Commission nationale de l'informatique et des libertés

Délibération n° 2021-043 du 12 avril 2021 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre dans le cadre de la désignation des conducteurs ayant commis une infraction au code de la route

NOR : *CNIL2113933X*

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, notamment son article 58 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 8-I.2°-*b* ;

Vu le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Après avoir entendu M. Alexandre LINDEN, commissaire en son rapport et M. Benjamin TOUZANNE, commissaire du Gouvernement, en ses observations ;

Adopte un référentiel relatif aux traitements de données à caractère personnel mis en œuvre dans le cadre de la désignation des conducteurs ayant commis une infraction au code de la route et figurant en annexe.

La présidente,
M.-L. Denis

ANNEXE

RÉFÉRENTIEL RELATIF AUX TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL MIS EN ŒUVRE DANS LE CADRE DE LA DÉSIGNATION DES CONDUCTEURS AYANT COMMIS UNE INFRACTION AU CODE DE LA ROUTE (ADOPTÉ LE 12 AVRIL 2021)

1. **A qui s'adresse ce référentiel ?**

Ce référentiel s'adresse aux employeurs de droit public ou privé mettant à disposition de leurs salariés des véhicules, aux entreprises utilisatrices, aux professionnels fournissant à leurs clients, à titre onéreux ou gratuit, des véhicules dits « de remplacement » 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.

Les organismes identifiant et désignant le conducteur en cas d'infraction au code de la route doivent s'assurer de leur conformité :
- aux dispositions du règlement général sur la protection des données (RGPD) ainsi qu'à celles de la loi « informatique et libertés » du 6 janvier 1978 modifiée (LIL) ;
- aux autres règles éventuellement applicables, conformément à la réglementation en vigueur, notamment le code de la route.

2. **Portée du référentiel**

Ce référentiel porte sur les traitements de données à caractère personnel mis en œuvre couramment par les organismes 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 a pour objectif de fournir un outil d'aide à la mise en conformité des personnes et organismes identifiant et désignant le conducteur en cas d'infraction routière *via* le système de contrôle automatisé des infractions.

Le présent référentiel ne porte pas sur la gestion du forfait post-stationnement (FPS), dont la procédure de paiement ne prévoit pas la désignation du conducteur pour exonérer de paiement le titulaire du certificat d'immatriculation.

Ce référentiel n'a pas de valeur contraignante. Il permet en principe d'assurer la conformité des traitements de données mis en œuvre par les organismes aux principes relatifs à la protection des données, dans un contexte d'évolution des pratiques à l'ère du numérique.

Les organismes qui s'écarteraient du référentiel au regard des conditions particulières tenant à leur situation peuvent le faire.

Il peut néanmoins leur être demandé de justifier de l'existence d'un tel besoin et des mesures mises en œuvre afin de garantir la conformité des traitements à la réglementation en matière de protection des données à caractère personnel.

Le référentiel n'a pas pour objet d'interpréter les règles de droit autres que celles relatives à la protection des données à caractère personnel. Il appartient aux acteurs concernés de s'assurer qu'ils respectent les autres réglementations qui peuvent par ailleurs trouver à s'appliquer et notamment le code de la route.

Ce référentiel constitue également une aide à la réalisation d'une analyse d'impact relative à la protection des données (AIPD), dans le cas où celle-ci est nécessaire.

Les organismes peuvent également se reporter aux outils méthodologiques proposés par la CNIL sur son site web en vue de faciliter la mise en conformité des traitements mis en œuvre. Ils seront ainsi à même de 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) et la maîtrise de leurs risques (point 10). Les organismes pourront également s'appuyer sur les lignes directrices de la CNIL sur les AIPD. Si les organismes en ont désigné un, le délégué à la protection des données (DPD/DPO) devra être consulté.

3. **Objectifs poursuivis par les traitements (finalités)**

Tout traitement doit répondre à un objectif précis et être justifié au regard des missions et des activités de l'organisme.

Les traitements relatifs à l'identification et la désignation des conducteurs ayant commis ou susceptibles d'avoir commis une infraction peuvent notamment être 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 ;
- suivre la procédure de recouvrement des contraventions au code de la route dont peuvent être redevables les organismes publics ou privés susvisés ;
- 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 en principe 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, en particulier le principe de finalité des traitements (par exemple, les traitements mis en œuvre pour les finalités énoncées ci-dessus ne doivent pas donner lieu à des interconnexions ou échanges autres que ceux nécessaires à l'accomplissement de celles-ci).

4. **Bases légales du traitement**

Chaque finalité du traitement doit reposer sur l'une des « bases légales » fixées par la réglementation (article 6 du RGPD). (Voir pour une explication de la règle : La licéité du traitement : l'essentiel sur les bases légales prévues par le RGPD).

Il appartient au responsable de traitement de déterminer ces bases légales avant toute opération de traitement, après avoir mené une réflexion, qu'il pourra documenter, au regard de sa situation spécifique et du contexte. Ayant un impact sur l'exercice de certains droits, ces bases légales font partie des informations devant être portées à la connaissance des personnes concernées.

Le tableau reproduit ci-dessous vise à apporter aux responsables de traitement une aide pour identifier les bases légales susceptibles d'être utilisées dans les cas les plus courants.

Ces éléments doivent être adaptés à la situation spécifique de chaque organisme concerné. Ainsi, par exemple, selon que l'organisme en question relève du secteur privé ou public, certains traitements répondant pourtant à la même finalité peuvent être fondés sur des bases légales différentes (par exemple, l'intérêt légitime dans le secteur privé et l'exécution d'une mission d'intérêt public dans le secteur public).

Finalités	Base légale
Désignation et identification du conducteur	Obligation légale conformément aux dispositions de l'article L. 121-6 du code de la route
Suivi de la procédure de recouvrement des contraventions au code de la route et gestion du contentieux	Intérêts légitimes
Réalisation de statistiques anonymes	Intérêts légitimes

5. **Données à caractère personnel concernées**

5.1. *Principes de pertinence et de minimisation des données*

En vertu du principe de minimisation des données, le responsable de traitement doit veiller à ce que seules les données nécessaires à la poursuite des finalités du traitement soient effectivement collectées et traitées. Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données relatives :

a) A la procédure de désignation du conducteur ;

b) Au suivi de la procédure de recouvrement.

Le tableau reproduit ci-dessous fournit des illustrations des données que la CNIL considère comme étant en principe adaptées selon les finalités du traitement.

Catégories de données	Exemples de données
A la procédure de désignation du conducteur (il s'agit des données transmises à l'ANTAI)	**Informations relatives au conducteur** Nom, nom d'usage, prénoms, sexe et, le cas échéant, civilité de la personne ; date et lieu de naissance, adresse postale et, le cas échéant, adresse électronique ; numéro du permis de conduire.
	Information relative au véhicule Numéro d'immatriculation du véhicule concerné.
	Informations relatives à l'employeur lorsqu'il loue sa flotte de véhicules Nom, prénoms et coordonnées du responsable de traitement et, le cas échéant, d'un contact au sein de l'organisme concerné.
	Informations relatives à la location Numéro et date de l'avis de contravention ; Le cas échéant, date et heure du début et de la fin de la location ; Le cas échéant, date et heure de l'infraction.
Au suivi de la procédure de recouvrement par le responsable de traitement	Numéro, date et heure du contrat de location ou de mise à disposition du véhicule ; numéro d'immatriculation du véhicule ; éventuel numéro de dossier communiqué par l'ANTAI ; date et mode de désignation ; données d'identification du client : nom, prénoms, date de naissance, adresse postale ; montant de la contravention.

5.2. *Le traitement de données relatives aux infractions et condamnations*

Certaines données traitées dans le cadre de la désignation des conducteurs appellent à une vigilance renforcée en raison de leur caractère particulièrement sensible. Bénéficiant d'une protection spécifique, elles ne peuvent être collectées et traitées que dans des conditions strictement définies par les textes.

De telles données ne peuvent être traitées que dans le respect des dispositions légales relatives aux données d'infractions (art. 46 de la LIL). En l'espèce, leur traitement est autorisé par des dispositions spécifiques du droit national, à savoir les articles A. 121-1 et suivants du code de la route.

6. **Destinataires des données et accès aux informations**

Les données à caractère personnel ne peuvent être rendues accessibles qu'aux personnes habilitées à en connaitre au regard de leurs attributions.

De manière générale, les habilitations d'accès doivent être documentées par les organismes, et les accès aux différents traitements doivent faire l'objet de mesures de traçabilité. **Voir point 10 relatif à la sécurité.**

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 et donne des exemples de clauses à intégrer dans les contrats.

6.1. *Les personnes accédant aux données pour le compte du responsable de traitement*

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

Il peut s'agir, par exemple, de personnes chargées de la gestion administrative du personnel.

6.2. *Les destinataires des données*

Le RGPD définit les destinataires comme « *tout organisme qui reçoit la communication des données* ».

Dans le cadre de ce référentiel, peuvent notamment être destinataires des données :

– l'ANTAI ;

– l'officier du ministère public ;
– les entreprises de travail temporaire.

7. **Conservation des données**

Une durée de conservation précise des données doit être fixée en fonction de chaque finalité : ces données ne peuvent en effet pas être conservées pour une durée indéfinie.

La durée de conservation de données ou, lorsqu'elle est impossible à fixer, les critères utilisés pour déterminer cette durée, font partie des informations qui doivent être communiquées aux personnes concernées.

Il incombe au responsable du traitement de déterminer cette durée avant de mettre en œuvre le traitement.

7.1. *Les durées de conservation*

Il est recommandé que les données collectées et traitées pour les besoins de la désignation des conducteurs soient conservées dans la base active pour une durée de quarante-cinq jours à compter de la réception de la contravention, sauf dispositions légales ou réglementaires contraires ou cas particulier.

Les données peuvent être conservées plus longtemps que les durées mentionnées ci-dessus, en archivage intermédiaire, dans certains cas particuliers, par exemple si le responsable du traitement en a l'obligation légale (par exemple, pour répondre à des obligations comptables, sociales ou fiscales) ou s'il a besoin de se constituer une preuve en cas de contentieux et dans la limite du délai de prescription/forclusion applicable (par exemple, la durée de la prescription en matière contraventionnelle est de douze mois). La durée de l'archivage intermédiaire doit cependant répondre à une réelle nécessité, dûment justifiée par le responsable de traitement après une analyse préalable de différents facteurs, notamment le contexte, la nature des données traitées et le niveau de risque d'un éventuel contentieux.

Dans le cadre d'une convention avec l'ANTAI, tous les échanges d'informations entre l'organisme et l'ANTAI sur les conducteurs de véhicules ayant commis une infraction au code de la route devraient être supprimés par l'organisme une fois la désignation effectuée.

> Lorsque les missions du salarié impliquent la conduite d'un véhicule à titre principal (chauffeur, livreur, ambulancier, etc.) ou que des déplacements fréquents sont nécessaires à la bonne exécution du contrat (commercial, technicien, etc.) et sous réserve que le salarié y ait librement consenti, l'organisme devrait pouvoir conserver les éléments nécessaires à la désignation d'un conducteur plus longtemps afin d'éviter à celui-ci d'avoir à fournir de nombreuses fois les mêmes données pour d'éventuelles désignations ultérieures.

7.2. *La conservation de données anonymisées*

La réglementation relative à la protection des données à caractère personnel ne s'applique pas, notamment en ce qui concerne les durées de conservation, aux **données anonymisées**. Il s'agit des données qui ne peuvent plus être mises en relation avec la personne physique identifiée à laquelle elles se rapportent.

L'anonymisation doit être distinguée de la pseudonymisation. Dans ce dernier cas, il est techniquement possible de retrouver l'identité de la personne concernée grâce à des données tierces. L'opération de pseudonymisation est réversible, contrairement à l'anonymisation.

Ainsi, le responsable du traitement peut conserver sans limitation de durée les données anonymisées.

Pour en savoir plus, vous pouvez vous référer aux guides de la CNIL :

– « Sécurité : Archiver de manière sécurisée » ;
– « Limiter la conservation des données » ;
– « Guide pratique : les durées de conservation ».

L'anonymisation est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et ce de manière irréversible. Aussi, une fois anonymisées, les données ne peuvent plus être reliées à une personne (Pour en savoir plus, vous pouvez vous référer aux lignes directrices du CEPD sur l'anonymisation).

8. **Information des personnes**

Un traitement de données à caractère personnel doit être mis en œuvre en toute transparence vis-à-vis des personnes concernées.

8.1. *Contenu de l'information à délivrer*

L'information communiquée aux personnes concernées doit se faire dans les conditions prévues par les articles 12, 13 et 14 du RGPD.

Dès le stade de la collecte des données à caractère personnel, les personnes concernées doivent notamment être informées de l'existence du traitement, de ses caractéristiques essentielles (parmi lesquelles l'identité du responsable du traitement et l'objectif poursuivi) et des droits dont elles disposent.

Des exemples de mentions d'information sont disponibles sur le site web de la CNIL et peuvent être consultés dans la rubrique « RGPD : exemples de mentions d'information ».

8.2. *Modalités de délivrance de l'information*

Afin de respecter pleinement les principes de loyauté et de transparence, conformément aux dispositions des articles 13 et 14 du RGPD, les personnes doivent être directement ou indirectement informées au moment où les données sont collectées.

Si le RGPD n'impose aucune forme spécifique, une information écrite devrait être privilégiée, de manière à pouvoir justifier de son contenu, ainsi que du moment où elle a été délivrée.

Dans le cadre du présent référentiel, le responsable du traitement procède à l'information des personnes concernées par tout moyen approprié conformément aux dispositions de l'article 12 du RGPD.

9. **Droits des personnes**

Les personnes concernées disposent des droits suivants, qu'elles exercent dans les conditions prévues par le RGPD (pour aller plus loin, voir la rubrique qui s'intitule « Comprendre mes droits » sur le site de la CNIL) :

- le droit d'accès, permet à la personne concernée de savoir si des données la concernant sont traitées par le responsable de traitement et, dans cette hypothèse, d'obtenir des précisions sur les conditions de ce traitement et, à sa demande, d'obtenir une copie des données le concernant détenues par ce responsable ;
- le droit de rectification, permet à la personne concernée de demander la rectification des informations inexactes ou incomplètes la concernant ;
- le droit à l'effacement, permet à la personne concernée de demander à un organisme l'effacement de données à caractère personnel la concernant ;
- le droit à la limitation du traitement : par exemple, lorsque la personne conteste l'exactitude de ses données, elle peut demander à l'organisme le gel temporaire du traitement de ses données, le temps que celui-ci procède aux vérifications nécessaires ;
- le droit de s'opposer au traitement des données concernant la personne, sous réserve des conditions d'exercice de ce droit en application des dispositions de l'article 21 du RGPD.

La personne concernée pourra s'opposer au traitement de ses données à condition d'invoquer des raisons tenant à sa situation particulière, et uniquement lorsque le traitement est mis en œuvre sur la base de l'intérêt légitime du responsable de traitement, ou pour l'exécution d'une mission d'intérêt public ou d'une mission relevant de l'autorité publique.

Le responsable du traitement pourra refuser de donner suite à cette demande d'opposition s'il démontre qu'il dispose d'intérêts légitimes et impérieux qui prévalent sur les droits et libertés du demandeur.

En ce qui concerne le présent référentiel, le responsable de traitement apparaît pouvoir refuser de faire droit à une telle demande dans le cadre du suivi de la procédure de recouvrement, dans la mesure où il dispose d'intérêts légitimes et impérieux qui prévalent sur les droits et libertés du demandeur, sauf circonstances particulières.

Attention : Le responsable de traitement doit répondre aux demandes reçues dans les meilleurs délais et dans un délai d'un mois maximum. Si un délai supplémentaire est nécessaire pour traiter la demande (par exemple, en raison de sa complexité), la personne concernée doit en être informée dans ce même délai d'un mois. Dans tous les cas, une réponse doit être apportée dans un délai qui ne peut pas dépasser trois mois.
L'exercice des droits par les personnes doit être facilité par le responsable de traitement et être gratuit. Les personnes concernées doivent être informées de leur possibilité d'adresser une réclamation à la Commission nationale de l'informatique et des libertés si elles ne sont pas satisfaites du traitement des données à caractère personnel les concernant.

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, l'organisme est invité à mettre en œuvre les mesures suivantes, ou à être en mesure de justifier de la mise en place de mesures équivalentes ou de leur absence de nécessité ou de possibilité (les particuliers traitant un volume faible de données prennent, par exemple, les mesures élémentaires de sécurité pour assurer la sécurité et la confidentialité des données qu'ils traitent) :

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 mot 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

Catégories	Mesures
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 ordiphones
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, WPA2-PSK ou WPA3 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 n'est transmis 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.*)
Sécuriser les échanges avec d'autres organismes	Chiffrer les données avant leur envoi
	S'assurer qu'il s'agit du bon destinataire

Catégories	Mesures
	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
	Tester sur des données fictives ou anonymisées
Utiliser des fonctions cryptographiques	Utiliser des algorithmes, des logiciels et des bibliothèques reconnues
	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 (AIPD)**

En application des dispositions de l'article 35 du RGPD, le responsable de traitement pourrait avoir à réaliser une analyse d'impact dès lors que le traitement qu'il met en œuvre est susceptible de présenter un risque élevé pour les droits et les libertés des personnes concernées.

Il conviendra tout d'abord de se référer :

– à la liste des traitements pour lesquels une analyse d'impact n'est pas requise ;
– puis, à la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise ;
– si le traitement mis en œuvre n'est pas présent sur l'une de ces listes, il faut alors s'interroger sur la nécessité d'effectuer une AIPD.

Pour ce faire, il convient de s'appuyer sur les critères établis par le Comité européen de la protection des données (CEPD) dans les lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD).

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

S'il est, en revanche, mis en œuvre dans une entreprise 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 dès lors qu'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 un, le DPD/DPO devra être consulté.

Conformément à l'article 36 du RGPD, le responsable de traitement doit consulter la CNIL préalablement à la mise en œuvre du traitement si l'analyse d'impact indique qu'il ne parvient pas à identifier des mesures suffisantes pour réduire les risques à un niveau acceptable.