aux personnes concernées d'exercer un contrôle effectif sur leurs données[12].

1.2 Législation applicable

9. Le cadre juridique pertinent de l'UE est le RGPD. Celui-ci s'applique dès que le traitement de données dans le cadre de véhicules connectés passe par le traitement de données à caractère personnel de personnes physiques.

10. Outre le RGPD, la directive 2002/58/CE, telle que modifiée par la directive 2009/136/CE (ci-après la «directive "vie privée et communications électroniques"»), **établit une norme spécifique pour tous les acteurs qui souhaitent stocker des informations ou accéder à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur dans l'EEE.**

11. En effet, si la plupart des dispositions de la directive «vie privée et communications électroniques» (article 6, article 9, etc.) ne s'appliquent qu'aux fournisseurs de services de communications électroniques accessibles au public et aux fournisseurs de réseaux de communications publics, l'article 5, paragraphe 3, de cette directive est une disposition

[7] Cybersécurité et résilience des voitures intelligentes; https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars.
[8] Résolution sur la protection des données dans les véhicules automatisés et connectés; https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf.
[9] Document de travail sur les véhicules connectés; https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/.
[10] Aspects relatifs à la protection des données liés à l'utilisation de véhicules connectés et non connectés; https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf.
[11] Principes de cybersécurité pour les véhicules connectés et automatisés; https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles.
[12] Pack de conformité pour une utilisation responsable des données dans les voitures connectées; https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data.

générale qui s'applique non seulement aux services de communications électroniques, mais également à toute entité, privée ou publique, qui stocke ou consulte des informations provenant d'un équipement terminal, quelle que soit la nature des données stockées ou consultées.

12. La notion d'«équipement terminal» est définie dans la directive 2008/63/CE[13]. L'article 1er, point 1), de la directive définit l'équipement terminal comme étant «*a) tout équipement qui est connecté directement ou indirectement à l'interface d'un réseau public de télécommunications pour transmettre, traiter ou recevoir des informations; dans les deux cas, direct ou indirect, la connexion peut être établie par fil, fibre optique ou voie électromagnétique; une connexion est indirecte si un appareil est interposé entre l'équipement terminal et l'interface du réseau public; b) les équipements de stations terrestres de satellites*».

13. Ainsi, pour autant que les critères susmentionnés soient remplis, il convient de considérer le véhicule connecté et l'appareil qui lui est raccordé comme un «équipement terminal» (au même titre qu'un ordinateur, un téléphone intelligent ou une télévision intelligente), et les dispositions de l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» s'appliquent le cas échéant.

14. Comme l'EDPB l'a souligné dans son avis 5/2019 relatif aux interactions entre la directive «vie privée et communications électroniques» et le RGPD[14], l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» dispose que, de manière générale, et sous réserve des exceptions à cette règle évoquées au point 17 ci-dessous, le consentement préalable est nécessaire pour le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur. Dans la mesure où les informations stockées sur l'appareil de l'utilisateur final constituent des données à caractère personnel, l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» prime l'article 6 du RGPD pour ce qui des activités consistant à stocker ce type d'informations ou à y accéder[15]. Toute opération de traitement de données à caractère personnel effectuée à l'issue des opérations de traitement susmentionnées, y compris le traitement des données à caractère personnel obtenues en accédant à des informations dans l'équipement terminal, doit avoir une base juridique en vertu de l'article 6 du RGPD afin d'être licite[16].

15. Lorsqu'il sollicite le consentement pour le stockage d'informations ou l'obtention de l'accès à des informations conformément à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques», le responsable du traitement est tenu d'informer la personne concernée de toutes les finalités du traitement – y compris tout traitement effectué après les opérations susmentionnées (soit tout «traitement ultérieur»). Le consentement au titre de l'article 6 du RGPD constitue donc généralement la base juridique la plus appropriée pour couvrir le traitement de données à caractère personnel effectué à la suite de ces opérations (dans la mesure où la finalité de ce traitement est prise en considération dans le consentement de la personne concernée, voir points 53 et 54 ci-dessous). Dès lors, le consentement est susceptible de constituer la base juridique tant pour

[13] Directive 2008/63/CE de la Commission du 20 juin 2008 relative à la concurrence dans les marchés des équipements terminaux de télécommunications (Texte présentant de l'intérêt pour l'EEE) (version codifiée); https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A32008L0063.

[14] Comité européen de la protection des données, avis 5/2019 relatif aux interactions entre la directive «vie privée et communications électroniques» et le RGPD, en particulier en ce qui concerne la compétence, les missions et les pouvoirs des autorités de protection des données, adopté le 12 mars 2019 (ci-après l'«avis 5/2019»), point 40.

[15] Ibid., point 40.

[16] Ibid., point 41.

le stockage d'informations et l'obtention de l'accès à des informations déjà stockées que pour le traitement ultérieur de données à caractère personnel[17]. En effet, lors de l'évaluation de la conformité avec l'article 6 du RGPD, il convient de tenir compte du fait que le traitement dans son ensemble implique des activités spécifiques pour lesquelles le législateur européen a cherché à fournir une protection supplémentaire[18]. De plus, lorsqu'ils déterminent la base juridique appropriée, les responsables du traitement doivent tenir compte de l'incidence sur les droits des personnes concernées, afin de respecter le principe de loyauté[19]. En conclusion, l'article 6 du RGPD ne peut être invoqué par les responsables du traitement pour affaiblir la protection supplémentaire prévue à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques».

16. L'EDPB rappelle que la notion de consentement utilisée dans la directive «vie privée et communications électroniques» est identique à celle figurant dans le RGPD et qu'elle doit satisfaire à toutes les exigences du consentement prévues à l'article 4, paragraphe 11, et à l'article 7 du RGPD.

17. Toutefois, si le consentement est le principe, l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» permet d'exempter le stockage d'informations ou l'obtention de l'accès à des informations déjà stockées dans l'équipement terminal de l'obligation de consentement éclairé s'il satisfait à l'un des critères suivants:

- **critère d'exemption nº 1:** le stockage ou l'accès vise exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques;
- **critère d'exemption nº 2:** le stockage ou l'accès est strictement nécessaire au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur.

18. Dans ces cas, le traitement de données à caractère personnel, y compris de données à caractère personnel obtenues en accédant à des informations stockées dans l'équipement terminal, repose sur l'une des bases juridiques prévues à l'article 6 du RGPD. À titre d'exemple, le consentement n'est pas requis si le traitement des données est nécessaire pour fournir les services de navigation GPS demandés par la personne concernée lorsque ces services peuvent être qualifiés de services de la société de l'information.

1.3 Champ d'application

19. L'EDPB tient à souligner que les présentes lignes directrices visent à faciliter la conformité du traitement des données à caractère personnel effectué par un large éventail de parties prenantes actives dans ce domaine. Elles ne sont toutefois pas destinées à couvrir tous les cas d'utilisation possibles dans ce contexte ni à fournir des orientations pour chaque situation spécifique envisageable.

20. Le champ d'application du présent document est essentiellement axé sur le traitement de données à caractère personnel en rapport avec l'utilisation non professionnelle de véhicules connectés par des personnes concernées: conducteurs, passagers, propriétaires de véhicules, autres usagers de la route, etc. Les présentes lignes directrices traitent plus précisément des données à caractère personnel: i) faisant l'objet d'un traitement à

[17] Le consentement requis en vertu de l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» et le consentement nécessaire comme base juridique pour le traitement de données (article 6 du RGPD) dans le même but précis peuvent être obtenus simultanément (par exemple, en cochant une case indiquant clairement ce à quoi la personne concernée consent).
[18] Avis 5/2019, point 41.
[19] Comité européen de la protection des données, lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées, version 2.0, 8 octobre 2019, point 1.

l'intérieur du véhicule, ii) échangées entre le véhicule et les appareils qui lui sont raccordés (par exemple, le téléphone intelligent de l'utilisateur) ou iii) recueillies localement au sein du véhicule et transférées à des entités extérieures (par exemple, les constructeurs de véhicules, les gestionnaires d'infrastructures, les compagnies d'assurance, les réparateurs de véhicules automobiles) pour un traitement ultérieur.

21. La définition du véhicule connecté doit être comprise comme un concept large dans le présent document. Le véhicule connecté peut être défini comme un véhicule équipé de nombreuses unités de commande électronique (UCE) reliées entre elles au moyen d'un réseau embarqué ainsi que de dispositifs de connectivité lui permettant de partager des informations avec d'autres appareils, tant à l'intérieur qu'à l'extérieur du véhicule. Ainsi, des données peuvent être échangées entre le véhicule et les appareils personnels qui lui sont raccordés, en permettant par exemple l'émulation d'applications mobiles sur l'unité d'information et de divertissement intégrée au tableau de bord du véhicule. En outre, le développement d'applications mobiles autonomes, c'est-à-dire indépendantes du véhicule (par exemple, des applications reposant sur la seule utilisation du téléphone intelligent), pour aider les conducteurs s'inscrit dans le champ d'application du présent document, puisque ces applications contribuent aux capacités de connectivité du véhicule même si elles ne reposent pas effectivement sur la transmission de données avec le véhicule en tant que tel. Les applications pour véhicules connectés sont multiples et variées et peuvent comprendre les fonctions suivantes[20]:

22. *Gestion de la mobilité:* fonctions permettant au conducteur d'atteindre une destination rapidement, et de façon économe, en fournissant en temps utile des informations sur la navigation GPS, les conditions environnementales potentiellement dangereuses (routes verglacées, par exemple), les encombrements de la circulation ou les travaux de construction routière, l'aide au stationnement dans un parking ou un garage, l'optimisation de la consommation de carburant ou la tarification routière.

23. *Gestion du véhicule:* fonctions censées aider le conducteur à réduire les coûts d'exploitation du véhicule et à faciliter son utilisation, telles que les notifications relatives à l'état du véhicule et les rappels d'entretien, le transfert des données d'usage (par exemple, pour les services de réparation du véhicule), les assurances personnalisées (au kilomètre/selon la conduite), les opérations à distance (système de chauffage, par exemple) ou les configurations de profil (position assise, par exemple).

24. *Sécurité routière:* fonctions avertissant le conducteur des dangers externes et des réactions internes, comme les systèmes de protection contre les collisions, les alertes en cas de danger, les systèmes de détection de dérive de la trajectoire, les systèmes de détection de somnolence du conducteur, les systèmes d'appel d'urgence (eCall) ou les «boîtes noires» visant à faciliter les enquêtes en cas d'accident (enregistreur de données d'événement).

25. *Divertissement:* fonctions d'information et de divertissement du conducteur et des passagers, comme les interfaces des téléphones intelligents (communications téléphoniques «mains libres», messages textes générés par la voix), les points chauds des réseaux locaux sans fil, la musique, les vidéos, l'internet, les médias sociaux, les services de bureau mobile ou de maison intelligente.

26. *Aide au conducteur:* fonctions de conduite partiellement ou entièrement automatisée, comme une aide opérationnelle ou un système de pilote automatique lorsque la circulation est dense, en cas de stationnement ou sur les autoroutes.

[20] PwC Strategy& 2014, «In the fast lane. The bright future of connected cars»: https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf.

27. *Bien-être:* fonctions permettant de surveiller le confort du conducteur, ses capacités et son aptitude à la conduite, comme les fonctions de détection de fatigue ou d'assistance médicale.

28. Ainsi, les véhicules peuvent être connectés nativement ou non et des données à caractère personnel peuvent être collectées à l'aide de plusieurs moyens, notamment par: i) des capteurs installés dans les véhicules, ii) des boîtiers télématiques ou iii) des applications mobiles (auxquelles le conducteur peut accéder à partir d'un appareil lui appartenant). Pour relever du présent document, les applications mobiles doivent être liées à l'environnement de conduite. À titre d'exemple, les applications de navigation GPS entrent dans le champ d'application. Par contre, les applications dont les fonctionnalités ne font que proposer des lieux d'intérêt (restaurants, monuments historiques, etc.) aux conducteurs ne relèvent pas des présentes lignes directrices.

29. La plupart des données générées par un véhicule connecté concernent une personne physique identifiée ou identifiable et constituent donc des données à caractère personnel. Il s'agit notamment de données permettant une identification directe (par exemple, l'identité complète du conducteur) et de données permettant une identification indirecte, comme le détail des trajets effectués, les données d'usage du véhicule (par exemple, les données relatives au style de conduite ou à la distance parcourue) ou les données techniques du véhicule (par exemple, les données relatives à l'usure des pièces du véhicule), qui, par recoupement avec d'autres fichiers et notamment le numéro d'identification du véhicule (VIN), peuvent être reliées à une personne physique. Parmi les données à caractère personnel que l'on retrouve dans les véhicules connectés figurent également des métadonnées relatives, par exemple, à l'état d'entretien du véhicule. En d'autres termes, toute donnée pouvant être associée à une personne physique relève donc du présent document.

30. L'écosystème des véhicules connectés couvre un large éventail de parties prenantes. Cet écosystème comprend plus précisément les acteurs traditionnels de l'industrie automobile et les acteurs émergents de l'industrie numérique. Les présentes lignes directrices s'adressent donc aux constructeurs de véhicules, aux fabricants d'équipements, aux fournisseurs automobiles, aux réparateurs de véhicules automobiles, aux concessionnaires automobiles, aux prestataires de services automobiles, aux gestionnaires de parcs automobiles, aux compagnies d'assurances automobiles, aux prestataires de services de divertissement, aux opérateurs de télécommunications, aux gestionnaires des infrastructures routières, aux autorités publiques et aux personnes concernées. L'EDPB souligne que les catégories de personnes concernées diffèrent d'un service à l'autre (par exemple, conducteurs, propriétaires, passagers, etc.). Il s'agit d'une liste non exhaustive, car cet écosystème comprend un large éventail de services, parmi lesquels des services nécessitant une authentification ou une identification directe et des services n'en nécessitant pas.

31. Certains traitements de données sont effectués par des personnes physiques à l'intérieur du véhicule «*dans le cadre d'une activité strictement personnelle ou domestique*» et ne relèvent donc pas du RGPD[21]. Il s'agit notamment de l'utilisation de données à caractère personnel à l'intérieur des véhicules par les seules personnes concernées qui ont fourni ces données dans le tableau de bord du véhicule. L'EDPB rappelle toutefois qu'en vertu de son considérant 18, le RGPD «*s'applique aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques*».

[21] Voir article 2, paragraphe 2, point c), du RGPD.

1.3.1 Hors du champ d'application du présent document

32. Les employeurs qui fournissent des voitures de société aux membres de leur personnel pourraient vouloir surveiller les actions de leurs employés (par exemple, afin de garantir la sécurité des employés, des marchandises ou des véhicules, d'affecter des ressources, d'assurer le suivi et la facturation d'un service ou de vérifier le temps de travail). Le traitement des données effectué par les employeurs à cet égard soulève des considérations spécifiques au contexte de l'emploi, qui peuvent être régies par le droit du travail au niveau national, lequel ne peut être détaillé dans les présentes lignes directrices[22].

33. Si le traitement des données dans le contexte des véhicules utilitaires utilisés à des fins professionnelles (comme les transports publics) ainsi que le transport partagé et la solution de mobilité à la demande (MaaS) peuvent soulever des considérations spécifiques qui ne relèvent pas des présentes lignes directrices générales, de nombreux principes et recommandations figurant dans le présent document s'appliquent toutefois à ces types de traitement.

34. Les véhicules connectés sont des systèmes radio. Ils font donc l'objet d'un suivi passif notamment par Wi-Fi ou Bluetooth. En ce sens, ils ne diffèrent pas des autres appareils connectés et relèvent de la directive «vie privée et communications électroniques», qui est en cours de révision. Cette logique exclut donc également le suivi à grande échelle des véhicules équipés de Wi-Fi[23] par un réseau dense de passants utilisant des services communs de localisation des téléphones intelligents. Ceux-ci signalent systématiquement tous les réseaux Wi-Fi visibles aux serveurs centraux. Le Wi-Fi pouvant être considéré comme un identificateur secondaire du véhicule[24], cela risque d'entraîner la collecte systématique et constante de profils complets des mouvements du véhicule.

35. Les véhicules sont de plus en plus équipés de dispositifs d'enregistrement d'images (système de caméra de stationnement ou caméra-témoin de circulation, par exemple). Comme il s'agit de filmer des lieux publics, ce qui nécessite une évaluation du cadre législatif pertinent propre à chaque État membre, ce traitement de données ne relève pas des présentes lignes directrices.

36. Le traitement des données permettant la mise en œuvre de systèmes de transport intelligents coopératifs (STI-C) – définis dans la directive 2010/40/UE[25] – est examiné dans un avis spécifique du groupe de travail «article 29»[26]. Bien que la définition du concept de STI-C figurant dans la directive ne comporte aucune spécification technique, dans son avis, le groupe de travail «article 29» se concentre sur les communications à courte portée, c'est-à-dire des communications qui ne nécessitent pas l'intervention d'un opérateur de réseau. Plus précisément, le groupe de travail «article 29» présente une analyse de cas d'utilisation spécifiques pour le déploiement initial et s'engage à examiner à un stade ultérieur les nouvelles questions qui se poseront certainement lorsque des niveaux d'automatisation

[22] Le groupe de travail «article 29» aborde ce sujet dans son avis 2/2017 sur le traitement des données sur le lieu de travail (WP249); https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.
[23] Pour plus de détails, voir: https://www.datenschutzzentrum.de/artikel/1269-Location-Services-can-Systematically-Track-Vehicles-with-WiFi-Access-Points-at-Large-Scale.html.
[24] Markus Ullmann, Tobias Franz et Gerd Nolden, «Vehicle Identification Based on Secondary Vehicle Identifier – Analysis, and Measurements», *Proceedings*, VEHICULAR 2017, The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications, Nice, France, 23 au 27 juillet 2017, p. 32 à 37.
[25] Directive 2010/40/UE du 7 juillet 2020 concernant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport; https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32010L0040.
[26] Groupe de travail «article 29» – avis 3/2017 sur le traitement des données à caractère personnel dans le cadre des systèmes de transport intelligents coopératifs (STI-C); http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171.

supérieurs seront atteints. Étant donné que les implications en matière de protection des données dans le contexte des STI-C sont très spécifiques (quantités inédites de données de localisation, diffusion continue de données à caractère personnel, échange de données entre véhicules et autres infrastructures routières, etc.) et que cette question est toujours en cours de discussion au niveau européen, les présentes lignes directrices ne couvrent pas le traitement des données à caractère personnel dans ce contexte.

37. Enfin, le présent document n'a pas pour objet d'aborder tous les problèmes et questions que peuvent poser les véhicules connectés et ne saurait donc être considéré comme exhaustif.

1.4 Définitions

38. Le **traitement** de données à caractère personnel désigne toute opération faisant intervenir des données à caractère personnel, comme la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction, etc.[27]

39. La **personne concernée** désigne la personne physique à laquelle se rapportent les données qui font l'objet du traitement. Dans le contexte des véhicules connectés, il peut notamment s'agir du conducteur (principal ou occasionnel), du passager ou du propriétaire du véhicule[28].

40. Le **responsable du traitement** désigne la personne qui détermine les finalités et les moyens du traitement effectué dans des véhicules connectés[29]. Il peut s'agir de prestataires de services qui traitent les données du véhicule pour envoyer au conducteur des informations sur la circulation, des messages de conduite écologique ou des alertes relatives au fonctionnement du véhicule, de compagnies d'assurance proposant des contrats au kilomètre ou de constructeurs de véhicules collectant des données sur l'usure des pièces du véhicule afin d'améliorer sa qualité. Conformément à l'article 26 du RGPD, deux ou plusieurs responsables du traitement peuvent déterminer conjointement les finalités et les moyens du traitement et peuvent donc être considérés comme des responsables conjoints du traitement. Dans ce cas, ils doivent déterminer clairement leurs obligations respectives, notamment en ce qui concerne l'exercice des droits des personnes concernées et la fourniture des informations visées aux articles 13 et 14 du RGPD.

41. Le **sous-traitant** désigne toute personne chargée de traiter des données à caractère personnel au nom et pour le compte du responsable du traitement[30]. Le sous-traitant collecte et traite des données sur instruction du responsable du traitement, sans les utiliser à ses propres fins. Par exemple, dans un certain nombre de cas, les fabricants d'équipements et les fournisseurs automobiles peuvent traiter des données pour le compte de constructeurs de véhicules (ce qui ne veut pas dire qu'ils ne peuvent pas être des responsables du traitement à d'autres fins). Outre l'obligation faite aux sous-traitants de mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, l'article 28 du RGPD énonce les obligations des sous-traitants.

[27] Voir article 4, paragraphe 2, du RGPD.
[28] Voir article 4, paragraphe 1, du RGPD.
[29] Voir article 4, paragraphe 7, du RGPD et comité européen de la protection des données, lignes directrices 07/2020 sur les notions de responsable de traitement et de sous-traitant dans le RGPD (ci-après les «lignes directrices 07/2020»).
[30] Voir article 4, paragraphe 8, du RGPD et lignes directrices 07/2020.

42. Le **destinataire** désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers[31]. À titre d'exemple, le partenaire commercial d'un prestataire de services qui reçoit de ce dernier des données à caractère personnel tirées du véhicule est un destinataire de données à caractère personnel. Qu'il agisse en tant que nouveau responsable du traitement ou en tant que sous-traitant, le destinataire est tenu de respecter toutes les obligations imposées par le RGPD.

43. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires[32]; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement. Par exemple, les services répressifs sont des tiers autorisés lorsqu'ils demandent des données à caractère personnel dans le cadre d'une enquête conformément au droit de l'Union européenne ou au droit d'un État membre.

[31] Voir article 4, paragraphe 9, du RGPD et lignes directrices 07/2020.
[32] Article 4, paragraphe 9, et considérant 31 du RGPD.

1.5 Risques liés à la protection des données et de la vie privée

44. Le groupe de travail «article 29» a déjà exprimé à propos des systèmes de l'internet des objets (IDO) plusieurs préoccupations qui peuvent également s'appliquer aux véhicules connectés[33]. Déjà mises en évidence à propos de l'IDO, les questions relatives à la sécurité et au contrôle des données sont encore plus sensibles dans le contexte des véhicules connectés, car elles soulèvent des préoccupations en matière de sécurité routière – et peuvent avoir une incidence sur l'intégrité physique du conducteur – dans un environnement traditionnellement perçu comme isolé et protégé contre les interférences extérieures.

45. En outre, les véhicules connectés suscitent des préoccupations importantes en matière de protection des données et de respect de la vie privée en ce qui concerne le traitement des données de localisation. Leur caractère de plus en plus intrusif peut, en effet, mettre à rude épreuve les possibilités actuelles de préserver son anonymat. L'EDPB tient à accorder une attention particulière et à sensibiliser les parties prenantes au fait que l'utilisation de technologies de localisation appelle la mise en œuvre de garanties spécifiques afin de prévenir le risque que des personnes soient surveillées et des données exploitées abusivement.

1.5.1 Absence de contrôle et asymétrie de l'information

46. Les conducteurs et les passagers ne sont pas toujours correctement informés du traitement des données effectué dans un véhicule connecté ou par l'intermédiaire de celui-ci. Les informations ne peuvent être communiquées qu'au propriétaire du véhicule, qui n'est pas systématiquement le conducteur, et il arrive également qu'elles ne soient pas fournies en temps utile. Les fonctionnalités ou les options proposées risquent donc d'être insuffisantes pour exercer le contrôle nécessaire permettant aux personnes concernées de faire valoir leurs droits en matière de protection des données et de respect de la vie privée. Il s'agit d'un point important car, pendant leur durée de vie, les véhicules peuvent appartenir à plusieurs propriétaires, parce qu'ils sont revendus ou parce qu'ils sont pris en crédit-bail plutôt qu'achetés.

47. En outre, la communication dans le véhicule peut être déclenchée automatiquement ou par défaut, sans que la personne le sache. Lorsqu'il est impossible de contrôler effectivement les interactions entre le véhicule et l'équipement qui y est connecté, il est inévitablement extrêmement difficile pour l'utilisateur de contrôler le flux de données. Il est encore plus difficile de contrôler son utilisation ultérieure et d'éviter ainsi tout détournement d'usage.

1.5.2 Qualité du consentement de l'utilisateur

48. L'EDPB tient à souligner que, lorsque le traitement des données repose sur le consentement, tous les éléments du consentement valable doivent être réunis, ce qui signifie que le consentement doit être libre, spécifique et éclairé et constituer une indication univoque des souhaits de la personne concernée, tels qu'ils sont interprétés dans les lignes directrices de l'EDPB sur le consentement[34]. Les responsables du traitement des données doivent accorder une attention particulière aux modalités d'obtention d'un consentement valable de différents participants, comme les propriétaires ou les utilisateurs de véhicules. Ce consentement doit être donné séparément, à des fins spécifiques, et ne peut être associé au contrat d'achat ou de crédit-bail d'une voiture neuve. Le consentement doit pouvoir être aussi facilement retiré qu'il est donné.

---

[33] Groupe de travail «article 29» – avis 8/2014 sur les récentes évolutions relatives à l'internet des objets; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_fr.pdf.
[34] Comité européen de la protection des données, lignes directrices 5/2020 sur le consentement au sens du règlement 2016/679, version 1.1, 4 mai 2020 (ci-après les «lignes directrices 5/2020»).

49. Il en va de même lorsqu'il est nécessaire d'obtenir un consentement pour se conformer à la directive «vie privée et communications électroniques», par exemple en cas de stockage d'informations ou d'obtention de l'accès à des informations déjà stockées dans le véhicule, comme l'exige dans certains cas l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques». En effet, comme indiqué ci-dessus, le consentement dans ce contexte doit être interprété à la lumière du RGPD.

50. Dans de nombreux cas, l'utilisateur peut ne pas être au courant du traitement des données effectué dans son véhicule. Ce manque d'informations constitue un obstacle majeur à la démonstration d'un consentement valable au titre du RGPB, puisque le consentement doit être éclairé. Dans de telles circonstances, le consentement ne saurait être invoqué comme base juridique du traitement des données correspondant au titre du RGPD.

51. Il peut s'avérer difficile d'appliquer les mécanismes traditionnellement utilisés pour obtenir le consentement des personnes concernées dans le contexte des véhicules connectés, ce qui se traduit par un consentement «de mauvaise qualité» fondé sur des informations insuffisantes ou par l'impossibilité factuelle de fournir un consentement adapté en fonction des préférences exprimées par les personnes. Dans la pratique, il peut également être compliqué d'obtenir le consentement des conducteurs et des passagers qui ne sont pas liés au propriétaire du véhicule dans le cas des véhicules d'occasion, pris en crédit-bail, en location ou empruntés.

52. Lorsque la directive «vie privée et communications électroniques» n'exige pas le consentement de la personne concernée, il incombe néanmoins au responsable du traitement de choisir la base juridique visée à l'article 6 du RGPD qui est la mieux adaptée aux circonstances pour le traitement des données à caractère personnel.

1.5.3 Traitement ultérieur des données à caractère personnel

53. Lorsque des données sont collectées sur la base du consentement requis en vertu de l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» ou de l'une des dérogations prévues à l'article 5, paragraphe 3, puis traitées conformément à l'article 6 du RGPD, elles ne peuvent faire l'objet d'un traitement ultérieur que si le responsable du traitement sollicite un nouveau consentement pour cette autre finalité ou s'il peut démontrer que le traitement est fondé sur le droit de l'Union ou le droit d'un État membre afin de garantir les objectifs prévus à l'article 23, paragraphe 1, du RGPD[35]. L'EDPB estime qu'un traitement ultérieur sur la base d'un test de compatibilité conformément à l'article 6, paragraphe 4, du RGPD n'est pas possible dans de telles circonstances, car il porterait atteinte à la norme de protection des données de la directive «vie privée et communications électroniques». En effet, lorsque la directive «vie privée et communications électroniques» exige un consentement, celui-ci doit être spécifique et éclairé, ce qui signifie que les personnes concernées doivent avoir connaissance de chaque finalité du traitement des données et être habilitées à refuser des finalités spécifiques[36]. Le fait de considérer qu'un traitement ultérieur sur la base d'un test de compatibilité conformément à l'article 6, paragraphe 4, du RGPD est possible reviendrait à contourner le principe même des exigences en matière de consentement prévues dans la directive actuelle.

54. L'EDPB rappelle que le consentement initial ne légitime jamais un traitement ultérieur, puisque le consentement doit être éclairé et spécifique pour être valable.

55. Par exemple, les données télémétriques collectées lors de l'utilisation du véhicule à des fins de maintenance ne peuvent être divulguées sans le consentement des utilisateurs à des

[35] Voir également comité européen de la protection des données, lignes directrices 10/2020 sur les restrictions prévues à l'article 23 du RGPD.
[36] Lignes directrices 5/2020, sections 3.2 et 3.3.

compagnies d'assurance automobile afin que celles-ci créent des profils de conducteur pour proposer des polices d'assurance fondées sur le comportement au volant.

56. Par ailleurs, les données collectées par des véhicules connectés peuvent être traitées par les services répressifs pour détecter des excès de vitesse ou d'autres infractions si et quand les conditions spécifiques de la directive en matière de protection des données dans le domaine répressif sont remplies. Dans ce cas, ces données sont considérées comme se rapportant à des condamnations pénales et à des infractions dans les conditions prévues à l'article 10 du RGPD et à toute législation nationale applicable. Les constructeurs peuvent communiquer ces données aux services répressifs si les conditions spécifiques de ce traitement sont remplies. L'EDPB indique que le traitement de données à caractère personnel dans le seul but de répondre aux demandes des services répressifs ne constitue pas une finalité déterminée, explicite et légitime au sens de l'article 5, paragraphe 1, point b), du RGPD. Lorsque les services répressifs y sont autorisés par la loi, ils peuvent être des tiers au sens de l'article 4, paragraphe 10, du RGPD, auquel cas les constructeurs sont autorisés à leur fournir toutes les données dont ils disposent, sous réserve du cadre juridique applicable dans chaque État membre.

1.5.4 Collecte de données excessive

57. Face au nombre toujours plus grand de capteurs déployés dans les véhicules connectés, il existe un risque très élevé de collecte de données excessive au regard de ce qui est nécessaire pour atteindre la finalité du traitement.

58. La mise au point de nouvelles fonctionnalités, et plus particulièrement celles basées sur des algorithmes d'apprentissage automatique, peut nécessiter une grande quantité de données recueillies sur une longue période.

1.5.5 Sécurité des données à caractère personnel

59. La pluralité des fonctionnalités, services et interfaces (par exemple, web, USB, RFID, Wi-Fi) offerts par les véhicules connectés augmente la surface d'attaque et donc le nombre de vulnérabilités susceptibles de compromettre les données à caractère personnel. Contrairement à la plupart des dispositifs IDO, les véhicules connectés sont des systèmes essentiels dans lesquels une faille de sécurité peut mettre en danger la vie de l'utilisateur et des personnes qui l'entourent. Il est donc plus important que jamais de parer au risque que des pirates informatiques tentent d'exploiter les vulnérabilités des véhicules connectés.

60. En outre, les données à caractère personnel stockées dans les véhicules et/ou sur des sites extérieurs (par exemple, dans des infrastructures d'informatique en nuage) doivent être correctement protégées contre tout accès non autorisé. Par exemple, lors de l'entretien d'un véhicule, celui-ci est confié à un technicien qui doit avoir accès à certaines données techniques du véhicule. Le technicien a besoin d'accéder aux données techniques du véhicule, mais il est possible qu'il tente d'accéder à toutes les données qui y sont stockées.

2 RECOMMANDATIONS GÉNÉRALES

61. Afin d'atténuer les risques susmentionnés encourus par les personnes concernées, les recommandations générales suivantes devraient être suivies par les constructeurs de véhicules et d'équipements, les prestataires de services ou toute autre partie prenante susceptible d'agir en tant que responsable du traitement ou sous-traitant en ce qui concerne les véhicules connectés.

2.1 Catégories de données

62. Comme indiqué dans l'introduction, la plupart des données associées aux véhicules connectés sont considérées comme des données à caractère personnel dans la mesure où il est possible de les associer à une ou plusieurs personnes identifiables. Il s'agit notamment

des données techniques relatives aux mouvements du véhicule (par exemple, la vitesse, la distance parcourue) ainsi qu'à l'état du véhicule (par exemple, la température du liquide de refroidissement, le régime du moteur, la pression des pneus). Certaines données générées par des véhicules connectés peuvent également nécessiter une attention particulière en raison de leur sensibilité et/ou de leurs répercussions potentielles sur les droits et les intérêts des personnes concernées. À ce jour, l'EDPB a recensé trois catégories de données à caractère personnel nécessitant une attention particulière de la part des constructeurs de véhicules et d'équipements, des prestataires de services et des autres responsables du traitement: les données de localisation, les données biométriques (ainsi que toute catégorie particulière de données définie à l'article 9 du RGPD) et les données susceptibles de révéler des infractions routières ou autres.

2.1.1 Données de localisation

63. Lorsqu'ils collectent des données à caractère personnel, les constructeurs de véhicules et d'équipements, les prestataires de services et les autres responsables du traitement devraient garder à l'esprit que les données de localisation sont particulièrement révélatrices des habitudes de vie des personnes concernées. Les trajets réalisés sont très caractéristiques en ce qu'ils peuvent permettre de déduire le lieu de travail, le domicile ainsi que les centres d'intérêt (loisirs) du conducteur, et peuvent éventuellement révéler des informations sensibles comme la religion, par l'intermédiaire du lieu de culte, ou l'orientation sexuelle, par l'intermédiaire des lieux fréquentés. Par conséquent, les constructeurs de véhicules et d'équipements, les prestataires de services et les autres responsables du traitement devraient particulièrement veiller à ne pas collecter de données de localisation, à moins que cela ne soit absolument nécessaire pour la finalité du traitement. Par exemple, lorsque le traitement consiste à détecter le mouvement du véhicule, le gyroscope suffit à remplir cette fonction, sans qu'il soit nécessaire de collecter des données de localisation.

64. De manière générale, la collecte des données de localisation est également subordonnée au respect des principes suivants:

- un paramétrage adéquat de la fréquence d'accès aux données de localisation collectées et de la finesse de ces données par rapport à la finalité du traitement. À titre d'exemple, une application météo ne devrait pas pouvoir accéder toutes les secondes à la localisation du véhicule, et ce même avec le consentement de la personne concernée;
- la fourniture d'une information précise sur les finalités du traitement (par exemple, existe-t-il une conservation de l'historique des localisations? Dans l'affirmative, quel en est l'objectif?);
- lorsque le traitement est basé sur le consentement, le recueil d'un consentement valable (libre, spécifique et éclairé) distinct des conditions générales de vente ou d'utilisation, par exemple, sur l'ordinateur de bord;
- l'activation de la localisation uniquement lorsque l'utilisateur lance une fonctionnalité qui nécessite de connaître la localisation du véhicule, et non par défaut et en continu au démarrage de la voiture;
- l'information de l'utilisateur de l'activation de la localisation, notamment par le biais d'icônes (par exemple, une flèche qui se déplace à l'écran);
- la possibilité de désactiver la localisation à tout moment;
- la définition d'une durée de conservation limitée.

2.1.2 Données biométriques

65. Dans le contexte des véhicules connectés, les données biométriques utilisées aux fins d'identifier une personne physique de manière unique peuvent être traitées, conformément

à l'article 9 du RGPD et aux exceptions nationales, entre autres, pour permettre l'accès à un véhicule, authentifier le conducteur/propriétaire et/ou permettre l'accès aux paramètres et préférences du profil d'un conducteur. Lorsqu'un recours aux données biométriques est envisagé, garantir à la personne concernée un contrôle total de ses données consiste, d'une part, à prévoir l'existence d'une solution non biométrique (par exemple, l'utilisation d'une clé physique ou d'un code) sans contrainte supplémentaire (ce qui signifie que l'utilisation de données biométriques ne devrait pas être obligatoire) et, d'autre part, à stocker et à comparer le modèle biométrique sous forme chiffrée, uniquement en local, sans que les données biométriques ne soient traitées par un terminal de lecture/comparaison extérieur.

66. S'agissant des données biométriques[37], il importe de s'assurer que la solution d'authentification biométrique est suffisamment fiable, en observant notamment les principes suivants:

- le réglage de la solution biométrique utilisée (par exemple, les taux de faux positifs et de faux négatifs) est adapté au niveau de sécurisation du contrôle d'accès souhaité;
- la solution biométrique utilisée repose sur un capteur résistant aux attaques (comme l'utilisation d'une empreinte imprimée à plat pour la reconnaissance d'empreinte digitale);
- le nombre d'essais d'authentification est limité;
- le modèle/gabarit biométrique est stocké dans le véhicule, et ce de manière chiffrée à l'aide d'un algorithme cryptographique et d'une gestion des clés conforme à l'état des connaissances;
- les données brutes utilisées pour la constitution du gabarit biométrique et pour l'authentification de l'utilisateur sont traitées en temps réel sans être conservées, même en local.

2.1.3 Données révélant des infractions pénales ou autres

67. Afin de traiter les données relatives à d'éventuelles infractions pénales au sens de l'article de l'article 10 du RGPD, l'EDPB recommande de recourir au traitement local des données lorsque la personne concernée contrôle totalement le traitement en question (voir l'explication consacrée au traitement local à la section 2.4). En effet, à quelques exceptions près (voir l'étude de cas sur l'accidentologie présentée au point 3.3 ci-dessous), le traitement externe des données révélant des infractions pénales ou autres est interdit. Dès lors, en fonction de la sensibilité des données, des mesures de sécurité rigoureuses, comme celles décrites à la section 2.7, doivent être mises en place pour offrir une protection contre l'accès illégitime à ces données, leur modification et leur effacement.

68. En effet, certaines catégories de données à caractère personnel provenant de véhicules connectés pourraient révéler qu'une infraction pénale ou autre a été ou est commise (ci-après les «données relatives aux infractions») et donc être soumises à des restrictions particulières (par exemple, les données indiquant que le véhicule a franchi une ligne blanche, la vitesse instantanée d'un véhicule combinée à des données de localisation précises). En particulier, si ces données étaient traitées par les autorités nationales compétentes aux fins d'une enquête pénale ou de poursuites judiciaires relatives à des infractions pénales, les garanties prévues à l'article 10 du RGPD s'appliqueraient.

2.2 Finalités

69. Les données à caractère personnel peuvent être traitées à des fins très diverses en rapport avec les véhicules connectés, notamment la sécurité des conducteurs, les assurances, l'efficacité des transports et les services de divertissement ou d'information. Conformément

[37] Le principe d'interdiction énoncé à l'article 9, paragraphe 1, du RGPD ne concerne que les «*données biométriques aux fins d'identifier une personne physique de manière unique*».

au RGPD, les responsables du traitement doivent veiller à ce que les finalités du traitement des données à caractère personnel soient «déterminées, explicites et légitimes», à ce que ces données ne soient pas traitées ultérieurement d'une manière incompatible avec ces finalités et à ce qu'un fondement juridique valable soit prévu pour le traitement des données à caractère personnel, comme indiqué à l'article 5 du RGPD. La troisième partie des présentes lignes directrices contient des exemples concrets de finalités susceptibles d'être poursuivies par les responsables du traitement opérant dans le contexte des véhicules connectés, ainsi que des recommandations spécifiques pour chaque type de traitement.

2.3 Pertinence et minimisation des données

70. Afin de respecter le principe de minimisation des données[38], les constructeurs de véhicules et d'équipement, les prestataires de services et les autres responsables du traitement devraient accorder une attention particulière aux catégories de données qu'ils ont besoin d'obtenir d'un véhicule connecté, étant donné qu'ils ne doivent collecter que les données à caractère personnel pertinentes et nécessaires au traitement. Par exemple, les données de localisation sont particulièrement intrusives et peuvent révéler de nombreuses habitudes de vie des personnes concernées. Dès lors, les acteurs du secteur devraient particulièrement veiller à ne pas collecter de données de localisation, à moins que cela ne soit absolument nécessaire aux fins du traitement (voir l'explication consacrée aux données de localisation à la section 2.1 ci-dessus).

2.4 Protection des données dès la conception et protection des données par défaut

71. Compte tenu de la quantité et de la diversité de données à caractère personnel produites par les véhicules connectés, l'EDPB souligne que les responsables du traitement sont tenus de veiller à ce que les technologies déployées dans le contexte des véhicules connectés soient configurées de manière à respecter la vie privée des personnes en appliquant les obligations en matière de protection des données dès la conception et de protection des données par défaut prévues à l'article 25 du RGPD. Les technologies devraient être conçues de façon à réduire au minimum la collecte de données à caractère personnel, à proposer un paramétrage par défaut favorable au respect de la vie privée et à faire en sorte que les personnes concernées soient bien informées et aient la possibilité de modifier facilement les configurations associées à leurs données à caractère personnel. Des orientations spécifiques sur la manière dont les constructeurs et les prestataires de services peuvent respecter la protection des données dès la conception et la protection des données par défaut pourraient être utiles au secteur ainsi qu'aux fournisseurs tiers d'applications.

72. Certaines pratiques générales, décrites ci-dessous, peuvent également contribuer à atténuer les risques pour les droits et les libertés des personnes physiques associés aux véhicules connectés[39].

2.4.1 Traitement local des données à caractère personnel

73. De manière générale, les constructeurs de véhicules et d'équipements, les prestataires de services et les autres responsables du traitement devraient, dans la mesure du possible, utiliser des processus qui ne font pas intervenir de données à caractère personnel ou le transfert de données à caractère personnel en dehors du véhicule (les données étant donc traitées en interne). La nature des véhicules connectés présente toutefois des risques, comme la possibilité que des attaques soient commises par des acteurs extérieurs contre le traitement local ou que des données locales soient divulguées en raison de la vente de pièces du véhicule. Il convient donc d'accorder une attention particulière à cet égard et de prendre des mesures de sécurité appropriées pour faire en sorte que les données continuent

[38] Article 5, paragraphe 1, point c), du RGPD.

[39] Voir également comité européen de la protection des données, lignes directrices 4/2019 relatives à l'article 25 sur la protection des données dès la conception et la protection des données par défaut, version 2.0, adoptées le 20 octobre 2020 (ci-après les «lignes directrices 4/2019»).

d'être traitées au niveau local. Ce scénario présente l'avantage de garantir à l'utilisateur le contrôle exclusif et total de ses données à caractère personnel et comporte donc, «dès la conception», moins de risques pour le respect de la vie privée, notamment en interdisant tout traitement de données par des parties prenantes à l'insu de la personne concernée. Il permet également le traitement de données sensibles telles que les données biométriques ou les données relatives à des infractions pénales ou autres, ainsi que de données de localisation détaillées qui seraient autrement soumises à des règles plus strictes (voir ci-dessous). Dans le même ordre d'idées, ce scénario présente moins de risques en matière de cybersécurité et implique peu de latence, ce qui le rend particulièrement adapté aux fonctions automatisées d'assistance à la conduite. Voici quelques exemples de ce type de solution:

- des applications de conduite écologique qui traitent les données dans le véhicule afin d'afficher des conseils de conduite écologique en temps réel sur le tableau de bord;
- des applications qui passent par le transfert de données à caractère personnel vers un appareil tel qu'un téléphone intelligent que l'utilisateur contrôle totalement (par Bluetooth ou Wi-Fi, par exemple) et qui ne transmettent pas les données du véhicule aux fournisseurs d'applications ou aux constructeurs de véhicules; il peut s'agir, par exemple, du couplage de téléphones intelligents pour utiliser le dispositif d'affichage de la voiture, les systèmes multimédias, le microphone (ou d'autres capteurs) pour des appels téléphoniques, etc., dans la mesure où les données collectées restent sous le contrôle de la personne concernée et sont exclusivement utilisées pour fournir le service qu'elle a demandé;
- des applications renforçant la sécurité à bord du véhicule, comme celles qui envoient des signaux sonores ou des vibrations du volant en cas de dépassement sans clignotant ou de franchissement de ligne blanche ou qui alertent sur l'état du véhicule (par exemple, alerte sur l'usure des plaquettes de frein);
- des applications de déverrouillage, démarrage et/ou activation de certaines commandes du véhicule grâce aux données biométriques du conducteur qui sont stockées dans le véhicule (comme des modèles de visage ou de voix ou des points caractéristiques des empreintes digitales).

74. Les applications susmentionnées nécessitent un traitement effectué pour l'exécution d'activités purement personnelles par une personne physique (c'est-à-dire sans transfert de données à caractère personnel à un responsable du traitement ou à un sous-traitant). Par conséquent, conformément à l'article 2, paragraphe 2, du RGPD, **ces applications ne relèvent pas du RGPD**.

75. Toutefois, si le RGPD ne s'applique pas au traitement de données à caractère personnel par une personne physique dans le cadre d'une activité purement personnelle ou domestique, il s'applique aux responsables du traitement ou aux sous-traitants, qui fournissent les moyens de traiter des données à caractère personnel pour l'exécution de telles activités personnelles ou domestiques (constructeurs automobiles, prestataires de services, etc.) conformément au considérant 18 du RGPD. Par conséquent, lorsque ces personnes agissent en tant que responsables du traitement ou sous-traitants, elles doivent mettre au point une application embarquée sécurisée et dans le respect du principe de protection de la vie privée dès la conception et par défaut. Dans tous les cas, conformément au considérant 78 du RGPD, «[l]*ors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui reposent sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leurs fonctions, il convient d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications et, compte dûment*

tenu de l'état des connaissances, à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données»[40]. D'une part, cela favorisera l'élaboration de services centrés sur l'utilisateur et, d'autre part, cela facilitera et garantira toute utilisation ultérieure susceptible de relever du RGPD. Plus précisément, l'EDPB recommande de mettre au point une plateforme d'application embarquée sécurisée, physiquement séparée des fonctions liées à la sécurité des véhicules, de sorte que l'accès aux données relatives aux véhicules ne dépende pas de capacités externes inutiles en nuage.

76. Les constructeurs automobiles et les prestataires de services devraient envisager le traitement local des données, dans la mesure du possible, afin d'atténuer les risques éventuels liés au traitement en nuage mis en évidence dans l'avis rendu par le groupe de travail «article 29» sur l'informatique en nuage[41].

77. De manière générale, les utilisateurs devraient pouvoir contrôler la manière dont leurs données sont collectées et traitées dans le véhicule:

- les informations relatives au traitement doivent être fournies dans la langue du conducteur (manuel, paramètres, etc.);
- l'EDPB recommande que seules les données strictement nécessaires au fonctionnement du véhicule soient traitées par défaut. Les personnes concernées devraient avoir la possibilité d'activer ou de désactiver le traitement des données pour chaque finalité et chaque responsable du traitement/sous-traitant et de supprimer les données concernées, en tenant compte de la finalité et de la base juridique du traitement des données;
- les données ne devraient pas être transmises à des tiers (ce qui signifie que seul l'utilisateur y a accès);
- les données ne devraient être conservées que pendant la durée nécessaire à la prestation du service ou pendant la durée prescrite par le droit de l'Union ou d'un État membre;
- les personnes concernées devraient pouvoir supprimer définitivement toute donnée à caractère personnel avant la mise en vente des véhicules;
- les personnes concernées devraient, dans la mesure du possible, pouvoir accéder directement aux données générées par ces applications.

78. Enfin, bien qu'il ne soit pas toujours possible de recourir au traitement local des données pour chaque cas d'utilisation, un «traitement hybride» peut souvent être mis en place. Par exemple, dans le contexte d'une assurance basée sur l'utilisation, les données à caractère personnel relatives au comportement au volant (comme la force exercée par le conducteur sur la pédale de frein, les kilomètres parcourus, etc.) pourraient être traitées à l'intérieur du véhicule ou par le prestataire de services télématiques pour le compte de la compagnie d'assurance (le responsable du traitement) dans le but de générer des scores numériques transmis à la compagnie d'assurance sur une base déterminée (tous les mois, par exemple). De cette façon, la compagnie d'assurance n'a pas accès aux données comportementales brutes, mais uniquement au score total obtenu à l'issue du traitement. Cette démarche permet de garantir le respect des principes de minimisation des données dès la conception. Cela signifie également que les utilisateurs doivent être en mesure d'exercer leurs droits lorsque des données sont stockées par d'autres parties: par exemple, un utilisateur devrait

[40] Pour des recommandations supplémentaires sur le respect de la vie privée dès la conception et par défaut, voir également les lignes directrices 4/2019.
[41] Groupe de travail «article 29» – avis 5/2012 sur l'informatique en nuage; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf.

pouvoir supprimer les données stockées dans les systèmes d'un atelier d'entretien automobile ou d'un concessionnaire dans les conditions prévues à l'article 17 du RGPD.

2.4.2 Anonymisation et pseudonymisation

79. Si la transmission de données à caractère personnel en dehors du véhicule est envisagée, il convient de prévoir l'anonymisation de ces données avant leur transmission. Lors de l'anonymisation des données, le responsable du traitement devrait tenir compte de tous les traitements concernés susceptibles de conduire à une réidentification des données, comme la transmission de données anonymisées au niveau local. L'EDPB rappelle que les principes relatifs à la protection des données ne s'appliquent pas aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée n'est pas ou n'est plus identifiable[42]. Dès qu'un ensemble de données est réellement anonymisé et que les personnes ne sont plus identifiables, la législation européenne en matière de protection des données ne s'applique plus. L'anonymisation peut donc, le cas échéant, constituer une bonne stratégie pour préserver les avantages et atténuer les risques liés aux véhicules connectés.

80. Comme le groupe de travail «article 29» l'explique en détail dans son avis sur les techniques d'anonymisation, différentes méthodes peuvent être utilisées – parfois en combinaison – pour parvenir à l'anonymisation de données[43].

81. D'autres techniques, comme la pseudonymisation[44], peuvent contribuer à réduire au minimum les risques générés par le traitement des données, étant donné que, dans la plupart des cas, il n'est pas nécessaire de disposer de données directement identifiables pour atteindre la finalité du traitement. Si elle est renforcée par des garanties de sécurité, la pseudonymisation permet d'améliorer la protection des données à caractère personnel en réduisant les risques d'abus. Contrairement à l'anonymisation, la pseudonymisation est réversible, et les données pseudonymisées sont considérées comme des données à caractère personnel soumises au RGPD.

2.4.3 Analyses d'impact relatives à la protection des données

82. Étant donné l'ampleur et la sensibilité des données à caractère personnel susceptibles d'être générées par des véhicules connectés, le traitement – en particulier le traitement de données à caractère personnel en dehors du véhicule – engendre souvent un risque élevé pour les droits et libertés des personnes. Si tel est le cas, les acteurs du secteur sont tenus d'effectuer une analyse d'impact relative à la protection des données (AIPD) afin d'identifier et d'atténuer les risques, conformément aux articles 35 et 36 du RGPD. Même lorsqu'une AIPD n'est pas requise, il est de bonne pratique d'en effectuer une dès que possible dans le processus de conception. Cela permet aux acteurs du secteur de tenir compte des résultats de cette analyse dans leurs choix de conception avant le déploiement de nouvelles technologies.

[42] Voir article 4, paragraphe 1, et considérant 26 du RGPD.
[43] Groupe de travail «article 29» sur les techniques d'anonymisation; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf.
[44] Article 4, paragraphe 5, du RGPD. Rapport de l'ENISA du 3 décembre 2019: https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.

2.5 Informations

83. Avant le traitement de ses données à caractère personnel, la personne concernée est informée de l'identité du responsable du traitement (par exemple, le constructeur de véhicules et d'équipements ou le prestataire de services), des finalités du traitement, des destinataires des données, de la durée de conservation des données et des droits des personnes concernées en vertu du RGPD[45].

84. En outre, le constructeur de véhicules et d'équipements, le prestataire de services ou tout autre responsable du traitement devrait également communiquer à la personne concernée les informations suivantes dans un langage clair, simple et facilement accessible:

- les coordonnées du délégué à la protection des données;
- les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement;
- la mention explicite des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, lorsqu'ils constituent la base juridique du traitement;
- le cas échéant, les destinataires ou les catégories de destinataires des données à caractère personnel;
- la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;
- l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données;
- l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci lorsque le traitement est fondé sur le consentement;
- le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale ainsi que les garanties utilisées pour les transférer;
- des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences possibles de la non-fourniture de ces données;
- l'existence d'une prise de décision automatisée, y compris un profilage, produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire, et des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée. Tel pourrait être le cas notamment en ce qui concerne la fourniture à des particuliers d'une assurance basée sur l'utilisation;
- le droit d'introduire une réclamation auprès d'une autorité de contrôle;
- des informations sur un traitement ultérieur;

[45] Article 5, paragraphe 1, point a), et article 13 du RGPD. Voir également groupe de travail «article 29», lignes directrices sur la transparence au sens du règlement (UE) 2016/679, (wp260rev.01), approuvées par l'EDPB.

- en cas de contrôle conjoint des données, des informations claires et complètes sur les responsabilités de chaque responsable du traitement.

85. Dans certains cas, les données à caractère personnel ne sont pas collectées directement auprès de la personne concernée. Par exemple, un constructeur de véhicules et d'équipements peut s'appuyer sur un concessionnaire pour recueillir des informations sur le propriétaire du véhicule afin de proposer un service d'assistance routière d'urgence. Lorsque les données ne sont pas collectées directement, le constructeur de véhicules et d'équipements, le prestataire de services ou tout autre responsable du traitement des données indique, en plus des informations susmentionnées, les catégories de données à caractère personnel concernées, la source dont proviennent les données à caractère personnel et, le cas échéant, si ces données proviennent de sources accessibles au public. Le responsable du traitement fournit ces informations dans un délai raisonnable après l'obtention des données, et **au plus tard à la première des dates suivantes**, conformément à l'article 14, paragraphe 3, du RGPD: i) un mois après l'obtention des données, eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées, ii) lors de la première communication avec la personne concernée, ou iii) si ces données sont communiquées à un tiers, avant leur transmission.

86. Il peut également s'avérer nécessaire de fournir de nouvelles informations aux personnes concernées lorsqu'elles sont prises en charge par un nouveau responsable du traitement. Un service d'assistance routière interagissant avec des véhicules connectés peut être fourni par différents responsables du traitement en fonction du pays ou de la région où l'assistance est demandée. Les nouveaux responsables du traitement devraient communiquer les informations requises aux personnes concernées lorsque celles-ci franchissent les frontières et que les services interagissant avec des véhicules connectés sont fournis par de nouveaux responsables du traitement.

87. Les informations destinées aux personnes concernées peuvent être fournies en plusieurs niveaux[46], c'est-à-dire en séparant deux niveaux d'information: d'une part, les informations de premier niveau, qui sont les plus importantes pour les personnes concernées et, d'autre part, les informations qui présentent vraisemblablement un intérêt à un stade ultérieur. Les informations essentielles de premier niveau comprennent, outre l'identité du responsable du traitement, les finalités du traitement et une description des droits de la personne concernée, ainsi que toute information complémentaire sur le traitement qui aura le plus de répercussions sur la personne concernée et sur un traitement qui pourrait la prendre au dépourvu. Dans le contexte des véhicules connectés, l'EDPB recommande que les personnes concernées soient informées de l'identité de tous les destinataires des informations de premier niveau. Comme le groupe de travail «article 29» l'a indiqué dans ses lignes directrices sur la transparence, les responsables du traitement doivent fournir aux personnes concernées les informations les plus significatives sur les destinataires. En pratique, il s'agit généralement de destinataires nommément désignés afin que les personnes concernées puissent savoir exactement qui détient leurs données à caractère personnel. Si les responsables du traitement ne sont pas en mesure de fournir les noms des destinataires, les informations devraient être les plus spécifiques possible et indiquer le type de destinataire (en fonction des activités qu'il mène), l'industrie, le secteur et le sous-secteur ainsi que l'emplacement des destinataires.

88. Les personnes concernées peuvent être informées au moyen de clauses concises et aisément compréhensibles figurant dans le contrat de vente du véhicule, le contrat de

[46] Voir groupe de travail «article 29», lignes directrices sur la transparence au sens du règlement 2016/679 (wp260rev.01), approuvées par l'EDPB.

prestation de services et/ou tout support écrit, de documents distincts (par exemple, le carnet d'entretien ou le manuel du véhicule) ou de l'ordinateur de bord.

89. Des icônes normalisées peuvent accompagner les informations nécessaires, conformément aux articles 13 et 14 du RGPD, afin de favoriser la transparence en réduisant potentiellement la nécessité de présenter de grandes quantités d'informations écrites à une personne concernée. Ces icônes doivent être visibles dans les véhicules afin d'offrir une bonne vue d'ensemble compréhensible et clairement lisible du traitement prévu. L'EDPB insiste sur l'importance de l'harmonisation de ces icônes, de façon à ce que l'utilisateur retrouve les mêmes symboles, quel que soit la marque ou le modèle du véhicule. Par exemple, lorsque certains types de données sont collectées, comme des données de localisation, les véhicules pourraient disposer d'un signal clair à bord (tel qu'un éclairage à l'intérieur du véhicule) pour informer les passagers de la collecte de données.

2.6 Droits de la personne concernée

90. Les constructeurs de véhicules et d'équipements, les prestataires de services et autres responsables du traitement devraient faciliter le contrôle que les personnes concernées exercent sur leurs données pendant toute la durée du traitement, par la mise en œuvre d'outils spécifiques permettant aux personnes concernées d'exercer efficacement leurs droits, notamment leur droit d'accès, de rectification et d'effacement, leur droit à la limitation du traitement et, en fonction de la base juridique du traitement, leur droit à la portabilité des données et leur droit d'opposition.

91. Pour faciliter la modification des paramètres, un système de gestion des profils devrait être mis en place afin de conserver les préférences des conducteurs connus et de les aider à modifier facilement et à tout moment leurs paramètres de confidentialité. Le système de gestion des profils devrait centraliser tous les paramètres de données pour chaque traitement de données, notamment pour faciliter l'accès, l'effacement, la suppression et la portabilité des données à caractère personnel des systèmes du véhicule à la demande de la personne concernée. Les conducteurs devraient être autorisés à interrompre la collecte de certains types de données, de manière temporaire ou définitive, à tout moment, à moins que le responsable du traitement puisse invoquer un motif juridique particulier pour poursuivre la collecte de données spécifiques. Dans le cas d'un contrat fournissant une offre personnalisée fondée sur le comportement au volant, cela peut vouloir dire que l'utilisateur doit par conséquent être renvoyé aux conditions standard du contrat. Ces dispositifs devraient être mis en œuvre à l'intérieur du véhicule, bien qu'ils puissent également être fournis aux personnes concernées par des moyens supplémentaires (une application spécifique, par exemple). En outre, afin de permettre aux personnes concernées de supprimer rapidement et facilement les données à caractère personnel susceptibles d'être conservées dans le tableau de bord du véhicule (par exemple, historique de navigation GPS, navigation sur internet, etc.), l'EDPB recommande aux constructeurs de prévoir une fonction simple (comme un bouton de suppression).

92. La vente d'un véhicule connecté et le changement de propriétaire qui s'ensuit devraient également entraîner la suppression des données à caractère personnel, qui ne sont plus nécessaires aux fins spécifiées précédemment, et la personne concernée devrait pouvoir exercer son droit à la portabilité.

2.7 Sécurité

93. Les constructeurs de véhicules et d'équipements, les prestataires de services et autres responsables du traitement devraient mettre en place des mesures permettant de garantir la sécurité et la confidentialité des données traitées et prendre toutes les précautions utiles pour en empêcher la prise de contrôle par une personne non autorisée. Les acteurs du secteur devraient notamment envisager d'adopter les mesures suivantes:

- chiffrer les canaux de communication à l'aide d'un algorithme de pointe;
- mettre en place une gestion des clés de chiffrement propre à chaque véhicule et non à chaque modèle;
- chiffrer les données stockées à distance au moyen d'algorithmes de pointe;
- renouveler régulièrement les clés de chiffrement;
- protéger les clés de chiffrement de toute divulgation;
- authentifier les appareils de réception de données;
- garantir l'intégrité des données (par hachage, par exemple);
- subordonner l'accès aux données à caractère personnel à des techniques fiables d'authentification de l'utilisateur (mot de passe, certificat électronique, etc.);

94. En ce qui concerne plus particulièrement les constructeurs de véhicules, l'EDPB recommande la mise en œuvre des mesures de sécurité suivantes:

- cloisonner les fonctions vitales du véhicule par rapport à celles qui dépendent en permanence des capacités de télécommunication («infodivertissement», par exemple);
- mettre en œuvre des mesures techniques permettant aux constructeurs de véhicules de corriger rapidement les failles de sécurité pendant toute la durée de vie du véhicule;
- pour les fonctions vitales du véhicule, privilégier, autant que possible, le recours à des moyens de communication sécurisés spécifiquement dédiés aux transports;
- mettre en place un système d'alarme en cas d'attaque contre les systèmes du véhicule, avec la possibilité d'un fonctionnement en mode dégradé[47];
- conserver l'historique du journal d'accès au système d'information du véhicule, par exemple sur une durée de six mois au maximum, afin de comprendre l'origine d'une attaque éventuelle et de procéder à un examen périodique des informations enregistrées pour détecter d'éventuelles anomalies.

95. Il convient d'assortir ces recommandations générales d'exigences spécifiques tenant compte des caractéristiques et des finalités de chaque traitement de données.

2.8 Transmission de données à caractère personnel à des tiers

96. En principe, seuls le responsable du traitement et la personne concernée ont accès aux données générées par un véhicule connecté. Le responsable du traitement peut toutefois transmettre des données à caractère personnel à un partenaire commercial (destinataire), dans la mesure où cette transmission repose légalement sur l'une des bases juridiques énoncées à l'article 6 du RGPD.

97. Au regard de la sensibilité que peuvent présenter les données d'usage du véhicule (par exemple, les trajets effectués, le style de conduite), l'EDPB recommande de recueillir systématiquement le consentement de la personne concernée avant toute transmission de ses données à un partenaire commercial (par exemple, au moyen d'une case à cocher qui n'est pas cochée préalablement ou, lorsque c'est techniquement possible, par l'intermédiaire d'un dispositif physique ou logique auquel la personne peut accéder depuis

[47] Le mode dégradé est un mode de fonctionnement du véhicule qui permet de garantir les fonctions essentielles pour assurer la sécurité du fonctionnement du véhicule (c'est-à-dire les exigences minimales de sécurité), même en cas de désactivation d'autres fonctions moins importantes (par exemple, le fonctionnement du dispositif de guidage géographique peut être considéré comme non essentiel, contrairement au système de freinage).

le véhicule). Le partenaire commercial devient à son tour responsable des données qui lui sont transmises et est soumis à l'intégralité des dispositions du RGPD.

98. Le constructeur de véhicules, le prestataire de services ou tout autre responsable du traitement peut transmettre des données à caractère personnel à un sous-traitant sélectionné pour participer à la fourniture du service à la personne concernée, à condition que le sous-traitant n'utilise pas ces données pour ses propres besoins. Les responsables du traitement et les sous-traitants établissent un contrat ou tout autre document juridique précisant les obligations de chaque partie et énonçant les dispositions de l'article 28 du RGPD.

2.9 Transfert de données à caractère personnel en dehors de l'UE/EEE

99. Lorsque des données à caractère personnel sont transférées en dehors de l'Espace économique européen, des garanties spéciales sont prévues pour que ces données continuent de bénéficier du même niveau de protection.

100. Le responsable du traitement ne peut donc transférer des données à caractère personnel à un destinataire que si ce transfert est conforme aux conditions prévues au chapitre V du RGPD.

2.10 Utilisation de technologies Wi-Fi embarquées

101. Grâce aux progrès de la technologie cellulaire, on peut désormais utiliser facilement l'internet sur la route. S'il est possible d'obtenir une connectivité Wi-Fi dans un véhicule par l'intermédiaire d'un point d'accès fourni par un téléphone intelligent ou d'un dispositif dédié à cet effet (dongle OBD-II, modem ou routeur sans fil, etc.), la plupart des constructeurs proposent actuellement des modèles équipés d'une connexion de données cellulaires intégrée et également capables de créer des réseaux Wi-Fi. Selon les cas, différents aspects doivent être pris en considération:

- la connectivité Wi-Fi est proposée en tant que service par un professionnel de la route, comme un chauffeur de taxi pour ses clients. Dans ce cas, le professionnel ou son entreprise peut être considéré comme un fournisseur de service internet (FSI) et donc être soumis à des obligations et restrictions particulières en ce qui concerne le traitement des données à caractère personnel de ses clients;

- la connectivité Wi-Fi est mise en place pour le seul usage du conducteur (à l'exclusion de ses passagers). Dans ce cas, le traitement des données à caractère personnel est considéré comme une activité purement personnelle ou domestique conformément à l'article 2, paragraphe 2, point c), du RGPD et à son considérant 18.

102. De manière générale, la prolifération des interfaces de connexion internet via Wi-Fi présente des risques plus importants pour la vie privée des personnes. En effet, les utilisateurs deviennent, par l'intermédiaire de leurs véhicules, des diffuseurs continus et peuvent donc être identifiés et faire l'objet d'un suivi. Afin d'empêcher tout suivi, les constructeurs de véhicules et d'équipements devraient donc prévoir des options de refus simples à utiliser pour que l'identifiant de l'ensemble de services (SSID) du réseau Wi-Fi embarqué ne soit pas collecté.

3 ÉTUDES DE CAS

103. La présente section donne cinq exemples concrets de traitement dans le contexte des véhicules connectés, qui correspondent à des scénarios que les parties prenantes du secteur sont susceptibles de rencontrer. Ces exemples concernent un traitement de données qui nécessite une puissance de calcul ne pouvant être mobilisée localement dans le véhicule et/ou l'envoi de données à caractère personnel à un tiers pour effectuer une analyse plus approfondie ou fournir d'autres fonctions à distance. Pour chaque type de traitement, le présent document précise les finalités prévues, les catégories de données collectées, la durée de conservation de ces données, les droits des personnes concernées, les mesures de sécurité à mettre en place et les destinataires des informations. Si certains de ces domaines ne sont pas décrits ci-après, les recommandations générales données dans la partie précédente s'appliquent.

104. Les exemples choisis ne sont pas exhaustifs et sont censés refléter la diversité de types de traitement, de bases juridiques, d'acteurs, etc. susceptibles d'intervenir dans le contexte des véhicules connectés.

3.1 Prestation de services par des tiers

105. Les personnes concernées peuvent signer un contrat avec un prestataire de services afin d'obtenir des services à valeur ajoutée liés à leur véhicule. Par exemple, une personne concernée peut conclure un contrat d'assurance basée sur l'utilisation qui prévoit des primes d'assurance réduites en cas de conduite limitée (assurance au kilomètre) ou prudente (assurance selon la conduite) et qui nécessite, de la part de la société d'assurance, la surveillance des habitudes de conduite. Une personne concernée peut également signer un contrat avec une société d'assistance routière en cas de panne, qui implique la

transmission de la position du véhicule à la société, ou avec un prestataire de services afin de recevoir des messages ou des alertes en ce qui concerne le fonctionnement du véhicule (par exemple, une alerte relative à l'état d'usure d'un frein ou un rappel de la date du contrôle technique).

3.1.1 Assurance basée sur l'utilisation

106. L'assurance au kilomètre est un type d'assurance basée sur l'utilisation qui permet d'enregistrer les kilomètres parcourus par le conducteur et/ou ses habitudes de conduite afin de distinguer et de récompenser les conducteurs «prudents» en leur offrant des tarifs plus intéressants. L'assureur demande au conducteur d'installer un service télématique intégré ou une application mobile ou d'activer un module intégré dès la fabrication qui permet d'enregistrer les kilomètres parcourus et/ou le comportement de conduite (type de freinage, accélération rapide, etc.) du preneur d'assurance. Les informations recueillies par l'appareil télématique sont utilisées pour attribuer des scores au conducteur afin d'analyser les risques qu'il est susceptible de présenter pour la société d'assurance.

107. Étant donné qu'une assurance fondée sur l'utilisation nécessite un consentement en vertu de l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques», l'EDPB insiste sur le fait que le preneur d'assurance doit pouvoir choisir de souscrire une police d'assurance qui n'est pas fondée sur l'utilisation. Dans le cas contraire, le consentement ne serait pas considéré comme ayant été donné librement, puisque l'exécution du contrat serait subordonnée au consentement. De plus, en vertu de l'article 7, paragraphe 3, du RGPD, une personne concernée doit avoir le droit de retirer son consentement.

3.1.1.1 Base juridique

108. Lorsque les données sont recueillies par l'intermédiaire d'un service de communication électronique accessible au public (par exemple au moyen d'une carte SIM présente dans l'appareil télématique), le consentement est nécessaire pour accéder aux informations déjà stockées dans le véhicule, comme prévu à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques». En effet, aucune des dérogations prévues dans ces dispositions ne peut s'appliquer dans ce contexte: le traitement ne vise pas exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques et ne concerne pas un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur. Le consentement peut être recueilli lors de la conclusion du contrat.

109. En ce qui concerne le traitement de données à caractère personnel à la suite du stockage ou de l'accès à l'équipement terminal de l'utilisateur final, la société d'assurance peut s'appuyer sur l'article 6, paragraphe 1, point b), du RGPD dans ce contexte spécifique, à condition qu'elle puisse prouver que le traitement s'inscrit dans le cadre d'un contrat valable avec la personne concernée et que le traitement est nécessaire à l'exécution dudit contrat avec la personne concernée. Dans la mesure où le traitement est objectivement nécessaire à l'exécution du contrat signé avec la personne concernée, l'EDPB estime que le recours à l'article 6, paragraphe 1, point b), du RGPD n'aurait pas pour effet d'affaiblir la protection supplémentaire prévue à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» dans ce cas précis. La signature, par la personne concernée, d'un contrat avec la société d'assurance matérialise la base juridique.

3.1.1.2 Donnes collectées

110. Deux types de données à caractère personnel sont à prendre en considération:

- les **données commerciales et relatives aux transactions**: données d'identification de la personne concernée, données relatives aux transactions, données relatives aux moyens de paiement, etc.;

- les **données d'usage**: données à caractère personnel générées par le véhicule, habitudes de conduite, localisation, etc.

111. L'EDPB recommande que, dans la mesure du possible, et compte tenu du risque que les données collectées au moyen du boîtier télématique puissent être exploitées de manière abusive pour créer un profil précis des déplacements du conducteur, les données brutes relatives au comportement de conduite soient traitées:

- à bord du véhicule, dans des boîtiers télématiques ou dans le téléphone intelligent de l'utilisateur, afin que l'assureur n'accède qu'aux seules données de résultats (par exemple, un score correspondant aux habitudes de conduite) et non aux données brutes détaillées (voir section 2.1);

- ou par le prestataire de services télématiques pour le compte du responsable du traitement (la société d'assurance) pour générer des scores numériques transférés à la société d'assurance sur une base définie. Dans ce cas, les données brutes doivent être séparées des données directement liées à l'identité du conducteur. Ainsi, le prestataire de services télématiques reçoit les données en temps réel, sans connaître les noms, les plaques d'immatriculation, etc. des preneurs d'assurance, tandis que l'assureur connaît les noms des preneurs d'assurance, mais ne reçoit que les scores et le nombre total de kilomètres et non les données brutes utilisées pour générer ces scores.

112. Il convient par ailleurs de préciser que si seul le kilométrage est nécessaire à l'exécution du contrat, les données de localisation ne sont pas collectées.

3.1.1.3 Durée de conservation

113. En cas de traitement nécessaire à l'exécution d'un contrat (c'est-à-dire à la prestation d'un service), il est important de distinguer deux types de données avant de déterminer leurs durées de conservation respectives:

- **les données commerciales et relatives aux transactions:** ces données peuvent être conservées en base active pendant toute la durée du contrat. À l'issue du contrat, elles peuvent faire l'objet d'un archivage physique (sur support distinct: DVD, etc.) ou logique (par gestion des habilitations) en cas de litige éventuel. Ensuite, au terme de la durée de prescription légale, les données sont supprimées ou anonymisées;

- **les données d'usage:** ces données peuvent être classées comme données brutes et comme données agrégées. Comme indiqué ci-dessus, les responsables du traitement ou les sous-traitants ne devraient pas, dans la mesure du possible, traiter les données brutes. Le cas échéant, les données brutes ne devraient être conservées que le temps nécessaire pour élaborer les données agrégées et vérifier la validité de ce processus d'agrégation. Les données agrégées ne devraient être conservées que pendant la durée nécessaire à la prestation du service ou pendant la durée prescrite par le droit de l'Union ou d'un État membre.

3.1.1.4 Information et droits des personnes concernées

114. Avant le traitement de ses données à caractère personnel, la personne concernée est informée conformément à l'article 13 du RGPD, de manière transparente et compréhensible. Elle est notamment informée de la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, des critères utilisés pour déterminer cette durée. Dans ce dernier cas, l'EDPB préconise d'adopter une approche pédagogique pour mettre en évidence la différence entre les données brutes et le score obtenu sur cette base, en soulignant, lorsque c'est le cas, que l'assureur ne collectera que le résultat du score le cas échéant.

115. Lorsque des données ne sont pas traitées à bord du véhicule, mais par un prestataire de services télématiques pour le compte du responsable du traitement (la société d'assurance), les informations pourraient utilement mentionner que, dans ce cas, le prestataire n'aura pas

accès aux données directement liées à l'identité du conducteur (nom, plaque d'immatriculation, etc.). En outre, compte tenu de l'importance d'informer les personnes concernées des conséquences du traitement de leurs données à caractère personnel et du fait que les personnes concernées ne devraient pas être prises au dépourvu par le traitement de leurs données à caractère personnel, l'EDPB recommande que les personnes concernées soient informées de l'existence d'un profilage et de ses conséquences, même s'il n'entraîne aucune prise de décision automatisée au sens de l'article 22 du RGPD.

116. En ce qui concerne leurs droits, les personnes concernées sont spécifiquement informées des moyens dont elles disposent pour exercer leur droit d'accès, de rectification, de limitation et d'effacement. Étant donné que les données brutes collectées dans ce contexte sont fournies par la personne concernée (au moyen de formulaires spécifiques ou par l'intermédiaire de son activité) et traitées sur la base de l'article 6, paragraphe 1, point b), du RGPD (exécution d'un contrat), la personne concernée est habilitée à exercer son droit à la portabilité des données. Ainsi qu'il est souligné dans les lignes directrices sur le droit à la portabilité des données, l'EDPB recommande vivement «que les responsables du traitement expliquent clairement la différence entre les types de données qu'une personne peut recevoir en exerçant son droit d'accès et son droit à la portabilité»[48].

117. Ces informations peuvent être fournies à la signature du contrat.

3.1.1.5 Destinataire

118. L'EDPB recommande que, dans la mesure du possible, les données d'usage du véhicule soient traitées directement dans les boîtiers télématiques, afin que l'assureur n'accède qu'aux seules données de résultats (par exemple, un score) et non aux données brutes détaillées.

119. Si un prestataire de services télématiques collecte les données pour le compte du responsable du traitement (la compagnie d'assurance) afin de générer des scores numériques, il n'a pas besoin de connaître l'identité du conducteur (nom, plaque d'immatriculation, etc.) des preneurs d'assurance.

3.1.1.6 Sécurité

120. Les recommandations générales s'appliquent. Voir section 2.7.

3.1.2 Location et réservation d'un emplacement de stationnement

121. Le propriétaire d'un emplacement de stationnement peut vouloir le louer. Pour ce faire, il inscrit son emplacement sur une liste et fixe le prix correspondant sur une application web. Ensuite, une fois que l'emplacement de stationnement figure sur la liste, l'application informe le propriétaire lorsqu'un conducteur souhaite le réserver. Le conducteur peut choisir une destination et vérifier les emplacements de stationnement disponibles sur la base de plusieurs critères. Après l'approbation du propriétaire, la transaction est confirmée et le prestataire de services traite le paiement. Le conducteur se sert ensuite de la navigation pour se rendre jusqu'à l'emplacement.

3.1.2.1 Base juridique

122. Lorsque les données sont recueillies par l'intermédiaire d'un service de communication électronique accessible au public, l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» s'applique.

123. Comme il s'agit d'un service de la société de l'information, l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» n'exige pas l'obtention du

[48] Groupe de travail «article 29», lignes directrices relatives au droit à la portabilité des données, WP242 rev.01, approuvées par l'EDPB, p. 16.

consentement pour avoir accès aux informations déjà stockées dans le véhicule lorsque l'abonné fait explicitement la demande d'un tel service.

124. En ce qui concerne le traitement des données à caractère personnel et uniquement pour les données nécessaires à l'exécution du contrat auquel la personne concernée est partie, l'article 6, paragraphe 1, point b), du RGPD constitue la base juridique.

3.1.2.2 Donnes collectées

125. Parmi les données traitées figurent les coordonnées du conducteur (nom, adresse électronique, numéro de téléphone), le type de véhicule (par exemple, voiture, camion, motocycle), le numéro de la plaque d'immatriculation, la durée de stationnement, les données de paiement (par exemple, informations sur la carte de crédit), ainsi que les données de navigation.

3.1.2.3 Durée de conservation

126. Les données ne devraient être conservées que pendant la durée nécessaire à l'exécution du contrat de stationnement ou pendant la durée prescrite par le droit de l'Union ou d'un État membre. Après quoi, les données sont anonymisées ou supprimées.

3.1.2.4 Information et droits des personnes concernées

127. Avant le traitement de ses données à caractère personnel, la personne concernée devrait être informée conformément à l'article 13 du RGPD, de manière transparente et compréhensible.

128. La personne concernée devrait être spécifiquement informée des moyens dont elle dispose pour exercer son droit d'accès, de rectification, de limitation et d'effacement. Étant donné que les données collectées dans ce contexte sont fournies par la personne concernée (au moyen de formulaires spécifiques ou par l'intermédiaire de son activité) et traitées sur la base de l'article 6, paragraphe 1, point b), du RGPD (exécution d'un contrat), la personne concernée est habilitée à exercer son droit à la portabilité des données. Ainsi qu'il est souligné dans les lignes directrices sur le droit à la portabilité des données, l'EDPB recommande vivement «*que les responsables du traitement expliquent clairement la différence entre les types de données qu'une personne peut recevoir en exerçant son droit d'accès et son droit à la portabilité*».

3.1.2.5 Destinataire

129. En principe, seuls le responsable du traitement et le sous-traitant ont accès aux données.

3.1.2.6 Sécurité

130. Les recommandations générales s'appliquent. Voir section 2.7.

3.2 eCall

131. En cas d'accident grave sur le territoire de l'Union européenne, le véhicule déclenche automatiquement un appel eCall vers le 112, numéro d'appel d'urgence européen (voir section 1.1 pour plus de détails) qui permet d'envoyer rapidement une ambulance sur les lieux de l'accident conformément au règlement (UE) 2015/758 du 29 avril 2015 concernant les exigences en matière de réception par type pour le déploiement du système eCall embarqué fondé sur le service 112 et modifiant la directive 2007/46/CE [ci-après le «règlement (UE) 2015/758»].

132. En effet, le générateur eCall installé à l'intérieur du véhicule, qui permet la transmission par l'intermédiaire d'un réseau public de communications mobiles, envoie un appel d'urgence, qui est déclenché automatiquement grâce aux capteurs du véhicule ou manuellement par les occupants du véhicule uniquement en cas d'accident. Outre l'activation de la communication audio, en cas d'accident, un ensemble minimal de données (MSD) est automatiquement généré et envoyé au centre de réception des appels d'urgence (PSAP).

3.2.1 Base juridique

133. S'agissant de l'application de la directive «vie privée et communications électroniques», deux dispositions doivent être prises en considération:

- l'article 9 concernant les données de localisation autres que les données relatives au trafic qui ne s'applique qu'aux services de communications électroniques;
- l'article 5, paragraphe 3, en ce qui concerne l'accès aux informations stockées dans le générateur installé à l'intérieur du véhicule.

134. Bien que ces dispositions exigent en principe le consentement de la personne concernée, le règlement (UE) 2015/758 constitue une obligation légale à laquelle le responsable du traitement est soumis (la personne concernée n'a pas de choix véritable ou libre et ne pourra pas refuser le traitement de ses données). Dès lors, le règlement (UE) 2015/758 prévaut sur la nécessité d'obtenir le consentement du conducteur pour le traitement des données de localisation et du MSD[49].

135. La base juridique du traitement de ces données sera le respect d'une obligation légale prévue à l'article 6, paragraphe 1, point c), du RGPD [à savoir le règlement (UE) 2015/758].

3.2.2 Donnes collectées

136. Le règlement (UE) 2015/578 dispose que les données transmises par le système eCall embarqué fondé sur le numéro 112 comprennent uniquement les informations minimales visées dans la norme EN 15722:2015 «Systèmes de transport intelligents – eSafety – Ensemble minimal de données pour l'eCall (MSD)», notamment:

- l'indication du déclenchement manuel ou automatique du système eCall;
- le type de véhicule;
- le numéro d'identification du véhicule (VIN);
- le type de propulsion du véhicule;
- l'horodatage de la création du message de données initial dans le cadre de l'incident eCall en cours;
- la dernière position connue du véhicule (latitude et longitude), déterminée au dernier moment possible avant la création du message;
- la dernière direction connue suivie par le véhicule, déterminée au dernier moment possible avant la création du message (uniquement les trois dernières positions du véhicule).

3.2.3 Durée de conservation

137. Le règlement (UE) 2015/758 dispose que les données ne sont pas conservées plus longtemps qu'il n'est nécessaire aux fins du traitement des situations d'urgence. Ces données sont totalement effacées lorsqu'elles ne sont plus nécessaires à cette fin. En outre, dans la mémoire interne du système eCall, les données sont automatiquement et constamment effacées. Seules les trois dernières positions du véhicule peuvent être

[49] Il convient de préciser que l'article 8, paragraphe 1, point f), du mandat de négociation du Conseil relatif au projet de règlement «vie privée et communications électroniques» prévoit une dérogation spécifique pour le service eCall, le consentement n'étant pas nécessaire lorsqu'«*il est nécessaire de localiser des équipements terminaux quand un utilisateur final effectue une communication d'urgence soit vers le numéro d'urgence unique européen "112" soit vers un numéro d'urgence national, conformément à l'article 13, paragraphe 3*».

conservées dans la mesure où cela est strictement nécessaire pour préciser la position actuelle du véhicule et la direction suivie au moment de l'événement.

3.2.4 Information et droits des personnes concernées

138. L'article 6 du règlement (UE) 2015/758 dispose que les constructeurs fournissent des informations claires et complètes sur le traitement des données effectué par l'intermédiaire du système eCall. Les informations relatives au système eCall embarqué fondé sur le numéro 112 sont fournies dans le manuel du propriétaire séparément de celles relatives aux éventuels systèmes eCall pris en charge par des services tiers, et ce avant que le système ne soit utilisé. Il s'agit notamment des informations suivantes:

- la référence à la base juridique du traitement;
- le fait que le système eCall embarqué fondé sur le numéro 112 est activé par défaut;
- les modalités du traitement des données effectué par le système eCall embarqué fondé sur le numéro 112;
- le but spécifique du traitement eCall, qui est limité aux situations d'urgence visées à l'article 5, paragraphe 2, premier alinéa, du règlement (UE) 2015/758;
- les types de données collectées et traitées, ainsi que les destinataires de ces données;
- le délai de conservation des données dans le système eCall embarqué fondé sur le numéro 112;
- le fait qu'il n'y a pas de surveillance constante du véhicule;
- les modalités d'exercice des droits des personnes concernées, ainsi que le service de contact compétent pour le traitement des demandes d'accès;
- toute information complémentaire nécessaire pour ce qui est de la traçabilité, de la surveillance et du traitement des données à caractère personnel en rapport avec la fourniture d'un système eCall pris en charge par des services tiers (TPS) et/ou d'autres services à valeur ajoutée, laquelle est soumise à l'accord explicite du propriétaire et est conforme au RGPD. Une attention particulière est accordée au fait que des différences peuvent exister entre le traitement des données effectué par le système eCall embarqué fondé sur le numéro 112 et les systèmes de TPS eCall embarqués ou d'autres services à valeur ajoutée.

139. Par ailleurs, le prestataire de services fournit également des informations aux personnes concernées conformément à l'article 13 du RGPD, de manière transparente et compréhensible. En particulier, la personne concernée doit être informée des finalités du traitement auquel les données à caractère personnel sont destinées ainsi que du fait que le traitement des données à caractère personnel est fondé sur une obligation légale à laquelle le responsable du traitement est soumis.

140. De plus, compte tenu de la nature du traitement, les informations relatives aux destinataires ou catégories de destinataires des données à caractère personnel devraient être claires et les personnes concernées devraient être informées que les données ne peuvent être accessibles en dehors du système eCall embarqué fondé sur le numéro 112 à aucune entité avant le déclenchement de l'appel eCall.

141. En ce qui concerne les droits des personnes concernées, il convient de préciser que, comme le traitement est fondé sur une obligation légale, le droit d'opposition et le droit à la portabilité ne s'appliquent pas.

3.2.5 Destinataire

142. Les données ne peuvent être accessibles en dehors du système eCall embarqué fondé sur le numéro 112 à aucune entité avant le déclenchement de l'appel eCall.

143. Lorsqu'il est déclenché (manuellement par les occupants du véhicule ou automatiquement dès qu'un détecteur embarqué détecte une collision grave), le système eCall établit une connexion vocale avec le PSAP concerné et le MSD est transmis à l'opérateur du PSAP.

144. En outre, les données transmises via le système eCall embarqué fondé sur le numéro 112 et traitées par les PSAP peuvent être transmises au service d'urgence et aux partenaires de service visés dans la décision nº 585/2014/UE uniquement en cas d'incidents en relation avec des appels eCall et dans les conditions énoncées dans ladite décision, et sont utilisées exclusivement aux fins des objectifs de ladite décision. Les données traitées par les PSAP via le système eCall embarqué fondé sur le numéro 112 ne sont pas transmises à d'autres tiers sans l'accord explicite de la personne concernée.

3.2.6 Sécurité

145. Le règlement (UE) 2015/758 énonce les exigences relatives à l'intégration, dans le système eCall, de technologies renforçant la protection de la vie privée, afin d'offrir aux utilisateurs un niveau de protection de la vie privée approprié, ainsi que les garanties nécessaires pour prévenir la surveillance et les utilisations abusives. De plus, les constructeurs veillent à ce que le système eCall embarqué fondé sur le numéro 112 et tout autre système fournissant un eCall pris en charge par des services tiers ou un service à valeur ajoutée soient conçus de telle sorte que l'échange de données à caractère personnel entre ces systèmes soit impossible.

146. En ce qui concerne les PSAP, les États membres veillent à ce que les données à caractère personnel soient protégées contre toute utilisation abusive, notamment les accès non autorisés, les modifications ou les pertes et à ce que des protocoles concernant le stockage des données à caractère personnel, la durée de leur conservation, leur traitement et leur protection soient établis au niveau approprié et dûment appliqués.

3.3 Études d'accidentologie

147. Les personnes concernées peuvent accepter, sur la base du volontariat, de participer à des études d'accidentologie visant à mieux comprendre les causes des accidents de la route et menées, plus généralement, à des fins scientifiques.

3.3.1 Base juridique

148. Lorsque les données sont recueillies par l'intermédiaire d'un service de communication électronique accessible au public, le responsable du traitement doit obtenir le consentement de la personne concernée pour avoir accès aux informations qui sont déjà stockées dans le véhicule, conformément à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques». En effet, aucune des dérogations prévues dans ces dispositions ne peut s'appliquer dans ce contexte: le traitement ne vise pas exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques et ne concerne pas un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur.

149. En ce qui concerne le traitement des données à caractère personnel, et compte tenu de la variété et de la quantité de données à caractère personnel nécessaires aux études d'accidentologie, l'EDPB recommande que le traitement soit fondé sur le consentement préalable de la personne concernée conformément à l'article 6 du RGPD. Ce consentement préalable doit être communiqué dans un formulaire spécifique, au moyen duquel la personne concernée se porte volontaire pour participer à l'étude et accepte que ses données à caractère personnel soient traitées à cette fin. Le consentement est la manifestation de la volonté libre, spécifique et éclairée de la personne dont les données sont traitées (par exemple, en cochant une case qui ne l'est pas préalablement ou en configurant l'ordinateur de bord pour activer une fonction dans le véhicule). Ce consentement doit être fourni séparément, à des fins spécifiques. Il ne peut être associé au

contrat d'achat ou de location à bail d'une voiture neuve et doit pouvoir être aussi facilement retiré qu'il est donné. Le retrait du consentement entraîne l'interruption du traitement. Les données sont ensuite effacées de la base de données active ou anonymisées.

150. Le consentement requis en vertu de l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» et le consentement nécessaire comme base juridique pour le traitement de données peuvent être obtenus simultanément (par exemple, en cochant une case indiquant clairement ce à quoi la personne concernée consent).

151. Il convient de préciser qu'en fonction des conditions du traitement (nature du responsable du traitement, etc.), une autre base juridique peut être légalement choisie pour autant qu'elle n'affaiblit pas la protection supplémentaire prévue à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» (voir point 15). Si le traitement repose sur une autre base juridique, comme l'exécution d'une mission d'intérêt public [article 6, paragraphe 1, point e), du RGPD], l'EDPB recommande que les personnes concernées participent à l'étude à titre volontaire.

3.3.2 Donnes collectées

152. Le responsable du traitement collecte uniquement les données à caractère personnel strictement nécessaires au traitement.

153. Deux types de données sont à prendre en considération:

- **les données relatives aux participants et aux véhicules**;
- **les données techniques issues des véhicules** (vitesse instantanée, etc.).

154. Les recherches scientifiques liées à l'accidentologie justifient la collecte de la vitesse instantanée, y compris par des personnes morales ne gérant pas de service public au sens strict.

155. En effet, comme indiqué ci-dessus, l'EDPB considère que la vitesse instantanée collectée dans le cadre d'une étude d'accidentologie ne constitue pas une donnée d'infraction par destination (et qu'elle n'est donc pas collectée dans le cadre d'une enquête ou de poursuites relatives à une infraction), ce qui justifie sa collecte par des personnes morales ne gérant pas de service public au sens strict.

3.3.3 Durée de conservation

156. Il est important de faire la distinction entre deux types de données. Premièrement, les données relatives aux participants et aux véhicules peuvent être conservées pendant la durée de l'étude. Deuxièmement, les données techniques issues des véhicules devraient être conservées le moins de temps possible à cette fin. À cet égard, un délai de cinq ans à compter de la date de fin de l'étude semble être une durée raisonnable. À l'issue de cette durée, les données sont supprimées ou anonymisées.

3.3.4 Information et droits des personnes concernées

157. Avant le traitement de ses données à caractère personnel, la personne concernée est informée conformément à l'article 13 du RGPD, de manière transparente et compréhensible. En particulier, en ce qui concerne la collecte de la vitesse instantanée, les personnes concernées devraient être spécifiquement informées de la collecte des données. Lorsque le traitement des données est fondé sur le consentement, la personne concernée doit être spécifiquement informée de l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci. En outre, les données collectées dans ce contexte étant fournies par la personne concernée (au moyen de formulaires spécifiques ou par l'intermédiaire de son activité) et traitées sur la base de l'article 6, paragraphe 1, point a), du RGPD (consentement), la personne concernée est habilitée à exercer son droit à la

portabilité des données. Ainsi qu'il est souligné dans les lignes directrices sur le droit à la portabilité des données, l'EDPB recommande vivement «que les responsables du traitement expliquent clairement la différence entre les types de données qu'une personne peut recevoir en exerçant son droit d'accès et son droit à la portabilité». Le responsable du traitement devrait donc prévoir un moyen facile de retirer son consentement, librement et à tout moment, et mettre au point des outils permettant de répondre aux demandes de portabilité des données.

158. Ces informations peuvent être fournies à la signature du formulaire de participation à l'étude d'accidentologie.

3.3.5 Destinataire

159. En principe, seuls le responsable du traitement et le sous-traitant ont accès aux données.

3.3.6 Sécurité

160. Comme indiqué ci-dessus, les mesures de sécurité mises en place doivent être adaptées au niveau de sensibilité des données. Ainsi, en cas de collecte de la vitesse instantanée (ou de toute autre donnée liée à des condamnations pénales ou des infractions) dans le cadre d'une étude d'accidentologie, l'EDPB recommande la mise en place de mesures de sécurité fortes, telles que:

- la mise en œuvre de mesures de pseudonymisation (par exemple, le hachage avec clé secrète des données telles que le nom/prénom de la personne concernée et le numéro de série);
- le stockage des données relatives à la vitesse instantanée et à la localisation dans des bases de données distinctes (par exemple, au moyen d'un mécanisme de chiffrement de pointe avec des clés distinctes et des mécanismes d'approbation); et/ou
- la suppression des données de localisation dès la qualification de l'événement ou de la séquence de référence (par exemple, le type de route, jour/nuit) et la conservation des données permettant une identification directe dans une base distincte, à laquelle ne peuvent accéder qu'un nombre restreint de personnes.

3.4 Lutte contre le vol de véhicules

161. En cas de vol, les personnes concernées peuvent tenter de retrouver leur véhicule à l'aide de la localisation. L'utilisation des données de localisation est limitée aux stricts besoins de l'enquête et à l'instruction du dossier par les autorités judiciaires compétentes.

3.4.1 Base juridique

162. Lorsque les données sont recueillies par l'intermédiaire d'un service de communication électronique accessible au public, l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» s'applique.

163. Comme il s'agit d'un service de la société de l'information, l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» n'exige pas l'obtention du consentement pour avoir accès aux informations déjà stockées dans le véhicule lorsque l'abonné fait explicitement la demande d'un tel service.

164. En ce qui concerne le traitement des données à caractère personnel, la base juridique du traitement des données de localisation est le consentement du propriétaire du véhicule ou, le cas échéant, l'exécution d'un contrat (uniquement pour les données nécessaires à l'exécution du contrat auquel le propriétaire du véhicule est partie).

165. Le consentement est la manifestation de la volonté libre, spécifique et éclairée de la personne dont les données sont traitées (par exemple, en cochant une case qui ne l'est pas préalablement ou en configurant l'ordinateur de bord pour activer une fonction dans le véhicule). La liberté de donner son consentement consiste notamment à pouvoir le retirer

à tout moment, ce dont la personne concernée doit être expressément informée. Le retrait du consentement entraîne l'interruption du traitement. Il convient ensuite d'effacer les données, de les anonymiser ou de les archiver.

3.4.2 Donnes collectées

166. Les données de localisation ne peuvent être transmises qu'à partir de la déclaration de vol et ne sauraient être collectées en continu le reste du temps.

3.4.3 Durée de conservation

167. Les données de localisation ne peuvent être conservées que le temps de l'instruction du dossier par les autorités judiciaires compétentes ou jusqu'à l'issue d'une procédure de levée de doute n'aboutissant pas à la confirmation du vol du véhicule.

3.4.4 Information des personnes concernées

168. Avant le traitement de ses données à caractère personnel, la personne concernée devrait être informée conformément à l'article 13 du RGPD, de manière transparente et compréhensible. Plus précisément, l'EDPB recommande au responsable du traitement d'insister sur le fait que le véhicule ne fait pas l'objet d'un suivi constant et que les données de localisation ne peuvent être collectées et transmises qu'à partir de la déclaration de vol. En outre, le responsable du traitement doit fournir à la personne concernée les informations relatives au fait que seuls les agents habilités de la plateforme de télésurveillance et les autorités légalement habilitées ont accès aux données.

169. En ce qui concerne les droits des personnes concernées, lorsque le traitement des données est fondé sur le consentement, la personne concernée devrait être spécifiquement informée de l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci. De plus, lorsque les données collectées dans ce contexte sont fournies par la personne concernée (au moyen de formulaires spécifiques ou par l'intermédiaire de son activité) et traitées sur la base de l'article 6, paragraphe 1, point a), du RGPD (consentement) ou de l'article 6, paragraphe 1, point b), du même règlement (exécution d'un contrat), la personne concernée est habilitée à exercer son droit à la portabilité des données. Ainsi qu'il est souligné dans les lignes directrices sur le droit à la portabilité des données, l'EDPB recommande vivement «que les responsables du traitement expliquent clairement la différence entre les types de données qu'une personne peut recevoir en exerçant son droit d'accès et son droit à la portabilité».

170. Le responsable du traitement devrait donc prévoir un moyen facile de retirer son consentement (uniquement lorsque le consentement constitue la base juridique) librement et à tout moment, et mettre au point des outils permettant de répondre aux demandes de portabilité des données.

171. Ces informations peuvent être fournies à la signature du contrat.

3.4.5 Destinataires

172. En cas de déclaration de vol, les données de localisation peuvent être transmises i) aux agents habilités de la plateforme de télésurveillance et ii) aux autorités légalement habilitées.

3.4.6 Sécurité

173. Les recommandations générales s'appliquent. Voir section 2.7.