REFERENTIEL

RELATIF AUX TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL MIS EN ŒUVRE POUR LA GESION DU CONTENTIEUX LIE AU RECOUVREMENT DES CONTRAVENTIONS AU CODE DE LA ROUTE ET A L'IDENTIFICATION DES CONDUCTEURS DANS LE CADRE DU SYSTEME DE CONTROLE AUTOMATISE DES INFRACTIONS AU CODE DE LA ROUTE

Mise à jour de l'autorisation unique AU-010

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. A qui s'adresse le référentiel ?

Ce référentiel encadre les traitements relatifs à l'identification des conducteurs dans le cadre de la gestion du contentieux lié au recouvrement des contraventions au code de la route.

Il s'adresse principalement aux employeurs de droit public ou privé mettant à disposition de leurs salariés des véhicules ainsi qu'aux loueurs de véhicules courte et longue durée (ci-après « les organismes »).

Le terme « loueurs de véhicule » désigne l'ensemble des organismes offrant, à titre d'activité principale ou accessoire, un service de mise à disposition de véhicules en échange d'un loyer, et ce quelle qu'en soit la durée. Peuvent ainsi être considérés comme loueurs de véhicule les constructeurs automobiles, les sociétés bancaires et les établissements de crédit proposant un tel service.

2. Portée du référentiel

Les traitements visant à identifier et désigner le conducteur en cas d'infraction routière *via* le système de contrôle automatisé des infractions conduisent à collecter des données à caractère personnel relatives aux salariés et locataires de véhicule. A ce titre, ils sont soumis aux dispositions du Règlement général sur la protection des données (RGPD), de la loi du 6 janvier 1978 modifiée (LIL) ainsi qu'aux dispositions spécifiques relatives aux relations de travail (code du travail).

Les organismes concernés, en tant que responsables de traitement, doivent mettre en œuvre toutes les mesures techniques et organisationnelles appropriées afin de garantir un haut niveau de protection des données personnelles dès la conception des traitements et tout au long de la vie de ceux-ci. Ils doivent, en outre, être en mesure de démontrer cette conformité à tout instant. Les traitements mis en œuvre doivent être inscrits dans le registre prévu à l'article 30 du RGPD (voir les modèles de registre sur le site cnil.fr).

L'application de ce référentiel permet d'assurer la conformité des traitements mis en œuvre dans le cadre du système de contrôle automatisé des infractions au code de la route, aux principes relatifs à la protection des données.
Les organismes qui s'écarteraient du référentiel au regard des conditions particulières tenant à leur situation doivent être en mesure de justifier l'existence d'un tel besoin puis, de prendre toutes les mesures appropriées à même de garantir la conformité de ces traitements à la réglementation en matière de protection des données à caractère personnel.

Ce référentiel constitue également une aide à la réalisation d'une analyse d'impact relative à la protection des données (AIPD). Les organismes pourront ainsi définir les mesures permettant d'assurer la proportionnalité et la nécessité de leurs traitements (points 3 à 7), de garantir les droits des personnes (points 8 et 9) ainsi que la maîtrise de leurs risques (point 10). À cette fin, l'organisme pourra se référer aux lignes directrices de la CNIL sur les analyses d'impact relatives à la protection des données (AIPD).

Le présent référentiel ne porte pas sur la gestion du forfait post-stationnement dont la procédure de paiement ne prévoit pas la désignation du conducteur pour exonérer de paiement le titulaire du certificat d'immatriculation.
Les loueurs longue-durée recevant des Forfaits Post Stationnement (FPS) peuvent les contester au moyen d'un Recours Administratif Préalable Obligatoire (RAPO) ou se retourner contre le locataire pour recouvrer la somme après règlement du forfait : ils pourront dans ce dernier cas recourir à ce référentiel pour la démarche de contestation.

3. Objectifs poursuivis par le traitement (finalités)

Le traitement mis en œuvre doit répondre à un objectif déterminé, explicite et légitime et être justifié par les missions et les activités de l'organisme.

En ce qui concerne le dispositif d'identification du conducteur, le traitement est mis en œuvre afin :

- de **désigner auprès de l'Agence Nationale de Traitement Automatisé des Infractions (ANTAI) la personne** qui conduisait ou était susceptible de conduire le véhicule lorsque l'infraction a été constatée ;
- de **suivre la procédure** de recouvrement des contraventions au code de la route dont peuvent être redevables pécuniairement les organismes publics ou privés susvisés ;
- et de **réaliser des statistiques anonymes** en vue d'adapter les formations de prévention routière.

Les informations recueillies pour l'une de ces finalités ne peuvent pas être réutilisées pour poursuivre un autre objectif qui serait incompatible avec la finalité initiale.
Tout nouvel usage des données doit en effet respecter les principes de protection des données à caractère personnel. Les traitements mis en œuvre ne doivent pas donner lieu à des interconnexions ou échanges autres que ceux nécessaires à l'accomplissement des finalités ci-dessus énoncées.

4. Base(s) légale(s) du traitement

Chaque finalité du traitement doit reposer sur l'une des « bases légales » prévues par la réglementation.
Dans le cadre du présent traitement, cette base légale est le respect d'une obligation légale à laquelle est soumis le responsable de traitement.

L'article L121-6 du code de la route impose en effet aux organismes de désigner le conducteur ayant commis une infraction au code de la route.

En revanche, pour la réalisation de statistiques anonymes, la base légale est la réalisation de l'intérêt légitime poursuivi par l'organisme ou par un tiers, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

5. Données personnelles concernées

5.1 Principe de pertinence, de loyauté et de minimisation des données

Dans un souci de minimisation des données personnelles traitées, l'organisme doit veiller à ne collecter et n'utiliser que les données pertinentes et strictement nécessaires au regard de ses besoins de traitement des signalements.

A cet égard, pour le présent traitement, les seules données pouvant être transmises à l'ANTAI dans le cadre de la procédure de désignation sont :
- le nom, nom d'usage, prénom(s), sexe et, le cas échéant, civilité de la personne ;
- la date et le lieu de naissance ;
- l'adresse postale et, le cas échéant, l'adresse électronique ;
- le numéro d'immatriculation du véhicule concerné ;
- le nom, prénom et coordonnées du responsable de traitement et, le cas échéant, d'un contact au sein de l'organisme concerné ;
- le numéro et la date de l'avis de contravention ;
- le cas échéant, la date et l'heure du début de location et de la fin ;
- le cas échéant, la date et l'heure de l'infraction.

Les seules données à caractère personnel traitées par le responsable de traitement au titre du suivi de la procédure de recouvrement des contraventions au code de la route sont :
- le numéro, la date et l'heure du contrat de location ou de mise à disposition du véhicule ;
- l'éventuel numéro de dossier communiqué par l'ANTAI ;
- le montant de la contravention.

La copie du permis de conduire ne saurait être collectée par le responsable de traitement pour l'une des finalités précitées.

5.2 Exactitude et mise à jour des données

Le responsable de traitement doit veiller à l'exactitude des données traitées, et les mettre à jour si nécessaire. Les données obsolètes et inexactes doivent être supprimées du traitement, sauf lorsque la finalité du traitement rend nécessaire leur conservation.

6. Durées de conservation

Les informations ne peuvent être conservées de façon indéfinie dans les traitements : une durée de conservation précise doit être préalablement fixée en fonction de la finalité du ou des traitement(s).

Dans le cadre de la procédure de désignation, le responsable de traitement peut conserver dans la base active les données précitées le temps de procéder à la désignation, c'est-à-dire pendant une durée ne pouvant excéder **quarante-cinq (45) jours** à compter de la réception de la contravention.

A l'issue de cette période, les données peuvent être archivées, en archivage intermédiaire, au maximum le temps de la prescription en matière contraventionnelle, à savoir **douze (12) mois**.

Les données doivent par la suite être supprimées ou anonymisées.

Dans l'hypothèse d'une désignation automatisée et de la conclusion d'une convention avec l'ANTAI, les traces des requêtes effectuées par l'ANTAI sur les conducteurs de véhicules ayant commis une infraction au code de la route sont détruites après le retour d'information à l'ANTAI. Les organismes publics et privés ne peuvent garder trace de ces requêtes.

Pour en savoir plus, vous pouvez vous référer aux guides de la CNIL :
« Sécurité : Archiver de manière sécurisée » ;
« Limiter la conservation des données ».

Les données utilisées à des fins statistiques ne sont plus qualifiées de données à caractère personnel dès lors qu'elles ont été dûment anonymisées. La réglementation en matière de protection des données ne s'applique en effet qu'aux seules « *données à caractère personnel* ».

Lorsqu'un ensemble de données est purgé de tout élément permettant de réidentifier directement ou indirectement les personnes concernées, les données, désormais anonymisées échappent à la réglementation relative à la protection des données. Elles peuvent ainsi être conservées et traitées sans limitation de durée.

Pour aller plus loin : voir les lignes directrices du CEPD sur l'anonymisation (avis 05/2014).

7. Information des personnes

Les principes de transparence et de loyauté du traitement prévoient que les personnes concernées soient informées individuellement au moment de leur collecte, des caractéristiques du traitement de leurs données ainsi que des modalités d'exercice de leurs droits dans les conditions prévues par les articles 12, 13 et 14 du RGPD (voir les exemples de mentions d'information).

L'information peut être délivrée par l'organisme par tout moyen, par exemple par la remise d'un document écrit, y compris par voie électronique.

L'employeur peut, par exemple, rappeler ces informations dans la charte définissant les conditions d'utilisation du véhicule ou dans la charte informatique de l'entreprise. Les instances représentatives du personnel doivent par ailleurs être informées et consultées dans le cadre prévu par la législation sociale applicable.

8. Droits des personnes

Le RGPD reconnait aux personnes concernées différents droits, dont l'exercice est conditionné par la base légale retenue (voir la rubrique qui s'intitule « respecter les droits des personnes » sur le site de la CNIL). L'information délivrée aux personnes doit préciser la base légale et les droits associés.

Le traitement de données relatif à la gestion du contentieux lié au recouvrement des contraventions au code de la route et à l'identification des conducteurs dans le cadre du système de contrôle automatisé des infractions au code de la route est nécessaire au respect d'une obligation légale. Les personnes concernées disposent par conséquent :

- **des droits d'accès, de rectification et à l'effacement** des données qui les concernent ;
- de la **limitation** du traitement (par exemple, lorsque la personne conteste l'exactitude de ses données, elle peut demander par ailleurs le gel temporaire du traitement des données le temps que l'organisme procède aux vérifications nécessaires).

Dans le cadre de la réalisation de statistiques anonymes en vue d'adapter les formations de prévention routière, le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement. Par conséquent, les personnes concernées disposent :

- de la possibilité de **s'opposer préalablement au traitement** de leurs données en application de l'article 21 du RGPD.

9. Confidentialité des données

Le responsable de traitement doit préserver la confidentialité des données et empêcher que des tiers non autorisés y aient accès.

9.1 Les personnes accédant aux données pour le compte de l'organisme

Seules les personnes habilitées au titre de leurs missions ou de leurs fonctions doivent pouvoir accéder aux données à caractère personnel traitées, et ce, dans la stricte limite de leurs attributions respectives, de l'accomplissement de leurs missions ou de l'exercice de leurs fonctions.

Les habilitations d'accès doivent être documentées, et les accès aux différents traitements doivent faire l'objet de mesures de traçabilité (par exemple au travers de journaux d'événements). **Voir point 9 relatif à la sécurité.**

Dans le cas d'un employeur, il peut s'agir, par exemple des personnes habilitées chargées de la gestion administrative du personnel.

9.2 Les destinataires des données

Le RGPD définit le destinataire comme *« la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers »*.

Pour le présent traitement, les destinataires des données à caractère personnel sont l'ANTAI ainsi que l'officier du ministère public.

9.3 Les sous-traitants

Le responsable de traitement qui souhaite avoir recours à un sous-traitant doit veiller à ne faire appel qu'à des organismes présentant des garanties suffisantes. Un contrat définissant les caractéristiques du traitement ainsi que les différentes obligations des parties en matière de protection des données doit être établi entre elles (article 28 du RGPD). Un guide du sous-traitant édité par la CNIL, rappelle ces obligations ainsi que les clauses à intégrer dans les contrats.

10. Sécurité

L'organisme doit prendre toutes les précautions utiles au regard des risques présentés par son traitement pour préserver la sécurité des données à caractère personnel et, notamment au moment de leur collecte, durant leur transmission et leur conservation, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

En particulier, dans le contexte spécifique du présent référentiel, **soit l'organisme adopte les mesures suivantes, soit il justifie de leur équivalence ou du fait de ne pas avoir besoin ou pouvoir y recourir** :

Catégories	Mesures
Sensibiliser les utilisateurs	Informer et sensibiliser les personnes manipulant les données
	Rédiger une charte informatique et lui donner une force contraignante
Authentifier les utilisateurs	Définir un identifiant (*login*) unique à chaque utilisateur
	Adopter une politique de mots de passe utilisateur conforme aux recommandations de la CNIL
	Obliger l'utilisateur à changer son mot de passe après réinitialisation
	Limiter le nombre de tentatives d'accès à un compte
Gérer les habilitations	Définir des profils d'habilitation
	Supprimer les permissions d'accès obsolètes
	Réaliser une revue annuelle des habilitations
Tracer les accès et gérer les incidents	Prévoir un système de journalisation
	Informer les utilisateurs de la mise en place du système de journalisation
	Protéger les équipements de journalisation et les informations journalisées
	Prévoir les procédures pour les notifications de violation de données à caractère personnel
Sécuriser les postes de travail	Prévoir une procédure de verrouillage automatique de session
	Utiliser des antivirus régulièrement mis à jour
	Installer un « pare-feu » (*firewall*) logiciel
	Recueillir l'accord de l'utilisateur avant toute intervention sur son poste
Sécuriser l'informatique mobile	Prévoir des moyens de chiffrement des équipements mobiles
	Faire des sauvegardes ou des synchronisations régulières des données
	Exiger un secret pour le déverrouillage des *smartphones*
Protéger le réseau informatique interne	Limiter les flux réseau au strict nécessaire
	Sécuriser les accès distants des appareils informatiques nomades par VPN
	Mettre en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi
Sécuriser les serveurs	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées
	Installer sans délai les mises à jour critiques
	Assurer une disponibilité des données
Sécuriser les sites web	Utiliser le protocole TLS et vérifier sa mise en œuvre
	Vérifier qu'aucun mot de passe ou identifiant ne passe dans les url
	Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu
	Mettre un bandeau de consentement pour les *cookies* non nécessaires au service
Sauvegarder et prévoir la continuité d'activité	Effectuer des sauvegardes régulières
	Stocker les supports de sauvegarde dans un endroit sûr
	Prévoir des moyens de sécurité pour le convoyage des sauvegardes
	Prévoir et tester régulièrement la continuité d'activité
Archiver de manière sécurisée	Mettre en œuvre des modalités d'accès spécifiques aux données archivées
	Détruire les archives obsolètes de manière sécurisée
Encadrer la maintenance et la destruction des données	Enregistrer les interventions de maintenance dans une main courante
	Encadrer par un responsable de l'organisme les interventions par des tiers
	Effacer les données de tout matériel avant sa mise au rebut
Gérer la sous-traitance	Prévoir une clause spécifique dans les contrats des sous-traitants
	Prévoir les conditions de restitution et de destruction des données
	S'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, *etc.*)
	Chiffrer les données avant leur envoi

Catégories	Mesures
Sécuriser les échanges avec d'autres organismes	S'assurer qu'il s'agit du bon destinataire
	Transmettre le secret lors d'un envoi distinct et via un canal différent
Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées
	Installer des alarmes anti-intrusion et les vérifier périodiquement
Encadrer les développements informatiques	Proposer des paramètres respectueux de la vie privée aux utilisateurs finaux
	Éviter les zones de commentaires ou les encadrer strictement
	Tester sur des données fictives ou anonymisées
Utiliser des fonctions cryptographiques	Utiliser des algorithmes, des logiciels et des bibliothèques reconnus
	Conserver les secrets et les clés cryptographiques de manière sécurisée

Pour ce faire, le responsable de traitement pourra utilement se référer au guide de la sécurité des données personnelles.

11. Analyse d'impact relative à la protection des données

En application des dispositions de l'article 35 du RGPD, le responsable de traitement doit réaliser une analyse d'impact relative à la protection des données (AIPD) dès lors que son traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes.

Pour porter cette appréciation, il pourra se référer d'une part aux lignes directrices concernant l'AIPD établies par le Comité européen de la protection des données (CEPD), et d'autre part, à la liste adoptée par la CNIL relative aux types d'opérations de traitement pour lesquelles une AIPD est requise.

Aussi, une analyse d'impact sera obligatoire :
- si le traitement envisagé figure dans la liste des types d'opérations de traitement pour lesquelles la CNIL a estimé obligatoire de réaliser une AIPD, ou ;
- si le traitement remplit au moins deux des neuf critères issus des lignes directrices du CEPD.

Dès lors qu'il est mis en œuvre par un employeur de moins de 250 salariés, ce traitement figure sur la liste des types d'opérations de traitement pour lesquels aucune AIPD n'est requise.

S'il est, en revanche, mis en œuvre par un employeur de plus de 250 salariés ou par un loueur de dans le cadre d'un traitement à grande échelle, le traitement doit faire l'objet d'une analyse d'impact dans la mesure où il remplit au moins deux des neufs critères établis par le CEPD et plus particulièrement ceux relatifs :

- aux données à caractère personnel relatives aux condamnations pénales ou aux infractions ;
- aux personnes vulnérables (salariés) ;
- à la large échelle.

Pour réaliser une analyse d'impact, le responsable de traitement pourra se reporter :
- aux principes contenus dans ce référentiel ;
- aux outils méthodologiques proposés par la CNIL sur son site web.

Si l'organisme en a désigné, le délégué à la protection des données (DPO) devra être consulté.

Conformément à l'article 36 du RGPD, l'AIPD doit être transmise à la CNIL dans les cas suivants :
- s'il apparaît que le niveau de risque résiduel reste élevé malgré les mesures ;
- quand la législation nationale d'un État membre l'exige ;
- en cas de demande de la CNIL.

ILLUSTRATION PRATIQUE DES DROITS		
Finalités de traitement	Bases légales	Droits de la personne concernée
Désignation auprès de l'ANTAI de la personne qui conduisait ou était susceptible de conduire	Respect d'une obligation légale à laquelle est soumis le responsable de traitement	- Droit d'accès et de rectification ; - Droit à la limitation du traitement
Suivi de la procédure de recouvrement des contraventions au code de la route	Respect d'une obligation légale à laquelle est soumis le responsable de traitement	- Droit d'accès et de rectification ; - Droit à la limitation du traitement
Réalisation de statistiques anonymes en vue d'adapter les formations de prévention routière	Intérêt légitime poursuivi par l'organisme (ou par un tiers)	- Droit d'opposition

Document de référence

Loi Informatique et libertés

Lien : www.cnil.fr