PACK DE
CONFORMITÉ

VÉHICULES CONNECTÉS ET DONNÉES PERSONNELLES

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

PACK DE CONFORMITÉ - INTRODUCTION

VÉHICULES CONNECTÉS ET DONNÉES PERSONNELLES

SOMMAIRE

INTRODUCTION

La CNIL, soucieuse de favoriser les écosystèmes d'innovation et d'assurer la protection des données personnelles des usagers de l'automobile, a lancé en mars 2016 les travaux du pack de conformité « véhicules connectés ».

Ce pack a été élaboré en concertation avec les acteurs de la filière automobile, les entreprises de plusieurs secteurs d'activité, dont les assurances et les télécoms, et les autorités publiques, afin de proposer un référentiel sectoriel, véritable boîte à outils pour une utilisation responsable des données.

L'enjeu est d'intégrer la dimension « protection des données personnelles » dès la phase de conception des produits et d'assurer la transparence et le contrôle par les personnes de leurs données. Une telle démarche conditionne la confiance des utilisateurs, et donc le développement pérenne de ces technologies.

Les lignes directrices dégagées dans ce pack constituent l'interprétation de la CNIL de la loi Informatique et Libertés, telle qu'appliquée aux véhicules connectés. Elles reflètent la grille d'analyse utilisée par la CNIL pour apprécier d'éventuels manquements à la loi et constituent un élément de sécurisation juridique pour les responsables de traitement.

Ces lignes permettent aussi aux acteurs concernés d'être en conformité avec le règlement général sur la protection des données, applicable à partir du 25 mai 2018. Le pack a vocation à être porté au niveau européen pour permettre aux acteurs de se positionner sur un marché européen voire mondial. Il pourrait constituer une ligne directrice européenne, comme le prévoit le règlement.

Le pack propose trois hypothèses de travail qui correspondent à trois scenarii rencontrés par les professionnels du secteur. Ces lignes directrices permettent, pour chaque type de traitement identifié, de préciser leurs finalités, les catégories de données collectées, leurs durées de conservation, les droits des personnes, les mesures de sécurité à mettre en place et les destinataires des informations.

INTRODUCTION

Liste des organismes ayant été consultés lors de l'élaboration du pack :

SECTEUR PUBLIC

- Agence de l'Environnement et de la Maîtrise de l'Energie (« ADEME »)
- Autorité de Régulation des Communications Electroniques et des Postes (« ARCEP »)
- Direction Générale des Entreprises (« DGE »)
- Gendarmerie Nationale
- Institut Français des Sciences et Technologies des Transports de l'Aménagement et des Réseaux (« IFSTTAR »)
- Ministère de la Transition Ecologique et Solidaire

PROFESSIONNELS DE L'AUTOMOBILE

- Avis Location
- Comité des Constructeurs Français d'Automobiles (« CCFA »)
- Conseil National des Professions de l'Automobile (« CNPA »)
- Chambre Syndicale Internationale de l'Automobile et du Motocycle (« CSIAM »)
- Drust
- Eliocity (Xee)
- Fédération des Industries des Equipements pour Véhicules (« FIEV »)
- Fédération des Syndicats de la Distribution Automobile (« FSDA »)
- Michelin
- Nexyad
- PSA
- Renault

PROFESSIONNELS DE L'ASSURANCE

- Fédération Française de l'Assurance (« FFA »)

PROFESSIONNELS DES TELECOMS

- Fédération Française des Télécoms (« FFT »)

PROFESSIONNELS DES INDUSTRIES ÉLECTRIQUES, ÉLECTRONIQUES ET DE COMMUNICATION

- Fédération des Industries Electriques, Electroniques et de Communication (« FIEEC »)

Le périmètre du pack

Le pack s'applique aux véhicules connectés, c'est-à-dire aux véhicules qui communiquent avec l'extérieur (applications mobiles, autres véhicules, infrastructure, etc.).

Le pack couvre les seuls usages privés, à l'exclusion de l'utilisation de véhicules de fonction mis à disposition de salariés par leur employeur.

Le pack a pour périmètre les traitements de données personnelles collectées *via* les capteurs des véhicules, les boîtiers télématiques ou les applications mobiles, que les données soient traitées à bord des véhicules ou exportées vers un serveur centralisé.

Les données personnelles concernées comprennent l'ensemble des données associées ou pouvant l'être à une personne physique (conducteur, titulaire de la carte grise, passager, etc.), notamment *via* le numéro de série du véhicule.

Ainsi, il peut s'agir de données directement identifiantes, comme le nom du conducteur, mais également de données indirectement identifiantes, telles que le détail des trajets effectués, les données d'usage du véhicule (par exemple, les données relatives au style de conduite ou au nombre de kilomètres parcourus) ou les données techniques du véhicule (par exemple, les données relatives à l'état d'usure des pièces) qui, par croisement avec d'autres fichiers, peuvent être rattachées à une personne physique.

Ces lignes directrices sont représentatives de l'appréhension, à un moment donné, des technologies et usages associés et feront l'objet d'un bilan régulier. Ainsi, le pack n'est pas prospectif et a vocation à préciser les règles pour des services d'ores et déjà existants sur le marché. À titre d'exemple, les systèmes de transport intelligent (« ITS ») ne sont pas couverts par le pack car les conditions d'un éventuel déploiement ne sont pas encore stabilisées.

1. PÉRIMÈTRE DE LA LOI INFORMATIQUE ET LIBERTÉS ET DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

La loi Informatique et Libertés du 6 janvier 1978 modifiée et le règlement général sur la protection des données s'appliquent dès lors qu'il est procédé à un traitement de données à caractère personnel.

La notion de donnée à caractère personnel est définie largement par la loi Informatique et Libertés. En l'espèce, doivent être considérées comme des données personnelles toutes les données du véhicule qui, seules ou combinées entre elles, peuvent être rattachées à une personne physique (conducteur, titulaire de la carte grise, passager, etc.), notamment *via* le numéro de série du véhicule. Pour déterminer si une personne est identifiée ou identifiable, il convient de prendre en considération l'ensemble des moyens susceptibles d'être utilisés par le responsable de traitement ou par toute autre personne.

En présence d'un traitement de données personnelles, la loi prévoit un certain nombre d'obligations à la charge du responsable de traitement : information des personnes quant au traitement mis en place, voire recueil du consentement, droit d'accès aux données, formalités préalables à effectuer auprès de la CNIL, etc.

En revanche, la loi Informatique et Libertés ne s'applique pas lorsque les données traitées sont anonymes, c'est-à-dire lorsqu'elles ne peuvent pas être associées directement ou indirectement à une personne physique. Pour déterminer le mécanisme à mettre en place pour obtenir des données anonymes, le responsable de traitement doit s'interroger quant à la possibilité de réidentifier les personnes à partir des données obtenues. Les mécanismes d'anonymisation doivent donc être définis au cas par cas, notamment en fonction du niveau de détail des données.

De même, la loi Informatique et Libertés ne s'applique pas dans le cas des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles (comme les traitements décrits dans la fiche n° 1).

2. DÉFINITION DES NOTIONS CLÉS DE LA LOI INFORMATIQUE ET LIBERTÉS ET DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Constitue un **traitement de données personnelles** toute opération (collecte, enregistrement, conservation, modification, extraction, consultation, utilisation, communication, interconnexion, destruction, etc.) portant sur des données personnelles.

Constitue une **donnée à caractère personnel** toute information relative à une personne physique identifiée ou identifiable, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Ainsi, sont des données personnelles toutes les données qui, seules ou combinées entre elles, peuvent être rattachées à un usager identifié ou identifiable, notamment *via* le numéro de série du véhicule ou le numéro de la plaque d'immatriculation, que ce soit par le responsable de traitement ou par toute autre personne. À titre d'exemple, sont des données à caractère personnel les données relatives aux trajets effectués, à l'état d'usure des pièces, aux dates des contrôles techniques, au nombre de kilomètres, ou au style de conduite, dans la mesure où elles sont susceptibles d'être rattachées à une personne physique, notamment *via* le numéro de série du véhicule et le numéro de la plaque d'immatriculation, par le responsable de traitement ou par toute autre personne. Les données personnelles ne sont donc pas uniquement les données nominatives (nom et prénom).

Dans le cadre du présent pack, les catégories de données suivantes seraient notamment concernées :

- les données « client » (nom, prénom, adresse, numéros de téléphone, courriel, etc.) ;
- le numéro de série du véhicule ou tout identifiant unique du véhicule ou d'une pièce (par exemple, le numéro de la plaque d'immatriculation) ;
- les données de géolocalisation ;
- les données techniques liées à l'état du véhicule et des pièces ;
- les données biométriques du conducteur ;
- les données liées à l'utilisation du véhicule par le conducteur ou les occupants (par exemple, les données relatives au style de conduite, au kilométrage, à la vie à bord, etc.).

Constitue **un fichier** tout ensemble structuré et stable de données personnelles accessibles selon des critères déterminés. Il peut s'agir de fichiers informatisés mais également de dossiers papiers classés par exemple par ordre alphabétique ou chronologique.

Le **responsable de traitement** est, sauf désignation expresse par les dispositions législatives ou réglementaires, la personne qui détermine les finalités ou les moyens du traitement. À titre d'exemple, sera qualifié de responsable de traitement le fournisseur de services qui traite les données du véhicule pour adresser au conducteur des messages d'info-trafic, d'éco-conduite ou des alertes sur le fonctionnement du véhicule. Le responsable de traitement doit respecter l'ensemble des obligations imposées par la loi Informatique et Libertés (notamment information voire recueil du consentement de la personne concernée, mise en place de mesures de sécurité adaptées ou réalisation des formalités préalables auprès de la CNIL).

En application de l'article 26 du règlement général sur la protection des données, plusieurs entreprises peuvent se voir reconnaître conjointement la qualité de responsable de traitement. Dans ce cas, il leur appartient de définir de manière transparente leurs obligations respectives, notamment en ce qui concerne l'exercice des droits et l'information de la personne concernée.

Le **sous-traitant** est toute personne traitant des données à caractère personnel au nom et pour le compte du responsable de traitement. Le sous-traitant collecte et traite les données sur instruction du responsable de traitement, sans les exploiter pour son propre compte.

L'article 28 du règlement général sur la protection des données renforce les obligations des sous-traitants. Ainsi, outre l'obligation de mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, les sous-traitants :

- ne pourront pas sous-traiter à un tiers sans l'accord écrit spécifique du responsable de traitement et devront informer le responsable de traitement de toutes modifications concernant leurs propres sous-traitants, afin de donner au responsable de traitement la possibilité d'objecter à de telles modifications ;
- devront s'assurer que toute personne qu'ils autorisent à traiter les données personnelles est soumise à une obligation de confidentialité ;
- devront assister le responsable de traitement dans le respect de ses obligations Informatique et Libertés par des mesures techniques et organisationnelles appropriées ;
- au choix du responsable de traitement, devront effacer ou retourner les données au responsable de traitement au terme du contrat ;
- devront mettre à disposition du responsable de traitement toutes les informations nécessaires pour démontrer son respect de la règlementation Informatique et Libertés ;

- devront informer le responsable de traitement s'ils estiment que le traitement viole le règlement général sur la protection des données ;
- et devront tenir à jour un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement.

La **personne concernée** par un traitement de données personnelles est la personne physique à laquelle se rapportent les données qui font l'objet du traitement. Dans le cadre du présent pack, il peut notamment s'agir du conducteur (principal ou occasionnel), du passager ou du titulaire du certificat d'immatriculation.

Le **destinataire** est toute personne habilitée à recevoir communication des données personnelles, autre que la personne concernée, le responsable de traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données. À titre d'exemple, il peut s'agir d'un partenaire commercial du fournisseur de services.

Le destinataire collecte et traite les données pour son propre compte. Il est donc également responsable de traitement pour les données qui lui sont transmises. Il doit, à ce titre, respecter l'ensemble des obligations imposées par la loi Informatique et Libertés (notamment information, voire recueil du consentement de la personne concernée, mise en place de mesures de sécurité adaptées ou réalisation des formalités préalables auprès de la CNIL).

Précision : les autorités légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à demander à un responsable de traitement la communication de données personnelles ne sont pas des destinataires. À titre d'exemple, sont des tiers autorisés les officiers de police judiciaire, de la police et de la gendarmerie lorsqu'ils demandent à se faire communiquer des données personnelles dans le cadre d'une enquête préliminaire, d'une enquête de flagrance ou d'une commission rogatoire, dans les conditions du code de procédure pénale.

Enfin, la **pseudonymisation** est une technique qui consiste à remplacer des données personnelles directement identifiantes par un pseudonyme non-signifiant. Cela peut par exemple être réalisé par le calcul d'une empreinte obtenue par l'utilisation d'un algorithme de hachage à clé secrète. Le recours à la pseudonymisation des données permet d'améliorer la protection de la confidentialité des informations à caractère personnel en réduisant les risques de mésusage. L'opération de pseudonymisation n'est pas irréversible, contrairement à l'anonymisation (voir avis n° 05/2014 sur « *les techniques d'anonymisation* » rendu par le G29 le 10 avril 2014). Des données anonymes ne sont plus soumises à la loi Informatique et Libertés. En revanche, tel n'est pas le cas de données pseudonymisées, qui restent des données à caractère personnel.

3. LES PRINCIPES CLÉS À RESPECTER AU REGARD DE LA LOI INFORMATIQUE ET LIBERTÉS ET DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

La mise en place d'un traitement de données personnelles doit respecter les principes posés par la loi Informatique et Libertés. En effet, toute personne qui souhaite traiter des données personnelles est soumise à un certain nombre d'obligations légales.

L'AUTODÉTERMINATION INFORMATIONNELLE

(article 1 de la loi Informatique et Libertés)

L'article 1er la loi Informatique et Libertés prévoit que l'informatique doit être au service de chaque citoyen et ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. En outre, en application de l'article 1er, alinéa 2, toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données personnelles la concernant.

Ce droit à l'autodétermination informationnelle traduit la nécessaire maîtrise par l'individu de ses données tout au long du traitement.

FOCUS

Concrètement, cette maîtrise implique notamment :

- des paramétrages par défaut protecteurs de la vie privée ;
- la possibilité pour l'usager de modifier aisément ces paramétrages, tout au long du traitement, notamment aux fins d'activer ou de désactiver les services fondés sur le consentement ou l'exécution d'un contrat (par exemple, les offres commerciales personnalisées en fonction de la géolocalisation ou l'assistance dépannage) ;
- le cas échéant, la possibilité pour l'usager d'ajuster la granularité des données collectées au niveau de service demandé, par exemple en accédant à une carte sans être géolocalisé si l'usager ne souhaite pas être guidé ; et
- la possibilité pour l'usager d'accéder aisément à ses données.

L'OBLIGATION DE DISPOSER D'UNE BASE LÉGALE POUR LES TRAITEMENTS MIS EN ŒUVRE

(article 7 de la loi Informatique et Libertés et article 6 du règlement général sur la protection des données)

Un traitement doit avoir le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :

1 - le respect d'une obligation légale incombant au responsable de traitement ;
2 - la sauvegarde de la vie de la personne concernée ;
3 - l'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;

4 - l'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;

5 - la réalisation de l'intérêt légitime poursuivi par le responsable de traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Ce qui change avec le RGPD

Lorsque le consentement constitue la base légale du traitement, l'article 7 du règlement général sur la protection des données prévoit que celui-ci doit être spécifique, c'est-à-dire distingué clairement des autres questions, sous une forme compréhensible et aisément accessible, formulé en des termes clairs et simples. En outre, la personne concernée a le droit de retirer son consentement à tout moment, ce dont elle doit être expressément informée. Enfin, le responsable de traitement doit être en mesure de démontrer que la personne concernée a donné son consentement au traitement de données personnelles la concernant.

LA LOYAUTÉ DE LA COLLECTE

(article 6-1° de la loi Informatique et Libertés et article 5-1° a/ du règlement général sur la protection des données)

Tout traitement de données personnelles doit être effectué dans des conditions permettant d'en assurer la transparence vis-à-vis des personnes concernées et ne saurait être mis en œuvre à l'insu des personnes concernées.

Cette obligation implique *a minima* une information des personnes conforme à l'article 32 de la loi Informatique et Libertés, voire le recueil du consentement.

LA FINALITÉ

(article 6-2° de la loi Informatique et Libertés et article 5-1° b/ du règlement général sur la protection des données)

Des données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé, explicite et légitime. Les objectifs poursuivis par le responsable du traitement doivent donc être préalablement définis, de manière claire, explicite et exhaustive.

Toute utilisation de données à caractère personnel pour un objectif incompatible avec la finalité première du traitement est un détournement de finalité passible de sanctions administratives ou pénales.

Par exemple, *un garagiste ne saurait vendre aux assureurs les données techniques du véhicule pour leur permettre d'en déduire les profils de conduite de leurs assurés.*

LES PRINCIPES DE PROPORTIONNALITÉ DES DONNÉES

(article 6-3° de la loi Informatique et Libertés et article 5-1° c/ du règlement général sur la protection des données)

Seules doivent être traitées les informations pertinentes, adéquates et non excessives au regard de la finalité du traitement, c'est-à-dire de son objectif. Le règlement général sur la protection des données parle à ce titre du principe de « *minimisation des données* ».

Par exemple, *un responsable de traitement ne saurait traiter en continu la localisation précise et détaillée du véhicule pour une finalité de maintenance technique ou d'optimisation de modèles.*

LA DURÉE LIMITÉE DE CONSERVATION DES DONNÉES

(article 6-5° de la loi Informatique et Libertés et article 5-1° e/ du règlement général sur la protection des données)

Des données à caractère personnel ne peuvent être conservées de façon indéfinie dans un fichier.

Une durée de conservation précise doit impérativement être déterminée, en fonction de la finalité de chaque traitement, par le responsable du traitement.

Par exemple, *un responsable de traitement ne saurait conserver sans limitation de durée les données techniques de véhicules identifiés (notamment par le biais du numéro de série) à des fins d'amélioration du produit, sauf anonymisation des données.*

Des dispositions législatives ou réglementaires peuvent toutefois contraindre un responsable de traitement à conserver des données au-delà de leur durée de conservation en base active.

Dans ce cas, les données peuvent être conservées dans une base d'archive, le temps nécessaire au respect de l'obligation en question, dans le respect des conditions prévues par la délibération de la CNIL relative aux modalités d'archivage électronique dans le secteur privé (voir délibération n° 2005-213 du 11 octobre 2005) : on parle alors d'archivage intermédiaire.

LA SÉCURITÉ ASSURANT LA CONFIDENTIALITÉ DES DONNÉES

(article 34 de la loi Informatique et Libertés et article 5-1° f/ du règlement général sur la protection des données)

Le responsable du traitement est astreint à une obligation de sécurité : il doit notamment prendre les mesures nécessaires pour garantir la confidentialité des données qu'il a collectées et éviter leur divulgation à des tiers non autorisés.

Dans le contexte du véhicule connecté, ce besoin de confidentialité et de sécurité des données devra s'appliquer aussi bien aux données collectées et traitées au sein du véhicule qu'aux données transmises à l'extérieur du véhicule. Des mesures générales de sécurité devront donc être prises, impliquant notamment :

- la mise en œuvre de mesures de chiffrement des canaux de communication (par exemple *via* l'ajout d'un module de sécurité de type « *Hardware Security Module* ») et leur correct paramétrage (renouvellement et sécurisation des clés par exemple) ;
- la gestion des habilitations au sein du système d'information traitant les données ;
- des mécanismes d'authentification des différents appareils prenant part à la communication (calculateurs embarqués, capteurs, serveurs, utilisateurs, tiers, etc.) ;
- un processus robuste et sécurisé de mise à jour des équipements ;
- un cloisonnement efficace des différents domaines et sous-domaines prenant part au traitement (fonctions vitales du véhicule, fonctions de communication, etc.) associé à la mise en œuvre de mesures de filtrage ; et
- dans le cas d'une authentification par mot de passe, application des recommandations de la Commission du 22 juin 2017 (voir délibération n° 2017-190 du 22 juin 2017) ;
- la détection d'intrusion dans le système d'information et la possibilité d'un fonctionnement en mode dégradé en cas d'attaque.

Les mesures de sécurité doivent être adaptées aux risques présentés par le traitement. Dès lors, compte tenu de ce qu'un traitement des données en local (scénario n° 1 « IN → IN ») présente moins de risques d'un point de vue sécurité qu'un traitement des données à l'extérieur de véhicule (scénarii n° 2 et n° 3), les exigences de sécurité pourront être allégées lorsque les données seront traitées à l'intérieur du véhicule.

Toutefois, quelle que soit leur localisation, la sensibilité de certaines données (par exemple, les données susceptibles de révéler des infractions) impose un niveau d'exigence supplémentaire en matière de sécurité, du fait des conséquences sur la vie privée que pourrait avoir la diffusion de ces données.

Enfin, les mesures de sécurité doivent être régulièrement révisées et actualisées par rapport à l'état de l'art et aux risques pesant sur le traitement, notamment au regard de la gravité des impacts potentiels sur la vie privée des personnes concernées (qui s'apprécie en particulier au regard de la nature des données traitées) et de leur vraisemblance. La capacité de mise à jour des mesures de sécurité dans le temps est donc également un enjeu, notamment au regard du nombre de véhicules concernés et de la longévité de ce type de produit.

Ce qui change avec le RGPD

En application de l'article 33 du règlement général sur la protection des données, en cas de violation de données à caractère personnel susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, il appartiendra au responsable de traitement de notifier la violation à la CNIL, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance. En application de l'article 34 du règlement général sur la protection des données, il appartiendra également au responsable de traitement d'en informer les personnes concernées si la violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés.

L'INFORMATION DES PERSONNES CONCERNÉES

(article 32 de la loi Informatique et Libertés et articles 12, 13 et 14 du règlement général sur la protection des données)

Toute personne physique auprès de laquelle sont recueillies des données à caractère personnel la concernant doit en être préalablement informée.

Plus particulièrement, les personnes concernées doivent être informées :

- de l'identité du responsable de traitement ou de son représentant ;
- des finalités poursuivies par le traitement ;
- du caractère obligatoire ou facultatif des réponses ;
- des conséquences éventuelles d'un défaut de réponse ;
- des destinataires ou catégories de destinataires des données ;
- de l'existence de droits à leur profit (droit d'opposition, droit d'accès aux données les concernant et droit de rectification) et des coordonnées du service auprès duquel ces droits peuvent être exercés ;
- de la durée de conservation des catégories de données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée ;
- le cas échéant, des transferts de données effectuées vers des pays non membres de l'Union européenne (pays d'établissement des destinataires, nature des données transférées, finalité du transfert, catégories de destinataires, niveau de protection offert par le(s) pays tiers).

Ce qui change avec le RGPD

Le règlement général sur la protection des données renforce l'obligation d'information des personnes concernées et prévoit la communication aux personnes concernées de nouvelles informations, en plus des obligations déjà existantes, en des termes clairs, simples et aisément accessibles, à savoir :

- les coordonnées du délégué à la protection des données ;
- la base juridique du traitement ;
- la mention explicite des intérêts légitimes poursuivis par le responsable de traitement lorsque ces derniers constituent la base juridique du traitement ;
- la mention du droit de demander au responsable de traitement l'effacement des données ou une limitation du traitement relatif à la personne concernée, ainsi que celle du droit à la portabilité des données ;
- l'existence du droit de retirer son consentement à tout moment ;
- le droit d'introduire une réclamation auprès de la CNIL ;
- des informations sur la question de savoir si l'exigence de fourniture de données personnelles 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 personnelles, ainsi que les conséquences éventuelles de la non-fourniture de ces données ;
- l'existence d'une prise de décision automatisée, y compris un profilage produisant des effets juridiques ou l'affectant de manière significative de façon similaire et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

De plus, lorsque les données n'ont pas été collectées directement par le responsable de traitement, le responsable doit également indiquer, en plus des informations mentionnées ci-dessus, la source auprès de laquelle il a obtenu ces données et, le cas échéant, si ces données étaient publiquement accessibles.

Ces informations doivent être communiquées dans une période raisonnable après l'obtention des données et au plus tard à la première des dates suivantes : (i) un mois après l'obtention des données, eu égard aux circonstances particulières dans lesquelles les données sont traitées, (ii) lors de la première communication avec la personne concernée ou (iii) en cas de communication de ces données à un tiers, avant une telle communication.

FOCUS

Les informations destinées aux personnes concernées peuvent être fournies par strates, c'est-à-dire en dissociant deux niveaux d'information : d'une part, les informations de premier niveau, qui sont les plus importantes pour les personnes, d'autre part, les informations qui ne présentent vraisemblablement d'intérêt qu'en seconde intention. Parmi les informations essentielles de premier niveau figurent, outre l'identité du responsable de traitement, les finalités du traitement et toute information supplémentaire nécessaire afin de garantir un traitement loyal de l'information vis-à-vis des personnes concernées (voir avis n° 10/2004 sur les « *dispositions davantage harmonisées en matière d'information* » rendu par le G29 le 25 novembre 2004).

La Commission recommande que les personnes concernées soient informées :

- par le biais de clauses, concises et aisément compréhensibles, figurant dans le contrat de vente du véhicule et / ou de prestation de services ; et
- par le biais de documents distincts (par exemple, le carnet d'entretien ou le manuel du véhicule) ou sur l'ordinateur de bord ; et
- par le recours à des icônes normalisées à l'intérieur des véhicules. La Commission encourage fortement la mise en place de ces icônes, afin d'informer les personnes concernées de manière claire, synthétique et facilement compréhensible du traitement de leur données. De plus, la Commission insiste sur l'importance de l'harmonisation de ces icônes, de façon à ce que l'usager retrouve les mêmes symboles quelle que soit la marque ou le modèle du véhicule.

LES DROITS DES PERSONNES

(articles 38, 39 et 40 de la loi Informatique et Libertés et articles 15 à 21 du règlement général sur la protection des données)

La personne concernée dispose des droits suivants :

- **le droit d'opposition pour motifs légitimes :** toute personne physique a le droit de s'opposer pour des motifs légitimes à ce que des données personnelles la concernant fassent l'objet d'un traitement, sauf si celui-ci résulte d'une obligation légale. Le responsable d'un traitement auprès duquel un droit d'opposition a été exercé doit informer sans délai de cette opposition tout autre responsable de traitement qu'il a rendu destinataire des données personnelles qui font l'objet de l'opposition ;

- **le droit d'opposition non subordonné aux motifs légitimes :** toute personne physique a le droit de s'opposer, quels qu'en soient les motifs, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale. Les personnes concernées doivent être en mesure d'exprimer leur opposition avant la validation définitive de leurs réponses ;

- **le droit d'accès :** toute personne physique justifiant de son identité peut obtenir une copie des données personnelles la concernant et accéder à toute information disponible quant à l'origine de celles-ci, ainsi qu'aux informations permettant de connaître et de contester la logique du traitement en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à son égard ;

- **le droit de rectification :** toute personne physique justifiant de son identité peut demander au responsable de traitement de rectifier les données personnelles la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite. Lorsque les données ont été transmises à un tiers, le responsable de traitement ayant procédé à leur rectification doit également en informer ce destinataire sans délai, lequel doit à son tour modifier son traitement.

Ce qui change avec le RGPD

Outre les droits mentionnés ci-dessus, le règlement général sur la protection des données instaure trois nouveaux droits, à savoir le droit à l'oubli, le droit à la portabilité et le droit à la limitation du traitement.

LE DROIT À L'OUBLI

(article 17 du règlement général sur la protection des données)

Toute personne peut demander l'effacement de ses données personnelles par le responsable de traitement lorsque :

- les données ne sont plus nécessaires au vu des finalités pour lesquelles elles ont été collectées ;
- la personne concernée retire son consentement (lorsque celui-ci constituait la base juridique du traitement) et il n'existe pas d'autre fondement juridique au traitement ;
- la personne concernée s'oppose à un traitement basé sur l'exécution d'une mission d'intérêt public ou sur des intérêts légitimes, pour des raisons tenant à sa situation particulière, et il n'existe pas de motif légitime impérieux pour le traitement ;
- la personne concernée s'oppose au traitement de ses données à des fins de prospection ;
- les données ont été traitées de manière illicite ;
- la loi applicable requiert l'effacement de ces données ;
- les données ont été collectées en lien avec les offres de services de la société de l'information et concernent un enfant.

Lorsque le responsable de traitement a rendu les données publiques et est obligé de les effacer, il doit prendre des mesures raisonnables au vu de la technologie disponible et des coûts de mise en œuvre, pour informer les tiers qui traitent lesdites données qu'une personne concernée leur demande d'effacer tous liens vers ces données à caractère personnel ou toute copie ou reproduction de celles-ci.

Le droit à l'oubli ne s'applique pas si la conservation des données est nécessaire à l'exercice du droit à la liberté d'expression, au respect d'une obligation légale de conserver les données ou à l'exécution d'une tâche d'intérêt public, dans le domaine de la santé publique ou pour des besoins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ou pour l'établissement, l'exercice ou la défense de droits en justice.

LE DROIT À LA PORTABILITÉ

(article 20 du règlement général sur la protection des données)

Le droit à la portabilité permet à une personne de recevoir les données personnelles la concernant, dans un format structuré, couramment utilisé et lisible par machine. La personne concernée peut, par la suite, transmettre ces données à un autre responsable de traitement ou, lorsque cela est techniquement possible, demander que les données personnelles soient transmises par le responsable de traitement directement au nouveau responsable de traitement. Celui qui détient les données ne peut s'opposer à la mise en œuvre de ce droit, qui s'exerce à titre gratuit, en application de l'article 12-5° du règlement général sur la protection des données.

Enfin, la présence de données relatives à des tiers (faisant souvent partie de l'entourage de la personne concernée, à l'exemple d'un carnet de contacts) dans les données demandées dans le cadre d'une portabilité ne peut justifier en elle-même un rejet de la demande de portabilité.

L'exercice de ce droit est cependant précisément encadré.

D'une part, il ne peut s'appliquer qu'à des données contenues dans des traitements automatisés, ce qui exclut les données contenues dans les fichiers dits « papiers ».

D'autre part, et surtout, ce droit ne peut s'appliquer qu'à des données personnelles traitées sur la base du consentement de la personne concernée ou dans le cadre d'un traitement nécessaire à l'exécution d'un contrat passé par elle (par exemple, données issues de la fourniture d'un service de géolocalisation à la demande du conducteur). Ainsi, les données personnelles traitées sur la seule base de l'intérêt légitime du responsable de traitement ne peuvent faire l'objet d'une demande de portabilité. À titre d'exemple, les données techniques collectées exclusivement pour l'optimisation de modèles par les constructeurs ne font pas partie des données pouvant être portées.

Les lignes directrices du G29 sur « *le droit à la portabilité* » du 5 avril 2017 ont notamment précisé l'étendue des données concernées par ce droit. Celui-ci s'applique aux données fournies par la personne concernée c'est-à-dire transmises au responsable de traitement par exemple par le biais d'un formulaire (nom, adresse électronique, numéro de téléphone) ou d'un système de navigation du véhicule (les destinations vers lesquelles l'on souhaite être guidé). Il s'applique également aux données générées par l'activité du conducteur (historique de trajets, données relatives au style de conduite, etc.).

À l'inverse, le droit à la portabilité ne s'applique pas aux configurations techniques non fournies par l'usager (par exemple, les cartographies moteur ou les cartographies d'injection, etc.) et aux données inférées par le responsable de traitement lui-même à partir des données fournies par la personne (par exemple, score relatif à la façon de conduire, note d'éco-conduite, etc.) : en effet,

ces données ne sont pas fournies par la personne concernée, mais créées par le responsable de traitement lui-même.

Concernant les conditions de transmission des données personnelles à un autre responsable de traitement, le droit à la portabilité n'a pas vocation à permettre le contournement de dispositions particulières. Ainsi, ce droit ne peut faire échec au règlement européen du 20 juin 2007 modifié qui prévoit que la transmission par les constructeurs automobiles d'informations sur la réparation et l'entretien des véhicules aux opérateurs indépendants n'est pas gratuite et peut être subordonnée au paiement de « *frais raisonnables et proportionnés* ».

LE DROIT À LA LIMITATION DU TRAITEMENT

(article 18 du règlement général sur la protection des données)

La personne concernée a également le droit d'obtenir du responsable de traitement la limitation du traitement lorsque :

- l'exactitude des données est contestée par la personne concernée, pendant une durée permettant au responsable de traitement de vérifier l'exactitude des données ;
- le traitement est illicite ;
- le responsable de traitement n'a pas besoin des données mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ;
- la personne concernée s'est opposée à un traitement basé sur l'exécution d'une mission d'intérêt public ou sur des intérêts légitimes, pour des raisons tenant à sa situation particulière, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable de traitement prévalent sur ceux de la personne concernée.

Lorsque le traitement a été ainsi limité, les données personnelles ne peuvent, à l'exception de la conservation, être traitées qu'avec le consentement de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice, ou pour la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public.

Enfin, l'article 11 du règlement général sur la protection des données précise que le responsable de traitement n'est pas tenu d'obtenir des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter le règlement. Ainsi, dans l'optique d'une minimisation des données et de respect de la vie privée, les fournisseurs de services n'ont pas l'obligation de recueillir les données personnelles des passagers uniquement aux fins de leur permettre d'exercer leurs droits.

LA PROTECTION DES DONNÉES DÈS LA CONCEPTION ET LA PROTECTION DES DONNÉES PAR DÉFAUT

(article 25 du règlement général sur la protection des données)

L'article 25, alinéa 1, du règlement général sur la protection des données impose au responsable de traitement l'obligation d'intégrer la protection des données personnelles dès la phase d'élaboration et de conception du produit (« *privacy by design* »).

De plus, l'article 25, alinéa 2, du règlement général sur la protection des données dispose que le responsable de traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données personnelles qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées (« *privacy by default* »).

Les traitements de données personnelles mis en œuvre après le 25 mai 2018 devront être conformes à ces deux principes.

LES FORMALITÉS PRÉALABLES À LA MISE EN PLACE D'UN TRAITEMENT

Tout traitement de données à caractère personnel doit faire l'objet d'une formalité auprès de la CNIL préalablement à sa mise en œuvre, sauf s'il en est spécifiquement exonéré.

Les formalités à accomplir (déclaration, demande d'autorisation ou demande d'avis) dépendent de la finalité du traitement et de la nature des données collectées.

Toutes les formalités peuvent être effectuées en ligne sur le site web de la CNIL. En cas de doute sur le régime dont relève le traitement ou sur vos obligations, vous pouvez interroger les services de la CNIL.

Précision : La réception d'un accusé de réception d'une formalité effectuée auprès de la CNIL n'exonère pas le responsable de traitement des obligations de fond prévues par la loi Informatique et Libertés.

Ce qui change avec le RGPD

Le règlement général sur la protection des données entraîne un allègement des obligations en matière de formalités préalables, puisque le régime déclaratif sera supprimé. Il n'en demeure pas moins que les traitements de données personnelles *via* les véhicules connectés sont susceptibles de présenter un risque élevé pour le respect de la vie privée. En telle hypothèse, le responsable de traitement devra effectuer une étude d'impact, analyser les risques encourus et documenter sa conformité conformément au principe d'« *accountability* ».

Les bonnes questions à se poser avant de créer un traitement :

1 - Le traitement est-il légitime, notamment au regard de mes missions et des droits des personnes ?

2 - Quel est le but de ce traitement ? À quoi va-t-il servir ?

3 - Comment présenter cette finalité pour la rendre compréhensible par tous ?

4 - Quelles sont les données dont j'ai forcément besoin pour atteindre l'objectif fixé ?

5 - Est-il possible d'atteindre le même objectif en traitant moins de données ?

6 - Jusqu'à quand ces données me seront-elles utiles (évènement butoir, durée, obligations légales ou sauvegarde d'un droit en justice) ?

7 - Comment vais-je informer les personnes concernées, de manière claire et simple ?

8 - Comment vais-je garantir les droits des personnes concernées (notamment les droits d'accès, d'opposition et de rectification) ?

9 - Ai-je donné la complète maîtrise aux utilisateurs sur les traitements qui les concernent (activation / désactivation des fonctionnalités à tout moment) ?

10 - Ai-je mené une analyse de risques pour définir des mesures de sécurité adéquates (techniques et organisationnelles) ?

11 - Ai-je pris les mesures techniques permettant de corriger rapidement un défaut de sécurité ?

12 - Quelle est la formalité à accomplir auprès de la CNIL ?

SCÉNARIO N°1
IN → IN

LES DONNÉES DU VÉHICULE NE SONT PAS TRANSMISES AU FOURNISSEUR DE SERVICES

PÉRIMÈTRE

Dans ce scénario, les données collectées dans le véhicule restent sous la maîtrise unique de l'usager et ne sont pas transmises au fournisseur de services, ce qui peut notamment correspondre aux deux cas suivants :

1 **Les applications purement « IN → IN » :** plusieurs produits ou solutions communiquent entre eux à l'intérieur du véhicule, sans aucune sortie de données vers l'extérieur.

Exemple : *une solution d'éco-conduite qui traite les données dans le véhicule aux fins d'afficher des conseils d'éco-conduite en temps réel sur l'ordinateur de bord.*

2 **Les applications qui impliquent une sortie des données du véhicule, sans que ces données ne soient transmises au fournisseur de services. Sont ainsi concernées les applications pour lesquelles les données personnelles :**

- restent confinées sur des réseaux de communications intégralement sous la maîtrise de l'usager (type Wi-Fi, Bluetooth ou autre réseau local) ; ou
- circulent sur des réseaux de télécommunications ouverts au public (type ADSL, fibre, GSM).

Le fait que les données passent sur les réseaux gérés par des opérateurs de communications électroniques ne pose pas de difficultés dans la mesure où ces opérateurs ont des obligations renforcées quant à ce qu'ils peuvent faire avec ces données de trafic. Ceci n'est cependant valable que si l'opérateur en question agit bien en tant que fournisseur du service de communication électronique. À l'inverse, si l'opérateur souhaite fournir un autre service, les recommandations applicables sont celles des scénarii n° 2 ou n° 3.

Exemple : *une application par ordiphone qui communique directement avec le véhicule via l'ordinateur de bord, sans que les données du véhicule soient transmises au fournisseur de l'application et, à l'inverse, sans que les données de l'ordiphone ne soient transmises au constructeur.*

ANALYSE DES TRAITEMENTS DE DONNÉES PERSONNELLES AU REGARD DE LA LOI INFORMATIQUE ET LIBERTÉS ET DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

En application de l'article 2, alinéa 1, de la loi Informatique et Libertés et de l'article 2-2° c/ du règlement général sur la protection des données, les traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles ne sont pas soumis à la règlementation Informatique et Libertés.

Dès lors, les cas d'usage qui relèvent du scénario présenté dans cette fiche permettent de s'affranchir du respect de la loi Informatique et Libertés, sous réserve que les données ne soient pas transmises au fournisseur de services et que l'usager conserve l'entière maîtrise de ses données.

Concrètement, la maîtrise par l'usager de ses données implique notamment :

- que les données personnelles ne soient pas transmises au fournisseur de services ;
- la désactivation par défaut, au démarrage du véhicule, de la collecte en local des données de géolocalisation et des données relatives aux infractions, sauf en cas de traitement des données en temps réel ;
- la possibilité de désactiver à tout moment les fonctionnalités concernées, à l'exclusion des fonctionnalités strictement nécessaires au fonctionnement du véhicule ;
- en l'absence d'un traitement en temps réel, la possibilité d'accéder et de supprimer aisément l'historique de ses données d'usage (*via* par exemple, un bouton à l'intérieur du véhicule et / ou *via* son ordiphone et / ou ordinateur de bord) ;
- l'information de l'usager des données susceptibles d'être conservées en local, des finalités du traitement, ainsi que de la possibilité d'effacer les données.

FOCUS

Concernant la désactivation par défaut, celle-ci n'exclut pas la possibilité de prédéfinir des profils, activables à la main de l'usager, pour lesquels la collecte des données s'opérerait par défaut au démarrage du véhicule, de façon à ce que l'usager n'ait pas à paramétrer ses préférences à chaque démarrage.

Précision : ce scénario n'est pas applicable lorsque le véhicule est mis à disposition de salariés et que l'employeur impose l'utilisation de fonctionnalités telles que l'éco-conduite ou l'authentification biométrique. Dans ces cas de figure, même si les données restent stockées dans le véhicule, l'exception d'usage domestique n'est pas applicable.

Lorsque cela est possible au regard de la finalité, les traitements en temps réel sont à privilégier (par exemple, conseils d'éco-conduite ne nécessitant pas d'historique).

FINALITÉS POURSUIVIES PAR LES TRAITEMENTS (LISTE NON EXHAUSTIVE)

- **Finalité 1 : amélioration de l'expérience de conduite ou de la vie à bord (« *infotainment* »)** : l'usager bénéficie de fonctionnalités visant à améliorer son expérience de conduite (par exemple, réglage automatique des sièges en fonction de la taille du conducteur).

- **Finalité 2 : amélioration de la conduite d'un point de vue « sécurité routière » et maintenance préventive :** l'usager reçoit des messages pour améliorer sa conduite (par exemple, signal sonore ou vibration du volant en cas de dépassement sans clignotant, de franchissement de ligne blanche ou d'excès de vitesse) ou pour l'alerter sur l'état du véhicule (par exemple, alerte sur l'état d'usage des plaquettes de frein).

- **Finalité 3 : assistance automatisée à la conduite :** l'usager bénéficie de fonctions automatisées d'assistance à la conduite (par exemple, régulateur de vitesse adaptatif, stationnement automatique, freinage d'urgence automatique).

- **Finalité 4 : déverrouillage, démarrage et activation de certaines commandes du véhicule grâce aux données biométriques du conducteur :** l'usager souhaite déverrouiller ou démarrer son véhicule grâce à ses données biométriques (par exemple, son empreinte digitale), actionner certaines commandes du véhicule grâce à la reconnaissance vocale ou être alerté en cas d'assoupissement (par exemple, grâce à la reconnaissance des points de pression exercés par le dos du conducteur sur le siège avant).

BASE LÉGALE

Le présent scénario implique une entière maîtrise par l'usager de ses données.

Dans le cadre du présent scénario, la Commission estime que la maîtrise de données biométriques implique nécessairement, d'une part, la possibilité d'avoir recours à une alternative non biométrique (par exemple, l'usage d'une clé physique ou d'un code) sans contrainte additionnelle et, d'autre part, le stockage et la comparaison du gabarit biométrique, sous forme chiffrée, uniquement en local, sans que les données biométriques ne soient traitées par un terminal de lecture / comparaison extérieur.

DONNÉES COLLECTÉES

Compte tenu de ce que la loi Informatique et Libertés, et plus particulièrement son article 9, ne s'applique pas aux traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles, le présent scénario permet le traitement de données relatives aux infractions, sous réserve que ces données soient traitées sans être transmises au fournisseur de services.

Au regard de la nature de ces données, il est recommandé de traiter ces données en temps réel et sans stockage, y compris en local.

DURÉE DE CONSERVATION

L'utilisateur doit pouvoir supprimer à tout moment l'ensemble des données d'usage stockées en local dans le véhicule, à l'exception des données nécessaires au bon fonctionnement du véhicule.

Par défaut, les données sont conservées le temps nécessaire à la fourniture du service. Par exemple, les données nécessaires à la constitution d'un indicateur d'éco-conduite sont conservées le temps de calculer l'indice d'éco-conduite. L'indice d'éco-conduite peut quant à lui être conservé tant que l'usager ne vend pas son véhicule ou ne fait pas le choix de supprimer les données.

Pour les véhicules d'occasion, la CNIL recommande que les données d'usage soient systématiquement supprimées avant leur mise en vente. De même, les données doivent être supprimées avant la mise à la casse.

DESTINATAIRES

L'utilisateur peut seul avoir accès aux données.

INFORMATION ET DROITS DES PERSONNES

Pour permettre à l'utilisateur d'exercer une maîtrise effective sur ses données, il est nécessaire de l'informer des données susceptibles d'être traitées en local, des finalités du traitement, ainsi que de la possibilité de désactiver à tout moment la collecte et d'effacer les données concernées.

SÉCURITÉ

La CNIL recommande de prendre toutes les précautions utiles permettant de garantir la sécurité et la confidentialité des données personnelles.

Plus particulièrement, la Commission préconise :

- l'authentification des appareils destinataires des données ;
- la subordination de l'accès aux données personnelles à une authentification fiable de l'utilisateur (dans le cas d'une authentification par mot de passe, application des recommandations de la Commission du 22 juin 2017, certificat électronique, etc.).

Les mesures ainsi mises en place doivent être adaptées au niveau de sensibilité des données et aux capacités de contrôle des appareils. Ainsi, en cas de traitement de données relatives à des infractions, la Commission recommande la mise en place de mesures de sécurité fortes, telles que :

- le chiffrement des données avec des algorithmes à l'état de l'art, à la main de l'usager, par exemple, *via* un secret détenu par ce dernier ;
- le renouvellement régulier des clés de chiffrement ;
- la protection des clés de chiffrement de toute divulgation accidentelle ;
- la protection contre la lecture par une personne non habilitée ;
- la protection physique contre la modification de ces données par un tiers.

S'agissant des données biométriques, en complément des mesures ci-dessus, il convient de s'assurer que la solution d'authentification biométrique est suffisamment fiable, notamment en vérifiant :

- que 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 ;
- que la solution biométrique utilisée repose sur un capteur résistant aux attaques considérées comme triviales en l'état de l'art (telles que, à l'heure actuelle, l'utilisation d'une empreinte imprimée à plat pour la reconnaissance d'empreinte digitale) ;
- que le nombre d'essais d'authentification est limité ;
- que seul le gabarit biométrique est stocké dans le dispositif, et ce de manière chiffrée à l'aide d'un algorithme cryptographique et d'une gestion des clés conformes à l'état de l'art ; et
- que 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 en local (par exemple, les enregistrements audio dans le cas d'un système de reconnaissance vocale).

Dans l'hypothèse où les communications entre le véhicule et l'ordiphone se font via des réseaux de télécommunications, la Commission préconise un chiffrement du canal de communication avec un algorithme à l'état de l'art.

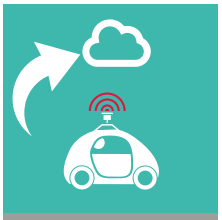
FORMALITÉS PRÉALABLES

Dans la mesure où les traitements sont mis en œuvre pour l'exercice d'activités exclusivement personnelles, il n'y a pas de formalités à effectuer auprès de la CNIL.

FOCUS

Ce scénario présente les avantages suivants :

- il confère à l'usager une bonne maîtrise de ses données, ce qui constitue un facteur de confiance et d'acceptabilité des produits ;
- il permet le traitement de données dont la collecte est strictement encadrée dans le cadre des scénarii n° 2 et n° 3 (par exemple, le traitement de données d'infraction et de données biométriques) ;
- il présente moins de risques de piratage et implique peu de latence, ce qui le rend particulièrement adapté aux fonctions automatisées d'assistance à la conduite ;
- pour certaines données, il implique des mesures de sécurité allégées par rapport aux autres scénarii ;
- sa mise en œuvre ne nécessite pas de formalité préalable auprès de la CNIL.



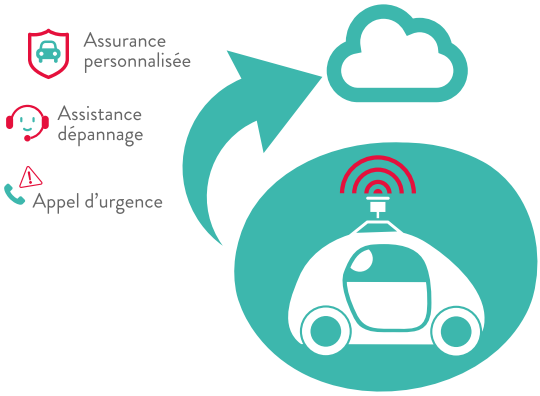
SCÉNARIO N°2
IN → OUT

LES DONNÉES DU VÉHICULE SONT TRANSMISES AU FOURNISSEUR DE SERVICES, SANS DÉCLENCHER À DISTANCE D'ACTION AUTOMATIQUE DANS LE VÉHICULE

PÉRIMÈTRE

Ce scénario couvre les cas dans lesquels les données collectées sont transmises au fournisseur de services, par exemple, afin de fournir un service à valeur ajoutée à l'usager ou améliorer les produits.

Il concerne l'hypothèse dans laquelle un service fonctionne à distance mais n'entraîne pas d'action automatique dans le véhicule (à la différence du scénario n° 3).



ANALYSE DES TRAITEMENTS DE DONNÉES PERSONNELLES AU REGARD DE LA LOI INFORMATIQUE ET LIBERTÉS ET DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

La mise en place d'un traitement de données personnelles doit respecter la règlementation Informatique et Libertés. En effet, toute personne qui souhaite traiter des données personnelles est soumise à un certain nombre d'obligations légales.

FINALITÉS POURSUIVIES PAR LES TRAITEMENTS (LISTE NON EXHAUSTIVE)

- **Finalité 1 : optimisation de modèles, amélioration du produit :** un fournisseur de services établit des statistiques sur les paramètres de fonctionnement du véhicule ou l'état d'usure des pièces sur la base des données d'usage de la personne concernée.
- **Finalité 2 : études d'accidentologie :** la personne concernée accepte, sur la base du volontariat, de participer à des études d'accidentologie visant à mieux comprendre les causes des accidents de la route.
- **Finalité 3 : exploitation commerciale des données du véhicule :** la personne concernée contracte avec un fournisseur de services aux fins d'obtenir des services à valeur ajoutée relatifs à son véhicule (par exemple, contrat de « *Pay as you drive* » ou assistance dépannage).
- **Finalité 4 : « *e-Call* » :** en cas d'accident grave sur le territoire de l'Union, le véhicule déclenche automatiquement un appel « *e-Call* » vers le 112, numéro d'appel d'urgence européen.
- **Finalité 5 : lutte contre le vol :** en cas de vol, la personne concernée souhaite retrouver son véhicule grâce à la géolocalisation. L'utilisation des données de localisation est limitée aux strictes nécessités de l'enquête et de l'instruction du dossier par les autorités judiciaires compétentes.

SCÉNARIO N°2 - « IN → OUT » :

Les données du véhicule sont transmises au fournisseur de services, sans déclencher à distance d'action automatique dans le véhicule

BASE LÉGALE

- **Pour la finalité 1** (optimisation de modèles, amélioration du produit), si les données sur lesquelles repose le traitement sont anonymisées, celles-ci ne sont plus des données personnelles et peuvent donc être librement utilisées. L'anonymisation suppose notamment la suppression irréversible du lien entre les données d'usage et le numéro de série du véhicule, rendant impossible la ré-identification des personnes concernées. À défaut d'anonymisation, l'intérêt légitime peut constituer une base légale pour l'établissement de statistiques, sous réserve d'une pseudonymisation des données (par exemple, *via* l'utilisation d'un algorithme irréversible de « hachage » avec une clé secrète, ladite clé devant être renouvelée régulièrement, ou l'utilisation de méthodes de chiffrement) et de leur minimisation (par exemple, collecte « physique » des données uniquement lors des contrôles techniques et non à distance, en continu).

- **Pour la finalité 2** (études d'accidentologie), la base légale du traitement est le consentement de la personne concernée.

- **Pour la finalité 3** (exploitation commerciale des données du véhicule) : la base légale du traitement est l'exécution d'un contrat auquel la personne concernée est partie. Cette base légale se matérialise par la souscription du contrat par la personne concernée auprès d'un fournisseur de services pour que ce dernier lui fournisse un service déterminé.

FOCUS

Dans le cas où le fournisseur de services est le constructeur automobile, le consentement devra être recueilli lors de la signature du contrat de prestation, qui devra être distinct du contrat de vente du véhicule. La vente du véhicule ne saurait être subordonnée à la signature du contrat de prestation et à l'acceptation de la collecte des données du véhicule par le constructeur automobile.

- **Pour la finalité 4** (« *eCall* ») : à partir d'avril 2018, la base légale du traitement sera le respect d'une obligation légale, à savoir le 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.

- **Pour la finalité 5** (lutte contre le vol) : la base légale du traitement est le consentement du propriétaire du véhicule ou, le cas échéant, l'exécution d'un contrat.

Le consentement doit être une manifestation de volonté libre, spécifique et informée de la personne à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement (par exemple, case à cocher non pré-cochée, paramétrage de l'ordinateur de bord pour activer une fonction dans le véhicule). La liberté du consentement implique la possibilité de pouvoir le retirer à tout moment, ce dont la personne concernée doit être expressément informée. Le retrait du consentement doit conduire à l'arrêt du traitement. Les données doivent alors être supprimées de la base active, anonymisées ou archivées.

En outre, en application de l'article 1er de la loi Informatique et Libertés, la personne concernée doit être en mesure de décider et de contrôler les usages qui sont faits de ses données personnelles.

Concrètement, le respect de ce droit à l'autodétermination informationnelle implique :

- des paramétrages par défaut protecteurs de la vie privée ;
- la possibilité pour l'usager de modifier aisément ces paramétrages, tout au long du traitement, notamment aux fins d'activer ou de désactiver les services fondés sur le consentement ou l'exécution d'un contrat (par exemple, les offres commerciales personnalisées en fonction de la géolocalisation ou l'assistance dépannage) ;
- le cas échéant, la possibilité pour l'usager d'ajuster la granularité des données collectées au niveau de service demandé, par exemple en accédant à une carte sans être géolocalisé s'il ne souhaite pas être guidé ; et
- la possibilité pour l'usager d'accéder aisément à ces données.

FOCUS

En ce qui concerne les données de géolocalisation, la CNIL rappelle qu'il s'agit de données particulièrement révélatrices des habitudes de vie des personnes concernées. En effet, 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'intérêts du conducteur (les loisirs et, le cas échéant, la religion *via* le lieu de culte ou encore l'orientation sexuelle *via* les endroits fréquentés).

Dès lors, le fournisseur de services doit être particulièrement vigilant à ne collecter les données de localisation que lorsqu'une telle collecte est absolument nécessaire à la finalité du traitement. En particulier, la CNIL rappelle que, lorsqu'il convient de détecter le mouvement de la voiture, l'accéléromètre et le gyromètre suffisent à remplir cette fonction, sans qu'il soit nécessaire de collecter les données de localisation.

De manière générale et sauf obligation légale, la collecte des données de géolocalisation est subordonnée au respect des principes suivants :

- le recueil d'un consentement spécifique, distinct des conditions générales de vente ou d'utilisation, par exemple, sur l'ordinateur de bord ;
- un paramétrage adéquat de la finesse de la géolocalisation par rapport à la finalité du traitement. À titre d'exemple, une application météo ne saurait accéder toutes les secondes à la géolocalisation du véhicule, et ce même avec le consentement de la personne concernée ;
- la possibilité de désactiver la géolocalisation à tout moment ;
- l'activation de la géolocalisation uniquement lorsque l'usager 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'usager de l'activation de la géolocalisation, notamment par le biais d'icônes (par exemple, une flèche qui se déplace à l'écran) ;
- 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 ?) ;
- la définition d'une durée de conservation limitée.

Ces règles ne sont pas applicables à la géolocalisation des véhicules de salariés, pour laquelle des règles spécifiques ont été définies par la CNIL dans la norme simplifiée NS-51 (voir délibération n° 2015-165 du 4 juin 2015 portant adoption d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés).

DONNÉES COLLECTÉES

Seules peuvent être collectées les données personnelles nécessaires à la finalité poursuivie par le traitement. Dans le cas d'un contrat de prestation de service souscrit par la personne, les seules données pouvant être collectées sont celles qui sont indispensables à la fourniture du service.

Sur les données relatives aux infractions :

- **Pour les finalités 1** (optimisation de modèles, amélioration du produit) **et 3** (exploitation commerciale des données du véhicule) : sauf disposition légale spécifique, les données relatives aux infractions ne sauraient être traitées par des personnes morales ne gérant pas de service public, sauf pour la défense de leurs droits en justice. Le traitement de ces données pourra en revanche être effectué en local, directement dans le véhicule, conformément au scénario n° 1, de façon à donner à l'usager la maîtrise sur ces données particulièrement sensibles et à limiter autant que possible les conséquences sur la vie privée.

- **Pour la finalité 2** (études d'accidentologie) : 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.

De manière générale, la CNIL estime pertinent de ne conserver que les enregistrements des 45 secondes précédant l'événement ou la séquence de référence et des 15 secondes après l'événement ou la séquence de référence.

Précision : la Commission considère que la vitesse instantanée n'est pas une donnée d'infraction par nature en ce qu'elle ne suffit pas à elle seule à établir une infraction : pour déduire une infraction de la vitesse instantanée, il est nécessaire d'associer la vitesse instantanée à la localisation du véhicule, les limites de vitesse variant en fonction du lieu (ville, route nationale, autoroute, etc.). En revanche, la vitesse instantanée constitue une donnée d'infraction par destination, c'est-à-dire qu'elle est susceptible d'entrer dans le champ de l'article 9 de la loi du 6 janvier 1978 modifiée, en raison des finalités pour lesquelles elle est collectée. S'agissant du cas précis de recherches scientifiques liées à l'accidentologie, la Commission considère que la vitesse instantanée ne constitue pas une donnée d'infraction par destination, ce qui justifie la collecte de la vitesse instantanée par des personnes morales ne gérant pas de service public au sens strict.

Sur les données de localisation :

- **Pour la finalité 1** (optimisation de modèles, amélioration du produit), le traitement d'une géolocalisation précise et détaillée apparaît excessif au sens de l'article 6-3° de la loi Informatique et Libertés.

- **Pour les finalités 3** (exploitation commerciale des données du véhicule) **et 8** (lutte contre le vol), les données de localisation ne peuvent être collectées en continu mais uniquement lorsque le client active le service. Par exemple, pour le service d'assistance dépannage, les données de localisation ne peuvent être remontées qu'à partir du moment où le client effectue une demande d'intervention. De même, pour la finalité 5 (lutte contre le vol), les données de localisation ne peuvent être remontées qu'à partir de la déclaration de vol et ne sauraient être collectées en continu le reste du temps.

DURÉE DE CONSERVATION

- **Pour la finalité 1** (optimisation de modèles, amélioration du produit) : en cas de pseudonymisation, la loi Informatique et Libertés continue de s'appliquer et les données ne peuvent être conservées sans limitation de durée. Dans ce cas, une durée de conservation de 3 ans semble proportionnée par rapport à la finalité poursuivie. Il est rappelé que la géolocalisation précise et détaillée est expressément exclue du champ des données pouvant être traitées pour la finalité 1 (optimisation de modèles, amélioration du produit). Une fois anonymisées, les données d'usage peuvent être conservées pour une durée illimitée.

- **Pour la finalité 2** (études d'accidentologie) : il convient de distinguer deux types de données :
  - **Les données relatives aux participants et aux véhicules :** ces données peuvent être conservées pendant la durée de l'étude.
  - **Les données techniques issues des véhicules :** la CNIL recommande que la conservation de ces données n'excède pas 5 ans à compter de la date de fin de l'étude. À l'issue de cette durée, les données doivent être supprimées ou anonymisées.

- **Pour la finalité 3** (exploitation commerciale des données du véhicule), nécessitant la conclusion d'un contrat de prestation de service, il convient de distinguer deux types de données :
  - **Les données commerciales (identité de la personne, données relatives aux transactions, aux moyens de paiement, etc.) :** ces données peuvent être conservées en base active pendant toute la durée du contrat. A l'issue du contrat, elles peuvent faire l'objet d'un archivage physique (sur support distinct : cédérom, etc.) ou logique (par gestion des habilitations) pour prévenir d'éventuels contentieux. Puis, à l'issue des durées de prescription légale, les données doivent être supprimées ou anonymisées.
  - **Les données d'usage :** ces données doivent être conservées pendant une durée limitée sous forme détaillée, puis doivent être agrégées pour le reste de la durée du contrat.

- **Pour la finalité 4** (« *eCall* ») : le règlement UE 2015/758 du 29 avril 2015 prévoit que les données ne sont pas conservées plus longtemps qu'il n'est nécessaire aux fins de traitement des situations d'urgence. Ces données doivent être totalement

effacées lorsqu'elles ne sont pas nécessaires à cette fin. En outre, dans la mémoire interne du système « *eCall* », les données doivent être automatiquement effacées. Seules les trois dernières positions du véhicule peuvent être 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.

- **Pour la finalité 5** (lutte contre le vol) : 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.

DESTINATAIRES ET SOUS-TRAITANTS

En principe, peuvent seuls avoir accès aux données le responsable de traitement et la personne concernée. Cependant, le responsable de traitement peut être amené à transmettre les données de la personne à un sous-traitant ou à un partenaire commercial (destinataire).

- **Transmission des données à un sous-traitant :** le fournisseur de services peut librement transmettre des données personnelles au sous-traitant auquel il fait appel pour participer à la fourniture du service à la personne concernée, sans que le sous-traitant exploite les données pour son propre compte. Dans cette hypothèse, le fournisseur de services, en tant que responsable de traitement, reste responsable des conditions de traitement des données par son sous-traitant.

- **Transmission des données à un partenaire commercial :**

  - **Si les données transmises sont des données anonymes :** le fournisseur de services peut librement transmettre les données à un partenaire commercial. Ni le fournisseur de services, ni le partenaire commercial n'ont alors d'obligation au regard de la loi Informatique et Libertés ou de règlement général sur la protection des données, ceux-ci n'étant pas applicables aux données anonymes ;
  - **Si les données transmises sont des données personnelles :** au regard de la sensibilité que peuvent présenter les données d'usage du véhicule (trajets effectués, style de conduite, etc.), la CNIL recommande de recueillir systématiquement le consentement de la personne avant toute transmission de ses données à un partenaire commercial (par exemple, *via* une case à cocher non pré-cochée ou, lorsque cela est techniquement possible, *via* un dispositif physique ou logique accessible du véhicule par la personne). Le partenaire commercial devient à son tour responsable de traitement pour le traitement des données qui lui sont transmises et est soumis à l'ensemble des dispositions de la loi Informatique et Libertés et du règlement général sur la protection des données.

- **Pour la finalité 3** (exploitation commerciale des données du véhicule) : la CNIL recommande que, dans la mesure du possible, les données d'usage du véhicule soient traitées directement dans les boîtiers télématiques, afin que le fournisseur de services n'accède qu'aux seules données de résultats (par exemple, un score) et non aux données brutes détaillées.

- **Pour la finalité 5** (lutte contre le vol) : en cas de déclaration de vol, les données de localisation peuvent être transmises aux (i) agents habilités de la plateforme de télésurveillance et (ii) aux autorités légalement habilitées.

INFORMATION DES PERSONNES

La personne doit être informée, préalablement à la mise en œuvre du traitement, de l'identité du responsable de traitement, de la finalité du traitement, des destinataires des données, de la durée de conservation des données, ainsi que des droits dont elle dispose au titre de la loi Informatique et Libertés.

- **Pour les finalités 1** (optimisation de modèles, amélioration du produit), **3** (exploitation commerciale des données du véhicule) et **5** (lutte contre le vol) : cette information pourra être effectuée lors de la signature du contrat.

- **Pour la finalité 2** (études d'accidentologie), en cas de collecte de données relatives aux infractions, il est nécessaire d'informer spécifiquement les personnes concernées de leur collecte. Cette information pourra être effectuée au moment de la signature du formulaire d'accord de participation à l'étude d'accidentologie.

- **Pour la finalité 4** (« *eCall* »), le règlement UE 2015/758 du 29 avril 2015 prévoit que les constructeurs fournissent, dans le manuel de l'usager, des informations claires et complètes sur le traitement des données effectué par

l'intermédiaire du système « *eCall* ».

Ces informations comprennent :

- la référence à la base juridique du traitement ;
- le fait que le système « *eCall* » est activé par défaut ;
- les modalités du traitement des données effectué par le système « *eCall* » ;
- le but spécifique du traitement « *eCall* », qui est limité aux situations d'urgence ;
- les types de données collectées et traitées, ainsi que les destinataires de ces données ;
- le délai de conservation des données dans le système « *eCall* » ;
- 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 « *eCall* » pris en charge par des services tiers et / ou d'autres services à valeur ajoutée, laquelle est soumise à l'accord explicite du propriétaire et est conforme à la directive 95/46/CE. 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 « *eCall* » embarqués pris en charge par des services tiers ou d'autres services à valeur ajoutée.

Le règlement UE 2015/758 du 29 avril 2015 prévoit que ces informations doivent être fournies dans un manuel du propriétaire séparément de celles relatives aux systèmes d' « *eCall* » pris en charge par des services tiers, et ce avant que le système soit utilisé.

En outre, en application du règlement général sur la protection des données, le fournisseur de services devra également informer les personnes concernées des éléments suivants, en des termes clairs, simples et aisément accessibles :

- les coordonnées du délégué à la protection des données ;
- la mention explicite des intérêts légitimes poursuivis lorsque ces derniers constituent la base juridique du traitement ;
- du droit de demander l'effacement des données ou une limitation du traitement relatif à la personne concernée ;
- le droit à la portabilité des données ;
- du droit de retirer son consentement à tout moment ;
- du droit d'introduire une réclamation auprès de la CNIL ;
- des informations sur la question de savoir si l'exigence de fourniture de données personnelles 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 personnelles, ainsi que les conséquences éventuelles de la non-fourniture de ces données ;
- l'existence d'une prise de décision automatisée, y compris un profilage produisant des effets juridiques ou l'affectant de manière significative de façon similaire et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

De plus, en application du règlement général sur la protection des données, lorsque les données n'ont pas été collectées directement par le responsable de traitement, le fournisseur de services devra également indiquer, en plus des informations mentionnées ci-dessus, la source auprès de laquelle il a obtenu ces données et, le cas échéant, si ces données étaient publiquement accessibles. Ces informations devront être communiquées dans une période raisonnable après l'obtention des données et au plus tard à la première des dates suivantes : (i) un mois après l'obtention des données, eu égard aux circonstances particulières dans lesquelles les données sont traitées, (ii) lors de la première communication avec la personne concernée ou (iii) en cas de communication de ces données à un tiers, avant une telle communication.

Ces informations pourront être fournies accompagnées d'icônes normalisées, afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible, du traitement prévu.

Précision : les informations destinées aux personnes concernées peuvent être fournies par strates, c'est-à-dire en dissociant deux niveaux d'information : d'une part, les informations de premier niveau, qui sont les plus importantes pour les personnes, d'autre part, les informations qui ne présentent vraisemblablement d'intérêt qu'en seconde intention. Parmi les informations essentielles de premier niveau figurent, outre l'identité du responsable de traitement, les finalités du traitement et toute information supplémentaire nécessaire afin de garantir un traitement loyal de l'information vis-à-vis des personnes concernées (voir avis n° 10/2004 sur les « *dispositions davantage harmonisées en matière d'information* » rendu par le G29 le 25 novembre 2004).

La Commission recommande que les personnes concernées soient informées :

- par le biais de clauses, concises et aisément compréhensibles, figurant dans le contrat de vente du véhicule et / ou de prestation de services ; et
- par le biais de documents distincts (par exemple, le carnet d'entretien ou le manuel du véhicule) ou de l'ordinateur de bord ; et
- par le recours à des icônes normalisées à l'intérieur des véhicules. La Commission encourage fortement la mise en place de ces icônes, afin d'informer les personnes concernées de manière claire, synthétique et facilement compréhensible du traitement de leurs données. De plus, la Commission insiste sur l'importance de l'harmonisation de ces icônes, de façon à ce que l'usager retrouve les mêmes symboles quelle que soit la marque ou le modèle du véhicule.

DROITS DES PERSONNES

La personne concernée dispose des droits d'accès, d'opposition et de rectification de ses données. Le fournisseur de services doit permettre à la personne d'exercer son droit d'accès de la façon la plus efficace possible, sachant que l'intégralité des données personnelles que détient le fournisseur de services est concernée par ce droit.

• **Pour la finalité 1** (optimisation de modèles, amélioration du produit), lorsque la base légale du traitement est l'intérêt légitime du responsable de traitement, la personne concernée dispose également, en application de l'article 21 du règlement général sur la protection des données, du droit de s'opposer à tout moment au traitement pour des raisons tenant à sa situation particulière. Dans ce cas, le responsable de traitement doit cesser de traiter les données personnelles de la personne concernée, à moins de prouver l'existence de motifs légitimes impérieux pour le traitement, qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.

Outre les droits mentionnés ci-dessus, le règlement général sur la protection des données instaure trois nouveaux droits, à savoir le droit à l'oubli, le droit à la portabilité et le droit à la limitation du traitement (voir l'introduction du pack).

SÉCURITÉ

Le fournisseur de services doit mettre en place des mesures permettant de garantir la sécurité et la confidentialité des données qu'il traite et doit prendre toutes les précautions utiles pour en empêcher la prise de contrôle par une personne non autorisée, notamment en :

- chiffrant le canal de communication avec un algorithme à l'état de l'art ;
- mettant en place une gestion des clés de chiffrement propre à chaque véhicule et non à chaque modèle ;
- chiffrant les données en base avec des algorithmes à l'état de l'art ;
- protégeant les clés de chiffrement de toute divulgation accidentelle ;
- authentifiant les appareils destinataires des données ;
- s'assurant de l'intégrité des données (par exemple par calcul d'empreinte) ;
- subordonnant l'accès aux données personnelles à une authentification fiable de l'utilisateur (mot de passe, certificat électronique, etc.) ;
- appliquant les recommandations de la Commission en date du 22 juin 2017, dans le cas d'une authentification par mot de passe (voir délibération n° 2017-190).

Concernant plus spécifiquement les constructeurs automobiles, la Commission recommande la mise en place des mesures de sécurité suivantes :

- le cloisonnement des fonctions vitales du véhicule par rapport à celles connectées en continu à Internet (« *infotainment* » par exemple) ;
- la mise en place de mesures techniques permettant de corriger rapidement un défaut de sécurité ;
- pour les fonctions vitales du véhicule, privilégier, autant que possible, le recours à des fréquences sécurisées spécifiquement dédiées aux transports ;
- la mise en place d'un système d'alerte en cas d'attaque et la possibilité d'un fonctionnement en mode dégradé ;
- la conservation d'un historique de logs d'une durée de six mois aux fins de permettre de comprendre l'origine de l'attaque.

Les mesures mises en place doivent être adaptées au niveau de sensibilité des données. Ainsi, en cas de collecte de la vitesse instantanée dans le cadre d'études d'accidentologie, la Commission recommande la mise en place de mesures de sécurité fortes, telles que :

- la mise en place 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) ; et
- le stockage des données relatives à la vitesse instantanée et à la géolocalisation dans des bases étanches (par exemple, par l'usage d'un mécanisme de chiffrement à l'état de l'art avec des clés distinctes et de mécanismes d'habilitation) ; ou
- la suppression des données de géolocalisation 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 directement identifiantes dans une base séparée, à laquelle ne pourrait accéder qu'un nombre restreint de personnes.

• **Pour la finalité 1** (optimisation de modèles, amélioration du produit), des mesures d'anonymisation ou a minima de pseudonymisation doivent être mises en place.

• **S'agissant de la finalité 4** (« *eCall* »), le règlement UE 2015/758 du 29 avril 2015 prévoit l'obligation d'intégrer dans le système « *eCall* » des technologies renforçant la protection de la vie privée afin d'offrir aux utilisateurs le niveau de protection de la vie privée approprié, ainsi que les garanties nécessaires pour prévenir la surveillance et les utilisations abusives. En outre, les constructeurs doivent veiller à ce que le système « *eCall* » 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. Concernant les mesures à mettre en place au niveau des infrastructures externes au véhicule, le fournisseur de services doit mener une étude des risques engendrés par le traitement afin de déterminer et de mettre en œuvre les mesures nécessaires à la protection de la vie privée des personnes. La CNIL met à disposition une méthode de ce type sur son site web (https://www.cnil.fr/fr/PIA-privacy-impact-assessment), mais d'autres méthodes équivalentes peuvent être utilisées.

Enfin, le fournisseur de services doit développer ses produits et services en intégrant dès l'origine la problématique des données personnelles (« *privacy by design* »). À tout le moins, le produit ou service doit limiter la sortie du véhicule des données à ce qui est strictement nécessaire à la fourniture du service, et privilégier les décisions prises localement à celles réalisées à l'extérieur du véhicule. Le fournisseur de services doit également favoriser une anonymisation des données le plus tôt possible dans la chaîne de collecte. Dès lors que les données sont anonymes, il est rappelé que la loi Informatique et Libertés et le règlement général sur la protection des données ne s'applique plus et que les données peuvent donc être conservées et échangées de façon illimitée.

FORMALITÉS PRÉALABLES

Le responsable de traitement doit effectuer une déclaration normale auprès de la CNIL, sauf à traiter des données relatives aux infractions, auquel cas une autorisation préalable de la CNIL est nécessaire.

La CNIL considère que les traitements de données personnelles remontées *via* les véhicules connectés peuvent présenter des risques pour le respect de la vie privée au sens du règlement général sur la protection des données. Dès lors, en telle hypothèse, le fournisseur de services devra effectuer une étude d'impact et analyser les risques encourus afin de mettre en œuvre les mesures permettant de les limiter.

De plus, en application de l'article 33 du règlement général sur la protection des données, en cas de violation de données à caractère personnel susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, il appartiendra au responsable de traitement de notifier la violation à la CNIL, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance. En application de l'article 34 du règlement général sur la protection des données, il appartiendra également au responsable de traitement d'en informer les personnes concernées si la violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés.

FOCUS

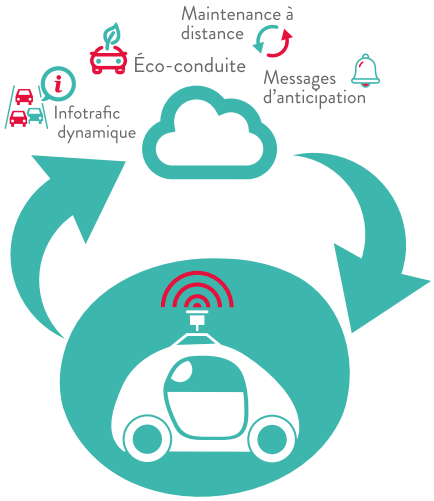
Ce scénario est appelé à être utilisé notamment lorsque le traitement de données personnelles requiert une puissance de calcul ne pouvant être mobilisée en local dans le véhicule, ou lorsque le traitement de données personnelles ne suffit pas en lui-même à la fourniture du service et nécessite de la part du fournisseur de services une analyse complémentaire.

SCÉNARIO N°3
IN → OUT → IN

LES DONNÉES DU VÉHICULE SONT TRANSMISES AU FOURNISSEUR DE SERVICES POUR DÉCLENCHER À DISTANCE UNE ACTION AUTOMATIQUE DANS LE VÉHICULE

PÉRIMÈTRE

Ce scénario couvre les cas dans lesquels les données collectées sont transmises au fournisseur de services pour déclencher à distance une action automatique dans le véhicule.



ANALYSE DES TRAITEMENTS DE DONNÉES PERSONNELLES AU REGARD DE LA LOI INFORMATIQUE ET LIBERTÉS ET DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

La mise en place d'un traitement de données personnelles doit respecter la loi Informatique et Libertés. En effet, toute personne qui souhaite traiter des données personnelles est soumise à un certain nombre d'obligations légales.

FINALITÉS POURSUIVIES PAR LES TRAITEMENTS (LISTE NON EXHAUSTIVE)

• **Finalité 1 : maintenance à distance :** la personne concernée contracte avec un fournisseur de services aux fins de recevoir des messages ou des alertes liés au fonctionnement du véhicule (par exemple, alerte sur l'état d'usage des freins ou rappel de la date de contrôle technique) ou recevoir à distance des mises à jour techniques dans le véhicule.

• **Finalité 2 : amélioration de l'expérience de conduite :** la personne concernée souhaite bénéficier de services aux fins d'améliorer son expérience de conduite (par exemple, infotrafic dynamique avec envoi d'un nouveau parcours suite à un incident sur la route, messages d'anticipation ou alertes d'éco-conduite).

BASE LÉGALE

• **Pour les finalités 1** (maintenance à distance) **et 2** (amélioration de l'expérience de conduite), la base légale du traitement est l'exécution du contrat auquel la personne concernée a choisi de souscrire.

En application de l'article 1er de la loi Informatique et Libertés, la personne concernée doit être en mesure de décider et de contrôler les usages qui sont faits de ses données personnelles.

Concrètement, cette maîtrise implique notamment :

- des paramétrages par défaut protecteurs de la vie privée ;
- la possibilité pour l'usager de modifier aisément ces paramétrages, tout au long du traitement, notamment aux fins d'activer ou de désactiver les services fondés sur le consentement ou l'exécution d'un contrat (par exemple, l'infotrafic dynamique) ;
- le cas échéant, la possibilité pour l'usager d'ajuster la granularité des données collectées au niveau de service demandé, par exemple en accédant à une carte sans être géolocalisé s'il ne souhaite pas être guidé ; et
- la possibilité pour l'usager d'accéder aisément à ces données.

SCÉNARIO N°3 - « IN → OUT → IN » :

Les données du véhicule sont transmises au fournisseur de services pour déclencher à distance une action automatique dans le véhicule

DONNÉES COLLECTÉES

Seules peuvent être collectées les données personnelles nécessaires à la finalité poursuivie par le traitement. Dans le cas d'un contrat de prestation de service souscrit par la personne, les seules données pouvant être collectées sont celles qui sont indispensables à la fourniture du service.

À titre d'exemple, la géolocalisation précise et détaillée ne saurait être traitée pour la finalité 1 (maintenance à distance).

Dans le cadre du présent scénario, sauf disposition légale spécifique, les données relatives aux infractions ne sauraient être traitées par des personnes morales ne gérant pas de service public, sauf pour la défense de leurs droits en justice. Le traitement de ces données peut en revanche être effectué en local, directement dans le véhicule, conformément au scénario n° 1, de façon à donner à l'usager la maîtrise sur ces données particulièrement sensibles et à limiter autant que possible les risques d'impact sur la vie privée.

DURÉE DE CONSERVATION

Il convient de distinguer deux types de données :

- **Les données commerciales (identité de la personne, données relatives aux transactions, aux moyens de paiement, etc.) :** ces données peuvent être conservées en base active pendant toute la durée du contrat. A l'issue du contrat, elles peuvent faire l'objet d'un archivage physique (sur support distinct : cédérom, etc.) ou logique (par gestion des habilitations) pour prévenir d'éventuels contentieux. Puis, à l'issue des durées de prescription légale, les données doivent être supprimées ou anonymisées.
- **Les données d'usage :** ces données doivent être conservées pendant une durée limitée sous forme détaillée, puis doivent être agrégées pour le reste de la durée du contrat. Toutefois, pour la finalité 1 (maintenance à distance), les données relatives aux interventions sur le véhicule peuvent être conservées pendant la durée de vie du véhicule.

DESTINATAIRES ET SOUS-TRAITANTS

En principe, peuvent seuls avoir accès aux données le fournisseur de services et la personne concernée. Cependant, le responsable de traitement peut être amené à transmettre les données de la personne au sous-traitant auquel il fait appel pour participer à l'exécution du service proposé à la personne, sans que ce dernier exploite les données pour son propre compte. Dans cette hypothèse, le fournisseur de services, en tant que responsable de traitement, reste responsable des conditions de traitement des données par son sous-traitant.

INFORMATION DES PERSONNES

La personne doit être informée, préalablement à la mise en œuvre du traitement, de l'identité du responsable de traitement, de la finalité du traitement, des destinataires des données, de la durée de conservation, ainsi que des droits dont elle dispose au titre de la loi Informatique et Libertés. Cette information pourrait être effectuée lors de la signature du contrat de prestation de service par la personne concernée.

En outre, en application du règlement général sur la protection des données, le fournisseur de services devra également informer les personnes concernées des éléments suivants, en des termes clairs, simples et aisément accessibles :

- les coordonnées délégué à la protection des données ;
- la mention explicite des intérêts légitimes poursuivis lorsque ces derniers constituent la base juridique du traitement ;
- le droit de demander l'effacement des données ou une limitation du traitement relatif à la personne concernée ;
- le droit à la portabilité des données ;
- le droit de retirer son consentement à tout moment ;
- le droit d'introduire une réclamation auprès de la CNIL ;
- les informations sur la question de savoir si l'exigence de fourniture de données personnelles 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 personnelles, ainsi que les conséquences éventuelles de la non-fourniture de ces données ;
- l'existence d'une prise de décision automatisée, y compris un profilage produisant des effets juridiques ou l'affectant de manière significative de façon similaire et, au moins en pareils cas, des informations utiles concernant la logique

sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

De plus, lorsque les données n'ont pas été collectées directement par le responsable de traitement, le fournisseur de services devra également indiquer, en plus des informations mentionnées ci-dessus, la source auprès de laquelle il a obtenu ces données et, le cas échéant, si ces données étaient publiquement accessibles. Ces informations devront être communiquées dans une période raisonnable après l'obtention des données et au plus tard à la première des dates suivantes : (i) un mois après l'obtention des données, eu égard aux circonstances particulières dans lesquelles les données sont traitées, (ii) lors de la première communication avec la personne concernée ou (iii) en cas de communication de ces données à un tiers, avant une telle communication.

Précision : les informations destinées aux personnes concernées peuvent être fournies par strates, c'est-à-dire en dissociant deux niveaux d'information : d'une part, les informations de premier niveau, qui sont les plus importantes pour les personnes, d'autre part, les informations qui ne présentent vraisemblablement d'intérêt qu'en seconde intention. Parmi les informations essentielles de premier niveau figurent, outre l'identité du responsable de traitement, les finalités du traitement et toute information supplémentaire nécessaire afin de garantir un traitement loyal de l'information vis-à-vis des personnes concernées (voir avis n° 10/2004 sur les « dispositions davantage harmonisées en matière d'information » rendu par le G29 le 25 novembre 2004).

La Commission recommande que les personnes concernées soient informées :

- par le biais de clauses, concises et aisément compréhensibles, figurant dans le contrat de vente du véhicule et / ou de prestation de services ; et
- par le biais de documents distincts (par exemple, le carnet d'entretien ou le manuel du véhicule) ou sur l'ordinateur de bord ; et
- par le recours à des icônes normalisées à l'intérieur des véhicules. La Commission encourage fortement la mise en place de ces icônes, afin d'informer les personnes concernées de manière claire, synthétique et facilement compréhensible du traitement de leur données. De plus, la Commission insiste sur l'importance de l'harmonisation de ces icônes, de façon à ce que l'usager retrouve les mêmes symboles quelle que soit la marque ou le modèle du véhicule.

DROITS DES PERSONNES

La personne concernée dispose des droits d'accès, d'opposition et de rectification de ses données. Le fournisseur de services doit permettre à la personne d'exercer son droit d'accès de la façon la plus efficace possible, sachant que l'intégralité des données personnelles que détient le fournisseur de services est concernée par ce droit.

Outre les droits mentionnés ci-dessus, le règlement général sur la protection des données instaure trois nouveaux droits, à savoir le droit à l'oubli, le droit à la portabilité et le droit à la limitation du traitement (voir l'introduction du pack).

SÉCURITÉ

Le fournisseur de services doit mettre en place des mesures permettant de garantir la sécurité et la confidentialité des données qu'il traite et doit prendre toutes les précautions utiles pour en empêcher la prise de contrôle par une personne non autorisée, notamment en :

- chiffrant le canal de communication avec un algorithme à l'état de l'art ;
- mettant en place une gestion des clés de chiffrement propre à chaque véhicule et non à chaque modèle ;
- chiffrant les données en base avec des algorithmes à l'état de l'art ;
- protégeant les clés de chiffrement de toute divulgation accidentelle ;
- authentifiant les appareils destinataires des données ;
- subordonnant l'accès aux données personnelles à une authentification fiable de l'utilisateur (mot de passe, certificat électronique, etc.) ;
- authentifiant les appareils émetteurs d'actions à destination du véhicule ;
- appliquant les recommandations de la Commission en date du 22 juin 2017, dans le cas d'une authentification par mot de passe (voir délibération n° 2017-190).

SCÉNARIO N°3 - « IN → OUT → IN » :

Les données du véhicule sont transmises au fournisseur de services pour déclencher à distance une action automatique dans le véhicule

Concernant plus spécifiquement les constructeurs automobiles, la Commission recommande la mise en place des mesures de sécurité suivantes :

- le cloisonnement des fonctions vitales du véhicule par rapport à celles connectées en continu à Internet (« *infotainment* » par exemple) ;
- la mise en place de mesures techniques permettant de corriger rapidement un défaut de sécurité ;
- pour les fonctions vitales du véhicule, privilégier, autant que possible, le recours à des fréquences sécurisées spécifiquement dédiées aux transports ;
- la mise en place d'un système d'alerte en cas d'attaque et la possibilité d'un fonctionnement en mode dégradé ;
- la conservation d'un historique de logs d'une durée de six mois aux fins de permettre de comprendre l'origine de l'attaque.

Les mesures mises en place doivent être adaptées au niveau de sensibilité des données et aux capacités de contrôle des appareils.

Concernant les mesures à mettre en place au niveau des infrastructures externes au véhicule, le fournisseur de services doit mener une étude des risques engendrés par le traitement afin de déterminer et de mettre en œuvre les mesures nécessaires à la protection de la vie privée des personnes. La CNIL met à disposition une méthode de ce type sur son site web (https://www.cnil.fr/fr/PIA-privacy-impact-assessment), mais d'autres méthodes équivalentes peuvent être utilisées.

Enfin, le fournisseur de services doit développer ses produits et services en intégrant dès l'origine la problématique des données personnelles (« *privacy by design* »). À tout le moins, le produit ou service doit limiter la sortie du véhicule des données à ce qui est strictement nécessaire à la fourniture du service, et privilégier les décisions prises localement à celles réalisées à l'extérieur du véhicule. Le fournisseur de services doit également favoriser une anonymisation des données le plus tôt possible dans la chaîne de collecte. Il est rappelé que, dès lors que les données sont anonymes, la loi Informatique et Libertés et le règlement général sur la protection des données ne s'appliquent plus et les données peuvent donc être conservées et échangées de façon illimitée.

FORMALITÉS PRÉALABLES

Le fournisseur de services doit effectuer une déclaration normale auprès de la CNIL. Cette déclaration doit être effectuée sur le site de la CNIL (https://www.cnil.fr/).

La CNIL considère que les traitements de données personnelles remontées *via* les véhicules connectés peuvent présenter des risques pour le respect de la vie privée au sens du règlement général sur la protection des données. Dès lors, en telle hypothèse, le fournisseur de services devra effectuer une étude d'impact et analyser les risques encourus afin de mettre en œuvre les mesures permettant de les limiter.

De plus, en application de l'article 33 du règlement général sur la protection des données, en cas de violation de données à caractère personnel susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, il appartiendra au responsable de traitement de notifier la violation à la CNIL, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance. En application de l'article 34 du règlement général sur la protection des données, il appartiendra également au responsable de traitement d'en informer les personnes concernées si la violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés.

FOCUS

Ce scénario est appelé à être utilisé notamment lorsque le traitement de données personnelles requiert une puissance de calcul ne pouvant être mobilisée en local dans le véhicule, ou lorsque la fourniture du service requiert des données complémentaires, extérieures au véhicule.