

Date de publication sur legifrance: 01/08/2014

Commission Nationale de l'Informatique et des Libertés

Délibération n°2014-312 du 17 juillet 2014

Délibération n° 2014-312 du 17 juillet 2014 portant autorisation unique de traitements de données à caractère personnel ayant pour finalité la lutte contre la fraude à l'assurance mis en œuvre par les organismes d'assurance, de capitalisation, de réassurance, d'assistance et par les intermédiaires d'assurance (AU 039)

NOR: CNIX1418319X

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 la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu le code des assurances ;

Vu le code civil ;

Vu le code général des impôts ;

Vu le code monétaire et financier ;

Vu le code de la mutualité ;

Vu le code pénal ;

Vu le code des postes et des communications électroniques ;

Vu le code rural ;

Vu le code de la santé publique ;

Vu le code de la sécurité sociale ;

Vu le code du travail ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 25 II , 25.I.3°, 25.I.4°, 25.I.5°, ou 25.I.6° et 69 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié 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. Jean-Luc VIVET, commissaire, en son rapport, et M. Jean-Alexandre SILVY, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

La lutte contre la fraude et les activités abusives constitue, pour les professionnels de l'assurance, une priorité majeure, avec les principaux objectifs qui la sous-tendent, en termes de justice, de protection des assurés, de dissuasion et de maîtrise des risques.

Il n'existe pas de définition légale de la fraude à l'assurance en France. Les praticiens considèrent toutefois qu'il y a fraude à l'assurance chaque fois qu'un acte intentionnel permettant de tirer un profit illégitime d'un contrat d'assurance" a été caractérisé. Cet acte peut concerner aussi bien le

contrat d'assurance que le sinistre, objet des garanties souscrites. Dès lors, l'autorisation unique couvre l'ensemble du périmètre assurantiel, quel que soit le type de contrats et quel que soit l'auteur de la fraude (fraude interne et fraude externe).

Le Code des assurances prévoit des sanctions spécifiques et parfois sévères en cas de fraude à l'assurance. Par ailleurs et nonobstant la mise en œuvre de sanctions civiles, des actions pénales peuvent également être introduites à l'encontre des fraudeurs.

Ainsi, les traitements de données à caractère personnel mis en œuvre par, les organismes d'assurance, de capitalisation, de réassurance, d'assistance et les intermédiaires d'assurance, au titre de la lutte contre la fraude visent à prévenir, à détecter et à gérer les alertes pouvant révéler une fraude à l'assurance.

L'identification de tels faits, en partie sur la base de critères intégrés dans les traitements automatisés des organismes, peut conduire ces derniers à collecter des données d'infractions et / ou le Numéro d'inscription au répertoire National d'Identification des Personnes Physiques (NIR) uniquement dans les cas prévus par la loi ou à rompre toute relation contractuelle avec les prestataires, les agents généraux, les mandataires d'assurance, les intermédiaires, les administrateurs, les mandataires sociaux, ou les élus des organismes. Enfin, ces traitements peuvent éventuellement donner lieu à des interconnexions de fichiers ayant des finalités principales différentes.

Par conséquent, ces traitements relèvent des dispositions des articles 25.I.3°, 25.I.4°, 25.I.5°, et 25.I.6° ainsi que des dispositions de l'article 69 de la loi du 6 janvier 1978 modifiée et doivent, à ce titre, être autorisés par la CNIL.

En vertu du II de l'article 25 de la loi du 6 janvier 1978 modifiée, la Commission peut autoriser par une décision unique une catégorie de traitements répondant aux mêmes finalités, portant sur des catégories de données identiques et ayant les mêmes catégories de destinataires.

Décide

- D'adopter une autorisation unique pour les traitements automatisés ou non de données à caractère personnel relevant des articles 25.I.3°, 25.I.4°, 25.I.5°, et 25.I.6°;
- Que les organismes mentionnés ci-dessous qui souhaiteront se référer à l'autorisation unique n° 39 adresseront à cette fin à la commission un engagement de conformité pour leurs traitements qui répondent strictement aux conditions définies dans la présente décision unique seront autorisés à mettre en œuvre ces traitements ;
- Tout projet de traitement automatisé ou non de données relevant des articles 25.I.3°, 25.I.4°, 25.I.5°, ou 25.I.6° de la loi du 6 janvier 1978 modifiée, dont les finalités ou les catégories de données ou de destinataires excèderaient le cadre défini par la présente autorisation unique ou qui ne respecteraient pas les exigences qui y sont définies devra faire l'objet d'une demande d'autorisation spécifique présentant et expliquant les différences entre le traitement envisagé et l'autorisation unique.

Article 1^{er} : Responsables de traitement

Seuls peuvent adresser un engagement de conformité à la présente autorisation unique les organismes d'assurance, de capitalisation, de réassurance, d'assistance et les intermédiaires d'assurance, ci après désignés organismes .

Article 2 : Finalités et caractéristiques des traitements

Dans le cadre des activités relatives à la passation, à la gestion et à l'exécution des contrats d'assurance, de capitalisation, de réassurance, et d'assistance (ci après désignés contrats), peuvent faire l'objet d'un engagement de conformité à la présente autorisation unique, les traitements automatisés de données à caractère personnel ayant pour finalités la lutte contre la fraude à l'assurance externe ou interne correspondant à un acte ou omission commis intentionnellement par une ou plusieurs personnes afin d'obtenir un avantage ou un bénéfice de façon illégitime, illicite ou

illégale.

Au titre de ces traitements sont visés :

- l'analyse et la détection des actes réalisés dans le cadre de la passation, la gestion et l'exécution des contrats présentant une anomalie, une incohérence, ou ayant fait l'objet d'un signalement pouvant révéler une fraude à l'assurance,

- la gestion des alertes en cas d'anomalies, d'incohérences ou de signalements,

- la constitution de listes des personnes dûment identifiées comme auteurs d'actes pouvant être constitutifs d'une fraude,

- la gestion des procédures amiables, contentieuses, et disciplinaires consécutives à un cas de fraude,

- l'exécution des dispositions contractuelles, législatives, réglementaires ou administratives en vigueur applicables consécutivement à une fraude.

Ces traitements permettent de prévenir, de détecter ou de gérer les opérations, actes, ou omissions présentant un risque de fraude et émanant soit :

- pour la fraude externe : des personnes parties, intéressées ou intervenant au contrat,

- pour la fraude interne : des personnels salariés, des prestataires, des agents généraux, des mandataires, des intermédiaires, des administrateurs, mandataires sociaux, ou des élus des organismes.

Des requêtes individuelles et ponctuelles peuvent être effectuées par l'employeur, dans le cadre de son pouvoir d'enquête interne, sur les données collectées au titre de la gestion administrative du personnel.

L'objectif de lutte contre la fraude à l'assurance peut donner lieu à des interconnexions entre les traitements de données mis en œuvre par le responsable de traitement ou par le groupe auquel il appartient, répondant aux finalités suivantes :

- la gestion commerciale de clients et de prospects telle qu'elle est prévue par la norme simplifiée n°56,

- la passation, la gestion et l'exécution des contrats prévue par la norme simplifiée n°16,

- la lutte contre le blanchiment et le financement du terrorisme telle que prévue par l'AU 003, pour les cas de fraude relevant également de cette finalité,

- la collecte et le traitement des données relatives aux infractions, aux condamnations et mesures de sûreté prévus par les dispositions légales, réglementaires et administratives en vigueur, ainsi que dans le cadre des contentieux liés à l'activité et permettant notamment à l'entreprise d'assurer la constatation, l'exercice ou la défense de ses droits en justice ou la défense des personnes concernées,

- la gestion des relations contractuelles avec les intermédiaires, les prestataires, les sous-traitants, les délégataires, et les partenaires.

Aucune décision produisant des effets juridiques à l'égard des personnes concernées par des données traitées dans le cadre de la lutte contre la fraude à l'assurance ne peut être prise sur le seul fondement de ces traitements automatisés. Dès lors, les requêtes ou alertes détectées automatiquement doivent donner lieu à une analyse non automatisée par le personnel habilité de l'organisme ou du groupe auquel il appartient, le cas échéant des investigations complémentaires pourront être diligentées. Enfin, la personne concernée doit être mise en mesure de présenter ses observations si une décision produisant des effets juridiques est prise à son égard dans le cadre de la

conclusion ou de l'exécution d'un contrat.

Article 3 : Catégories de données à caractère personnel traitées

- Peuvent être traitées, pour l'accomplissement des finalités décrites à l'article 2, les catégories de données suivantes, collectées dans le cadre :

- de la passation, de la gestion et de l'exécution des contrats conformément à la norme simplifiée n°16 qui vise les données relatives à :

- l'identification des personnes parties, intéressées ou intervenantes au contrat,
- la situation familiale, économique, patrimoniale et financière,
- la situation professionnelle,
- l'appréciation du risque,
- la passation, l'application du contrat, et la gestion des sinistres et des prestations,
- la détermination ou à l'évaluation des préjudices,
- la localisation des personnes ou des biens en relation avec les risques assurés,
- la vie personnelle et aux habitudes de vie en relation avec les risques assurés,
- la santé lors de la souscription du contrat, sous réserve de l'obtention du consentement exprès de la personne concernée. Pour la mise en œuvre des garanties, le consentement de la personne est exigé sauf s'il ne peut être matériellement ou juridiquement recueilli, ou que l'organisme est soumis à une obligation légale de recueillir ces informations.
- de la gestion et du suivi de la relation commerciale conformément à la norme simplifiée n° 56 qui vise les données relatives :

- à l'identification des personnes,
- à la situation familiale, économique, patrimoniale et financière et aux habitudes de vie en lien avec la relation commerciale,
- aux activités professionnelles et non professionnelles ayant un lien avec la relation commerciale,
- au suivi de la relation commerciale,
- à la localisation et à la connexion,
- de l'autorisation unique n° 32 concernant les infractions, condamnations et mesures de sûreté des personnes parties, intéressées ou intervenantes au contrat, à savoir :
- concernant les personnes :
- les données d'identification : nom et prénom(s), date et lieu de naissance,
- les coordonnées postales,
- le cas échéant, les données issues des procès verbaux de police ou de gendarmerie, les décisions judiciaires ou administratives et les enquêtes judiciaires.

- concernant les circonstances de l'infraction :
- les faits constatés,
- la présence de témoins, leur identification et leurs témoignages.
- suites données à la constatation de l'infraction :
- saisine ou absence de saisine,
- classement sans suite,
- engagement de poursuite,
- condamnations,
- mesures de sûreté.
- de la journalisation des accès aux traitements relevant de la norme simplifiée n°16, n°56 et des autorisations uniques n°31 et n°32.
- Le Numéro d'inscription au répertoire National d'Identification des Personnes Physiques (NIR) est traité par les organismes conformément aux dispositions légales en vigueur, dans les cas suivants :
- pour les activités d'assurance maladie, maternité, invalidité, retraite supplémentaire, dans le cadre des relations avec les professionnels, les établissements et les institutions de santé, pour les déclarations sociales des entreprises souscriptrices de contrats d'assurance et pour l'indemnisation des accidents,
- pour la gestion des rentes,
- enfin, le NIR peut être collecté dans le cadre de leurs activités d'assurance, pour les garanties pertes d'exploitation et perte d'emploi uniquement à des fins probatoires.
- les données collectées au titre de la gestion administrative du personnel uniquement dans le cadre de requêtes ponctuelles et individuelles consécutives à la détection d'une fraude.
- les données relatives aux anomalies, incohérences et signalement pouvant révéler une fraude.
- les données relatives aux investigations, à l'instruction du dossier de fraude et à l'évaluation du périmètre de la fraude.
- les données d'identification des personnes intervenant dans la détection et la gestion de la fraude.

Article 4 : Durées de conservation

Les organismes d'assurance disposent d'un délai de 6 mois à compter de l'émission des alertes pour les qualifier. Toute alerte qualifiée de non pertinente est supprimée sans délai. Les alertes n'ayant reçu aucune qualification à l'issue du délai de 6 mois sont supprimées.

En cas d'alerte pertinente, les données visées à l'article 3 sont conservées pour une durée maximale de 5 ans à compter de la clôture du dossier de fraude. Lorsqu'une procédure judiciaire est engagée, les données sont conservées jusqu'au terme de la procédure judiciaire. Elles sont ensuite archivées selon les durées de prescription applicables.

Pour les personnes inscrites sur une liste des fraudeurs présumés, les données les concernant sont supprimées passé le délai de 5 ans à compter de la date d'inscription sur cette liste.

Article 5 : Destinataires et personnes habilitées à traiter les données

- Dans la limite de leurs attributions respectives et pour l'exercice des finalités précitées, seuls peuvent être habilités à accéder aux données, les personnes suivantes :

- Aux fins de lutte contre la fraude interne :

- o Les personnes habilitées de la direction des ressources humaines pour des requêtes ponctuelles et individuelles réalisés dans le cadre d'enquêtes internes consécutives à la détection d'une fraude,

- o le conseil de discipline saisi en cas de fraude,

- o les représentants du personnel dans le cadre de l'accompagnement d'un salarié mis en cause pour fraude.

- Aux fins de lutte contre la fraude interne et externe :

- o les personnels en relation avec la clientèle et les gestionnaires de contrats et de sinistres,

- o les autres entités d'un même groupe dès lors qu'elles sont concernées par la fraude ou interviennent dans la gestion des dossiers ou de maîtrise du risque de fraude,

- o les personnels habilités en charge de la lutte contre la fraude, de la lutte anti-blanchiment et du contrôle interne, les inspecteurs, enquêteurs, experts, et auditeurs,

- o le personnel habilité de la direction générale, la direction juridique ou du service du contentieux pour la gestion des contentieux,

- o le personnel habilité des sous-traitants.

- Dès lors qu'ils sont directement concernés par une fraude, peuvent être destinataires des données relatives à cette fraude, les personnels habilités :

- des autres organismes d'assurance ou intermédiaires intervenant dans le cadre de dossier présentant une fraude,

- des organismes sociaux lorsque les régimes sociaux interviennent dans le règlement des sinistres ou lorsque les organismes d'assurances offrent des garanties complémentaires à celles des régimes sociaux,

- des organismes professionnels intervenant dans le cadre de dossiers présentant une fraude,

- les auxiliaires de justice et officiers ministériels,

- l'autorité judiciaire, médiateur, arbitre saisis d'un litige,

- les organismes tiers autorisés par une disposition légale à obtenir la communication de données à caractère personnel relatives à des précontentieux, contentieux ou condamnations,

- s'il y a lieu les victimes de fraudes ou leurs représentants.

La communication de ces données ne peut en aucun cas donner lieu à la création d'un fichier concernant les données relatives aux fraudes et mutualisé entre les destinataires.

Article 6 : Information et droit d'accès des personnes concernées

- Le responsable du traitement doit, conformément aux dispositions de l'article 32 de la loi du 6 janvier 1978 modifiée, informer préalablement à la mise en œuvre du traitement, les personnes auprès desquelles sont recueillies les données à caractère personnel les concernant :

- de son identité et, le cas échéant, de celle de son représentant,

- de la finalité poursuivie par le traitement auquel les données sont destinées,

- du caractère obligatoire ou facultatif des réponses,
 - des conséquences éventuelles, à son égard, d'un défaut de réponse,
 - des destinataires ou catégories de destinataires des données,
 - de l'existence et des modalités d'exercice des droits d'accès, de rectification et d'opposition,
 - du transfert éventuel des données personnelles à destination d'un Etat non membre de l'Union Européenne.
- De manière générale, les personnes sont informées du fait que le responsable de traitement met en œuvre un dispositif ayant pour finalité la lutte contre la fraude pouvant, notamment, conduire à l'inscription sur une liste de personnes présentant un risque de fraude. Cette information s'effectue selon les modalités suivantes :
- Pour la fraude interne :
- les salariés de l'organisme d'assurance sont informés individuellement dans le règlement intérieur ou dans tout autre support de communication échangé lors de l'exécution du contrat qu'il existe un traitement visant la lutte contre la fraude interne et externe au sein de l'organisme,
 - les prestataires, les agents généraux, les mandataires, les intermédiaires, les administrateurs, les mandataires sociaux ou les élus des organismes sont informés dans les documents contractuels ou tout autre support de communication adressés par l'organisme d'assurance.

Pour la fraude externe :

- les assurés sont informés de l'existence du traitement de lutte contre la fraude au moyen des documents qui leur sont communiqués au moment de la souscription du contrat, ou de tout autre support de communication échangé lors de l'exécution du contrat.
- Outre cette information générale, après un délai de 6 mois d'investigation, en cas de confirmation de l'anomalie et de décisions produisant des effets juridiques, la personne susceptible d'être inscrite sur une liste de personnes présentant un risque de fraude, doit être informée individuellement par écrit des dites conséquences en lui donnant la possibilité de présenter ses observations.

Article 7 : Mesures de sécurité

Le responsable du traitement prend toutes précautions utiles pour préserver la sécurité et la confidentialité des données traitées et notamment pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Le responsable de traitement définit une politique de sécurité adaptée aux risques présentés par les traitements et à la taille de l'organisme d'assurance. Cette politique devra décrire les objectifs de sécurité, et les mesures de sécurité physique, logique et organisationnelle permettant de les atteindre.

Les accès aux traitements de données nécessitent une authentification des personnes accédant aux données, au moyen d'un identifiant et d'un mot de passe individuels, suffisamment robustes et régulièrement renouvelés, ou par tout autre moyen d'authentification de même fiabilité.

Les droits permettant d'accéder aux données doivent être précisément définis en fonction des besoins réels de chaque utilisateur, il s'en suit que les permissions d'accès devront être supprimées pour tout utilisateur n'étant plus habilité.

Le responsable de traitement prend les mesures nécessaires pour assurer la maintenance du matériel. Ainsi, les interventions de maintenance doivent faire l'objet d'une traçabilité et le matériel remisé devra être nettoyé de toute donnée à caractère personnel.

Les conditions d'administration du système d'information prévoient l'existence de systèmes automatiques de traçabilité (journaux, audits...).

Dans le cas de l'utilisation d'un service de communication au public en ligne, le responsable de

traitement prend les mesures nécessaires pour se prémunir contre toute atteinte à la confidentialité des données traitées. Les données transitant sur des canaux de communication non sécurisés doivent notamment faire l'objet de mesures techniques visant à les rendre incompréhensibles à toute personne non autorisée à y avoir accès.

Le responsable de traitement devra aussi s'assurer que ses sous-traitants présentent des garanties en matière de sécurité des données.

S'agissant des données de santé, le responsable de traitement s'engage à respecter les dispositions prévues par la loi de bonne conduite annexé à la convention AERAS concernant la collecte et l'utilisation de données relatives à l'état de santé en vue de la souscription ou de l'exécution d'un contrat d'assurance.

Article 8 : Transferts de données vers l'étranger

Les transferts de données à caractère personnel réalisés vers des pays tiers à l'Union européenne qui ne sont pas membres de l'Espace économique européen peuvent être effectués lorsque l'une des conditions suivantes est réunie :

- les transferts s'effectuent à destination d'un pays reconnu par une décision de la Commission européenne comme assurant un niveau de protection suffisant, ou d'une entreprise américaine ayant adhéré aux principes du Safe Harbor ; ou

- le traitement garantit un niveau suffisant de protection de la vie privée ainsi que les droits et libertés fondamentaux des personnes par la mise en œuvre des clauses contractuelles types adoptées par la Commission européenne ou par l'adoption de règles internes d'entreprise dénommées BCR dont la CNIL a préalablement reconnu qu'elles garantissent un niveau de protection suffisant ou ;

- ces transferts sont réalisés dans le cadre de l'exécution des contrats ou pour la mise en œuvre des garanties (art. 69 [1°, 5°, 6°] de la loi Informatique et Libertés), ou lors de la gestion des actions ou contentieux liés à l'activité et permettant notamment à l'entreprise d'assurer la constatation, l'exercice ou la défense de ses droits en justice ou pour les besoins de défense des personnes concernées (art. 69 [3°] de la loi Informatique et Libertés).

Le recours à ces exceptions de l'article 69 n'est possible que pour les transferts dont le champ d'application est limité à des cas de transferts ponctuels et exceptionnels. Ainsi, les transferts répétitifs, massifs ou structurels de données personnelles doivent faire l'objet d'un encadrement juridique spécifique au moyen de BCR ou de clauses contractuelles types).

Le responsable de traitement s'engage, sur simple demande de la personne concernée, à apporter une information complète sur la finalité du transfert, les données transférées, les destinataires exacts des informations et les moyens mis en œuvre pour encadrer ce transfert.

Article 9 : Dispositions transitoires

Les traitements de données à caractère personnel dont la mise en œuvre est intervenue avant la publication de la présente délibération disposent d'un délai de 24 mois à compter de cette publication pour adresser à la Commission un engagement de conformité avec les dispositions de la présente autorisation unique.

Article 10 : Publication au Journal officiel

La présente délibération sera publiée au Journal officiel de la République française.

La Présidente

I. FALQUE-PIERROTIN

Nature de la délibération: AUTORISATION UNIQUE

