

Commission nationale de l'informatique et des libertés

Délibération n° 2017-217 du 13 juillet 2017 portant autorisation unique de traitements de données à caractère personnel aux fins de la lutte contre la fraude externe dans le secteur bancaire et financier (AU-054)

NOR : CNIL1721548X

La Commission nationale de l'informatique et des libertés,

Vu le code monétaire et financier ;

Vu le code civil ;

Vu le code général des impôts ;

Vu le code pénal ;

Vu le code de la consommation ;

Vu le code de commerce ;

Vu le code des postes et des communications électroniques ;

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) n° 575/2013 du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement n° 648/2012 ;

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

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 ;

Vu l'arrêté du 20 février 2007 relatif aux exigences de fonds propres applicables aux établissements de crédit et aux entreprises d'investissement ;

Vu l'arrêté du 23 décembre 2013 relatif au régime prudentiel des sociétés de financement ;

Vu l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution ;

Vu le règlement général de l'Autorité des marchés financiers ;

Vu la délibération n° 2016-005 du 14 janvier 2016 portant autorisation unique de traitements de données à caractère personnel mis en œuvre par les organismes publics et privés pour la préparation, l'exercice et le suivi de leurs contentieux ainsi que l'exécution des décisions rendues (AU-046) ;

Après avoir entendu M. Jean-Luc VIVET, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

La lutte contre la fraude constitue, pour les organismes bancaires et financiers, intermédiaires et groupes, une priorité avec les principaux objectifs qui la sous-tendent en termes de protection des clients, de dissuasion et de maîtrise des risques.

La présente autorisation unique vise à couvrir les seuls traitements mis en œuvre par les organismes relevant du secteur bancaire et financier à des fins de détection et de qualification des anomalies et de gestion des opérations qualifiées de fraude externe au sens de l'article 324 du règlement (UE) n° 575/2013 du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement. L'accès aux traitements de lutte contre la fraude est limité aux seules personnes spécifiquement habilitées et soumises à des obligations de déontologie et de confidentialité appropriées prenant part au processus du contrôle interne ou en charge de la gestion de la fraude.

Aux termes de l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution (ACPR), les établissements de crédit, les sociétés de financement, les entreprises d'investissement (autres que les sociétés de gestion de portefeuille), les établissements de paiement et les établissements de monnaie électronique ont l'obligation de se doter d'un dispositif de gouvernance solide, comprenant notamment un dispositif adéquat de contrôle interne.

Le contrôle interne comprend notamment des systèmes de surveillance et de maîtrise des risques. Le risque opérationnel en fait partie. Il s'agit des risques de pertes découlant d'une inadéquation ou d'une défaillance des processus, du personnel et des systèmes internes ou d'événements extérieurs, y compris le risque juridique. Le

risque opérationnel inclut notamment les risques liés à des événements de faible probabilité d'occurrence mais à fort impact, les risques de fraude externe définis à l'article 324 du règlement (UE) n° 575/2013 susvisé, et les risques liés au modèle.

Outre l'obligation prévue à l'article L. 511-41-1-B du code monétaire et financier (CMF) pour les établissements de crédit et les sociétés de financement, les entités doivent mettre en place, au titre de l'article L. 511-41-1-B du CMF et de l'article 4 de l'arrêté du 3 novembre 2014, des dispositifs, stratégies et procédures, permettant de détecter, de mesurer et de gérer leurs risques opérationnels sur une base consolidée. Les dispositifs de lutte contre la fraude doivent être adaptés en fonction de leurs activités, de la nature, de l'échelle, de la complexité des risques inhérents à leur modèle d'entreprise et à leur organisation.

L'article 10, j, de l'arrêté du 3 novembre 2014 définit la fraude externe par renvoi à l'article 324 du règlement (UE) n° 575/2013 du 26 juin 2013. La fraude externe est définie comme un événement causant des « pertes qui sont liées à des actes de tiers visant à commettre une fraude ou un détournement d'actif ou à enfreindre/contourner la loi ».

La notion de « groupe » dans la présente autorisation unique s'entend au sens des groupes soumis au contrôle de l'ACPR conformément à l'article L. 511-20-III du CMF et à l'arrêté du 3 novembre 2014. Les organismes d'assurance, de capitalisation, de réassurance, d'assistance et les intermédiaires d'assurance ne peuvent procéder à un engagement de conformité à la présente autorisation unique, mais doivent, le cas échéant, se référer à l'AU-039 relative au secteur de l'assurance (délibération n° 2014-312 du 17 juillet 2014).

Les entreprises assujetties relevant de la surveillance de l'ACPR sur une base consolidée, c'est-à-dire à l'échelle du groupe ou, le cas échéant, sous-consolidée, c'est-à-dire d'une entité mère au sens du 49 de l'article 4 du règlement (UE) n° 575/2013 du 26 juin 2013, veillent à s'assurer que les systèmes mis en place, au sein de ces entreprises, sont cohérents entre eux afin de permettre une mesure, une surveillance et une maîtrise des risques encourus au niveau consolidé ou, le cas échéant, sous-consolidé.

A cette fin, elles mettent en œuvre des traitements automatisés de données à caractère personnel objets de la présente autorisation unique, qui peuvent conduire à refuser ou à rompre toute relation précontractuelle ou contractuelle avec les personnes concernées et donner lieu à des rapprochements de traitements ayant des finalités différentes.

Par conséquent, ces traitements relèvent des dispositions des articles 25-I (3° et 4°) de la loi n° 78-17 du 6 janvier 1978 modifiée et doivent, à ce titre, être autorisés par la CNIL.

En vertu du II de l'article 25, 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 (4° et 5°) de la loi n° 78-17 du 6 janvier 1978 modifiée ;
- que les organismes mentionnés ci-dessous qui souhaiteront se référer à la présente autorisation unique 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 et seront autorisés à mettre en œuvre ces traitements.

Tout projet de traitement automatisé ou non de données relevant des articles 25-I (4° et 5°) de la loi du 6 janvier 1978 modifiée, dont les finalités ou les catégories de données ou de destinataires excéderaient 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.

Sur le responsable de traitement :

Seules peuvent adresser un engagement de conformité à la présente autorisation unique les entités agissant en tant que responsable de traitement pour leur propre compte et répondant aux critères cumulatifs suivants :

- être visées au livre V du CMF ;
- être régulées par l'ACPR, c'est-à-dire relever de la compétence de l'ACPR au regard de l'article L. 612-2-I, A, du CMF ou pouvant être soumis à son contrôle (article L. 612-2-II) ; et
- être soumises aux dispositions de l'arrêté du 3 novembre 2014 relatif au contrôle interne.

Les entités pouvant adresser un engagement de conformité sont donc les suivantes :

- les établissements de crédit ;
- les intermédiaires en opérations de banque et services de paiement ;
- les prestataires de services de paiement ;
- les prestataires de services d'investissement ;
- les personnes qui fournissent des services d'investissement ;
- les conseillers en investissement ;
- les sociétés de financement ;
- les établissements de monnaie électronique ;
- les compagnies financières holding ;

- les entreprises mères de société de financement.

Par ailleurs, pourront effectuer un engagement de conformité à cette autorisation unique les entités contrôlées par les organismes susmentionnés lorsque l'activité de ces entités peut être qualifiée de connexe au sens de l'article L. 311-2 du CMF et qu'elle relève par conséquent du périmètre consolidé du contrôle interne au sens de l'article 3 de l'arrêté du 3 novembre 2014.

Chacune de ces entités est désignée sous le terme « entité » dans la présente autorisation unique.

Sur la finalité du traitement :

Peuvent procéder à un engagement de conformité à la présente autorisation unique, les entités mettant en œuvre des traitements automatisés de données à caractère personnel ayant pour finalité la prévention et la lutte contre la fraude externe.

La présente autorisation unique ne vise que les cas de fraude externe et de fraude mixte (fraude externe intervenant avec la complicité d'un collaborateur de l'entité). Elle comprend le traitement de :

- l'alerte générée après la détection d'une anomalie, d'une incohérence ou du signalement d'un acte pouvant relever d'une fraude, alerte qui est analysée manuellement par les personnes habilitées ;
- la fraude avérée qui s'entend comme une fraude ou une tentative de fraude qualifiée comme telle par l'entité à la suite d'investigations par les personnes habilitées.

Les cas de fraude interne ne relèvent pas de cette autorisation unique. La fraude externe concerne les personnes parties ou intéressées au contrat (clients, bénéficiaires effectifs) et les personnes intervenant au contrat (sous-traitants et prestataires de services, intermédiaires financiers, etc.).

Le périmètre matériel de l'autorisation unique est la lutte contre la fraude dans le cadre des activités relatives aux contrats portant sur les services et produits bancaires, financiers, de paiement et de monnaie électronique tels que définis aux livres II et III du CMF (comptes, prêts et crédits, autres contrats et services bancaires et financiers) ainsi que des produits et services dits « connexes », délivrés par les organismes bancaires et financiers relevant du CMF (exemples : location longue durée, opération de change, tenue de coffre-fort, etc.), ci-après désignés globalement « services bancaires et financiers ».

Au titre des traitements couverts par la présente autorisation unique sont visées :

- la détection des actes réalisés dans le cadre de la passation, la gestion et l'exécution des contrats présentant une anomalie ou une incohérence ;
- la gestion et l'analyse des alertes provenant de sources d'information (le dispositif de contrôle interne au sens de l'arrêté du 3 novembre 2014, les réclamations clients, les réquisitions judiciaires et des autorités de régulation et les alertes émises directement par les collaborateurs) ;
- la constitution par l'entité de listes des personnes dûment identifiées comme auteurs d'actes qualifiés de fraude ou de tentative de fraude externe qualifiée comme telle par l'entité à la suite d'investigations.

Ces traitements permettent de prévenir, de détecter ou de gérer les opérations, actes, ou omissions dans le cadre de la passation, la gestion et l'exécution des contrats présentant un risque de fraude.

L'objectif de lutte contre la fraude peut donner lieu à des croisements ponctuels de données provenant des traitements mis en œuvre par les entités, répondant aux finalités suivantes :

- la gestion commerciale de clients et de prospects ;
- la passation, la gestion et l'exécution des contrats portant sur les « services bancaires et financiers » tels que définis dans la présente autorisation unique ;
- la gestion des relations contractuelles avec les intermédiaires en opérations de banque et services de paiement, les prestataires de services ou autres tâches opérationnelles essentielles ou importantes visés à l'article 10, r, de l'arrêté du 3 novembre 2014, les sous-traitants, les délégataires ;
- 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 gestion des alertes résultant d'un « dispositif d'alerte professionnelle », qui doit s'effectuer conformément à l'autorisation unique 004, délibération n° 2005-305 du 8 décembre 2005 modifiée ou à la délibération individuelle autorisant le traitement ;
- la constitution par l'entité de listes des personnes dûment identifiées comme auteurs d'actes qualifiés de fraude ou de tentative de fraude externe ;
- la gestion des procédures amiables et contentieuses, consécutives à un cas de fraude, mises en œuvre conformément à la délibération n° 2016-005 du 14 janvier 2016 portant autorisation unique de traitements de données à caractère personnel mis en œuvre par les organismes publics et privés pour la préparation, l'exercice et le suivi de leurs contentieux ainsi que l'exécution des décisions rendues (AU-046) ou à la délibération autorisant le traitement.

Sur le partage des données relatives à la fraude entre les entités d'un même groupe :

Au regard de leurs activités et de leur organisation, les entités d'un même groupe peuvent être amenées à partager ponctuellement les informations relatives aux soupçons de fraude (visés par l'article L. 561-20 du CMF dans le cadre de la déclaration de soupçon en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme) et de cas de fraude avérée (option n° 1), ou à avoir recours à un traitement mutualisé intragroupe

dans lequel sont consignées les données relatives aux auteurs de fraudes avérées et à leurs victimes (option n° 2). Les entités adressant un engagement de conformité à la présente autorisation unique peuvent selon les structures organisationnelles et les moyens techniques opter soit pour la première option (partage ponctuel) soit pour la seconde (base mutualisée entre les entités d'un même groupe). Le choix entre ces deux options s'opère au niveau du groupe.

Option n° 1 : partage ponctuel des données :

Le principe du partage doit s'inscrire dans le strict cadre du respect des obligations des entités au regard de l'arrêté du 3 novembre 2014 relatif au contrôle interne et de l'article L. 511-34 du CMF autorisant le partage des données liées à la fraude au sein du groupe dès lors que le partage répond à la gestion adéquate d'un risque opérationnel et qu'il intervient dans les conditions fixées à l'article précité. Ces partages d'informations sont notamment prévus pour les besoins de :

- la surveillance sur base consolidée ;
- l'organisation de la lutte contre le blanchiment de capitaux et contre le financement du terrorisme ;
- l'organisation de la détection des opérations d'initié ou des manipulations de cours.

En particulier, le partage d'informations ne devra pas méconnaître le principe du secret professionnel (« secret bancaire ») tel que défini par l'article L. 511-33 du CMF, qui interdit la communication d'informations confidentielles à des tiers sans l'accord exprès et au cas par cas du client, sauf hypothèses limitativement énumérées par le CMF.

Le partage des données relatives aux fraudes est réalisé selon des modalités permettant de garantir la sécurité, la confidentialité et le cloisonnement des données ainsi que leur communication aux seules personnes habilitées au regard de leurs attributions.

Peuvent être traitées dans le cadre du partage des données relatives aux soupçons de fraudes visées par l'article L. 531-20 du CMF et de fraudes avérées les données suivantes :

- les données d'identification de l'auteur de la fraude avérée et de la victime : nom ; nom d'usage ; prénoms ; sexe ; date et lieu de naissance ; nationalité ; adresse, numéros de téléphone ; adresse électronique ;
- le motif d'inscription (auteur/victime) ;
- la nature de la fraude et la typologie de la fraude ;
- les données d'identification des personnes à contacter au sein de la cellule fraude de l'entité déclarante.

Dans le cadre de la constitution du traitement recensant les cas de fraude avérée, seules peuvent être habilitées à accéder à tout ou partie des données sous réserve qu'elles soient nécessaires à l'accomplissement de leurs attributions les personnes suivantes :

- les personnels habilités en charge de la lutte contre la fraude au sein de l'entité et/ou des entités d'un même groupe répondant aux critères de l'article 1^{er} de la présente autorisation unique ;
- les personnels habilités en charge de la lutte contre le blanchiment et le financement du terrorisme au sein de l'entité et/ou des entités d'un même groupe répondant aux critères de l'article 1^{er} de la présente autorisation unique.

La commission rappelle que les personnes chargées du recueil et du traitement des alertes doivent être en nombre limité, spécialement formées et astreintes à une obligation renforcée de confidentialité préalablement définie.

Option n° 2 : mutualisation intragroupe des données relatives aux auteurs de fraudes avérées et à leurs victimes :

Au regard de leurs activités et de leur organisation, les entités d'un même groupe peuvent avoir recours à un traitement mutualisé intragroupe dans lequel sont consignées les données relatives aux auteurs de fraudes avérées et à leurs victimes.

Le partage des données liées à la fraude vise en particulier à prévenir de nouveaux agissements frauduleux opérés par les mêmes auteurs au détriment d'une ou de plusieurs entités d'un même groupe ou de leurs clients. Ce partage s'inscrit également dans le cadre du respect des obligations des entités au regard de l'arrêté du 3 novembre 2014 relatif au contrôle interne et de l'article L. 511-34 du CMF et doit être effectué dans le respect du secret professionnel (« secret bancaire »), tel que défini par l'article L. 511-33 du CMF.

Le partage des données relatives aux fraudes avérées est réalisé selon des modalités permettant de garantir la sécurité, la confidentialité et le cloisonnement des données ainsi que leur communication aux seules personnes habilitées au regard de leurs attributions.

A ce titre, des garanties techniques devraient être mises en œuvre via le recours à un traitement fonctionnant sur le principe d'une conservation des données par chaque entité ou service dédié, qui doit garder la maîtrise des données sources en assurant une meilleure sécurisation des données et des mises à jour plus aisées tout en permettant de requêter les bases de données. Les garanties suivantes doivent être prévues :

- limiter les éléments strictement nécessaires aux personnes ayant le droit d'en connaître ;
- authentifier les intervenants au système par des solutions d'authentification forte assurant une traçabilité de qualité ;
- assurer un suivi strict de ces traces et limiter la typologie des informations requérables en fonction des profils des utilisateurs ;

- définir la politique de gestion des habilitations dans le respect de l'organisation du contrôle interne du responsable de traitement ;
- s'assurer de l'existence de clauses contractuelles spécifiques dans les contrats de travail notamment s'agissant de la confidentialité ;
- organiser les données entrantes, sortantes et leur utilisation de façon claire et sécurisée (dans le transport, le stockage et les accès) ;
- cloisonner les environnements de plus grande sensibilité dans un système d'information dédié qui ne soit pas en lien avec les environnements de production de l'entreprise. Les accès à ces environnements ne doivent être possibles que depuis des postes spécifiques appartenant à un réseau cloisonné et physique identifié.

De manière générale, des règles minimales d'inscription dans les listes de fraudeurs qui soient communes au groupe doivent être prévues, à savoir :

- les listes doivent être proportionnées afin de préserver la sectorisation : les fichiers mutualisés ou communs ne peuvent être mis en œuvre que dans le secteur d'activité bancaire et financier avec des garanties propres à assurer le respect de la sectorisation, qu'elles soient d'ordre technique (contrôle d'accès, gestion des habilitations, journalisation des connexions ou des interrogations) ou contractuel ;
- seules les personnes identifiées de manière certaine devront faire l'objet d'une inscription (adoption de mesures permettant de pallier tout risque d'homonymie, notamment dans des cas signalés d'usurpation d'identité) ;
- les motifs d'inscription doivent être préétablis et reposer sur des motifs objectifs opposables à la personne concernée, faisant abstraction de tout jugement de valeur ou d'une appréciation de son comportement ;
- l'inscription doit être effectuée par des agents ayant la compétence pour vérifier le caractère certain de la tentative ou de la fraude imputée à la personne concernée ;
- les durées de conservation des données enregistrées doivent être proportionnées au regard des motifs d'inscription. Des procédures de mise à jour régulière et de suppression des informations doivent être mises en œuvre ;
- la sécurité et la confidentialité des données doivent être assurées.

En cas de demande d'entrée en relation, le traitement mutualisé intragroupe sera consulté par le service en charge de la prévention de la fraude de l'entité. En cas d'occurrence, le dossier fera l'objet d'une analyse approfondie par les personnels habilités en charge de la lutte contre la fraude, qui vérifieront notamment s'il s'agit d'un cas d'homonymie, ou si la personne est connue pour avoir perpétré ou tenté de perpétrer des fraudes ayant entraîné des pertes financières pour le groupe. Si tel est le cas, l'entité pourra refuser l'entrée en relation contractuelle.

Peuvent être traitées dans le cadre du partage des données relatives aux fraudes avérées les données suivantes :

- les données d'identification de l'auteur de la fraude avérée et de la victime : nom ; nom d'usage ; prénoms ; sexe ; date et lieu de naissance ; nationalité ; adresse, numéros de téléphone ; adresse électronique ; les données relatives à son employeur lorsque la personne concernée est employée d'un intermédiaire en opérations de banque et services de paiement, d'un prestataire de services ;
- le motif d'inscription (auteur/victime) ;
- la nature de la fraude et la typologie de la fraude ;
- les données d'identification des personnes à contacter au sein de la cellule fraude de l'entité déclarante pour obtenir des informations complémentaires.

Dans le cadre de la constitution du traitement recensant les cas de fraude avérée, seules peuvent être habilitées à accéder à tout ou partie des données sous réserve qu'elles soient nécessaires à l'accomplissement de leurs attributions les personnes suivantes :

- les personnels en relation avec la clientèle (pour les seuls messages d'alerte dans le cadre de l'étude du contrat portant sur les services bancaires et financiers) ;
- les personnels habilités en charge de la lutte contre la fraude au sein de l'entité et/ou des entités d'un même groupe répondant aux critères de l'article 1^{er} de la présente autorisation unique ;
- les personnels habilités en charge de la lutte contre le blanchiment et le financement du terrorisme au sein de l'entité et/ou des entités d'un même groupe répondant aux critères de l'article 1^{er} de la présente autorisation unique.

En particulier, le partage d'informations ne devra pas méconnaître le principe du secret professionnel (« secret bancaire ») qui interdit la communication d'informations confidentielles à des tiers sans l'accord exprès et au cas par cas du client, sauf hypothèses limitativement énumérées par le CMF.

La commission rappelle que les personnes chargées du recueil et du traitement des alertes doivent être en nombre limité, spécialement formées et astreintes à une obligation renforcée de confidentialité préalablement définie.

Sur la nature des données traitées :

Les entités du secteur bancaire et financier sont confrontées à différents types de fraudes. L'analyse et la détection d'anomalie pouvant révéler une fraude externe dans le cadre de la passation, la gestion et l'exécution des contrats peuvent conduire au traitement de nombreuses données.

La commission rappelle que les données à caractère personnel ne peuvent être collectées que si elles sont adéquates, pertinentes et non excessives au regard de la finalité poursuivie. L'entité doit dès lors être en mesure de justifier du caractère nécessaire des données à caractère personnel effectivement collectées.

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

- la passation, la gestion et l'exécution des contrats portant sur les « services bancaires et financiers » tels que définis dans la présente autorisation unique ainsi que celles relatives à la gestion de la relation commerciale :
 - les données d'identification des personnes parties au contrat (client, bénéficiaire effectif, etc.), ainsi que les prospects ;
 - les données relatives à la situation personnelle, familiale et professionnelle, les informations d'ordre économique et financier et habitudes de vie en lien avec la conclusion des contrats portant sur les « services bancaires et financiers » tels que définis dans la présente autorisation unique ;
 - les données relatives aux opérations commerciales et au suivi de la relation commerciale ;
 - 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 et de la nature de la fraude présumée ou avérée et à ses suites ;
 - les données relatives à l'appréciation du risque, à la détermination ou à l'évaluation des préjudices ;
 - les données d'identification des personnes intervenant dans la détection et la gestion de la fraude ;
 - les données relatives aux mouvements financiers, aux moyens de paiement, aux transactions/opérations (y compris transactions financières) ;
 - les données de navigation et de connexion aux systèmes d'information, pouvant comprendre les données de localisation et les données relatives au matériel (y compris la configuration), collectées dans le cadre des contrats souscrits, sous réserve de respecter les dispositions applicables à toute action tendant à accéder par voie de transmission électronique à des informations déjà stockées dans l'équipement terminal de communication électronique ou à inscrire des informations dans cet équipement ;
- la gestion des relations contractuelles avec les prestataires de services ou de tâches opérationnelles essentielles ou importantes au sens de l'article 10, *r*, de l'arrêté du 3 novembre 2014, les intermédiaires en opérations de banque et services de paiement, sous-traitants, mandataires :
 - les données d'identification ;
 - les données relatives aux anomalies, aux incohérences et aux signalements pouvant révéler une fraude ;
 - les données relatives au suivi de la relation contractuelle ;
 - les données relatives aux investigations, à l'instruction du dossier de fraude et à l'évaluation du périmètre et de la nature de la fraude présumée ou avérée et à ses suites ;
 - les données relatives à l'appréciation du risque, à la détermination ou à l'évaluation des préjudices ;
 - les données d'identification des personnes intervenant dans la détection et la gestion de la fraude.

En tout état de cause, ces données ne peuvent être collectées que dans le cadre des finalités définies dans la présente autorisation unique ;

- la gestion administrative du personnel uniquement dans le cadre de requêtes ponctuelles et individuelles consécutives à la détection d'une fraude mixte (complicité d'un collaborateur de l'entité) :
 - noms ;
 - prénoms ;
 - identifiants ;
 - adresse de messagerie ;
 - numéro de téléphone ;
 - absences ou congés.

En tout état de cause, la lutte contre la fraude externe ne doit pas conduire à une surveillance automatisée et systématique du personnel.

Chaque entité procédant à un engagement de conformité à la présente autorisation unique devra tenir à jour une liste des critères et des scénarios utilisés à des fins de détection de la fraude externe, qu'elle devra mettre à disposition de la CNIL.

Dans le cadre de la présente autorisation unique les données ci-dessus sont traitées directement en lien avec les typologies de fraudes listées ci-dessous.

Typologie de fraudes externes :

- fraude aux moyens de paiement (fraude chèque, fraude virement, fraude prélèvement, lettre de change relevé et billet à ordre relevé, cavalerie, détournement de fonds/titres, vol de moyens de paiement) ;
- fraude monétique (fraude à la carte de paiement, fraude au terminal de paiement [« TPE »], cavalerie) ;
- fraude documentaire et identitaire (ouverture de compte avec faux justificatifs, demande de financement, de location ou de tout autre « service bancaire et financier » tel que défini dans la présente autorisation unique avec faux documents, contrefaçon/falsification de documents, fausse facture, fausse garantie, usurpation d'identité, faux justificatifs d'identité, fausse identité, fausse entreprise, fausse qualité) ;

- fraude crédit/leasing/location longue durée (détournement de gage, détournement/vol du matériel financé, double financement d'actif, financement d'actif fictif, revente par le client ou un tiers du bien en crédit-bail, location avec promesse de vente ou location longue durée, soit en fraude au droit de propriété de l'entité) ;
- fraude liée à l'affacturage (fausse facture, financement de factures non causées, règlement direct non remboursé, double mobilisation de créance) ;
- fraude visant les clients ou l'entité (faux placements, montage Ponzi, fraude à l'héritage, fausse loterie, fraude aux annuaires, fraude au président, ingénierie sociale).

Les entités adressant un engagement de conformité à la présente autorisation unique établissent une étude d'impact relative à la protection des données pour tout scénario de fraude qui n'est pas expressément listé ci-dessus. Cette étude documente la liste des critères et scénarios utilisés à des fins de détection de la fraude externe, les risques sous-jacents et les mesures prises afin de limiter les risques pour les droits et libertés des personnes concernées. Elle devra être mise à jour régulièrement, et être mise à disposition de la CNIL.

Sur la durée de conservation des données :

La commission rappelle que des données à caractère personnel ne peuvent être conservées, conformément à l'article 6 (5°) de la loi du 6 janvier 1978 modifiée, que le temps strictement nécessaire à l'accomplissement de la finalité pour laquelle elles ont été collectées.

Les entités disposent d'un délai de 12 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 12 mois sont supprimées.

En cas d'alerte pertinente, les données relatives à la fraude avérée 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 légales de prescription applicables.

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

Sur les destinataires des données :

Pour l'accomplissement des finalités précitées, seules peuvent être habilitées à accéder à tout ou partie des données sous réserve qu'elles soient nécessaires à l'accomplissement de leurs attributions, les personnes suivantes :

- pour les alertes :
 - les personnels habilités en charge de la lutte contre la fraude dans l'entité concernée ou au sein d'une autre entité du groupe en charge de la lutte contre la fraude lorsqu'elle agit pour le compte de l'entité ;
 - les personnels habilités en charge de la lutte contre le blanchiment et le financement du terrorisme au sein de l'entité ;
 - les inspecteurs, enquêteurs, auditeurs et experts, de manière ponctuelle dans le cadre d'enquêtes ;
 - le personnel habilité de la direction de la conformité en charge du contrôle interne ou du service du contentieux pour la gestion des contentieux au sein de l'entité ;
 - les autorités légalement habilitées dans le cadre de leurs missions ou de l'exercice d'un droit de communication ;
- pour les fraudes avérées :
 - les personnels en relation avec la clientèle (pour les seuls messages d'alerte liés à la fraude avérée dans le cadre de l'étude du contrat portant sur les « services bancaires et financiers » tels que définis dans la présente autorisation unique) ;
 - les personnels habilités en charge de la lutte contre la fraude dans l'entité concernée ou au sein d'une autre entité du groupe ;
 - les personnels habilités en charge de la lutte contre le blanchiment et le financement du terrorisme au sein de l'entité ;
 - la direction générale, les directions des risques opérationnels, le personnel habilité de la direction de la conformité en charge du contrôle interne ou du service du contentieux, de la direction juridique, les personnels en charge du contrôle interne, l'audit, l'inspection générale, la sécurité financière ;
 - les prestataires de services ou tâches opérationnelles essentielles ou importantes au sens de l'article 10, *r*, de l'arrêté du 3 novembre 2014, intermédiaires en opérations de banque et services de paiement, dès lors qu'ils sont concernés par la fraude ou interviennent dans la gestion des dossiers ou de maîtrise du risque de fraude ;
 - les inspecteurs, auditeurs, enquêteurs, et experts, de manière ponctuelle dans le cadre d'enquêtes ;
 - s'il y a lieu les victimes de fraudes ou leurs représentants ;
 - les autorités légalement habilitées, dans le cadre de leurs missions ou de l'exercice d'un droit de communication.

Ces personnes n'ont accès à ces données que pour autant qu'elles soient habilitées dans le cadre de leur activité et de l'organisation mise en place au sein de chaque entité ayant procédé à un engagement de conformité à la présente autorisation unique.

Sur l'information et sur les droits d'accès, de rectification et d'opposition des personnes :

Le responsable du traitement procède, conformément aux dispositions de l'article 32 de la loi du 6 janvier 1978 modifiée, à l'information des personnes concernées, en précisant notamment à cette occasion l'identité du responsable de traitement ou de son représentant, la finalité poursuivie, les destinataires ou catégories de destinataires des données, les durées de conservation applicables et les modalités d'exercice des droits des personnes (droits d'accès, de rectification et d'opposition pour motif légitime).

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 ne peut être prise sur le seul fondement de ces traitements automatisés. Dès lors, les alertes générées automatiquement doivent donner lieu à une analyse non automatisée par le personnel habilité de l'entité ou du groupe auquel elle 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.

Cette information s'effectue selon les modalités suivantes :

- les personnes concernées sont informées de l'existence du traitement de lutte contre la fraude au moyen des documents qui leur sont communiqués au moment de la souscription/conclusion du contrat, ou de tout autre support de communication échangé lors de l'exécution du contrat. L'information doit être concise, transparente, compréhensible et aisément accessible ;
- outre cette information générale, après 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, sauf disposition légale ou réglementaire contraire, informée individuellement par écrit des conséquences de cette inscription, en particulier du partage des données avec les entités du groupe concernées, en lui donnant la possibilité de présenter ses observations.

Les droits d'accès, de rectification et d'opposition définis au chapitre V de la loi du 6 janvier 1978 modifiée s'exercent directement auprès du ou des services que le responsable de traitement doit désigner.

Sur la sécurité des données et la traçabilité des actions :

Le responsable du traitement prend toutes précautions utiles pour préserver la sécurité des données traitées, 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. Cette politique devra décrire les objectifs de sécurité, et les mesures de sécurité physique, logique et organisationnelle permettant de les atteindre. Elle sera mise à jour régulièrement pour tenir compte des évolutions du contexte et des moyens permettant à tous ceux devant l'appliquer de la connaître seront mis en œuvre.

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, gérés conformément à l'état de l'art, ou par tout autre moyen d'authentification de même fiabilité ou de fiabilité supérieure.

Les droits permettant d'accéder aux données doivent être précisément définis en fonction des besoins réels de chaque utilisateur, 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 remis 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, etc.).

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 suffisantes en matière de sécurité des données.

Sur les 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 Privacy Shield ;
- 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 de clauses contractuelles types adoptées par la Commission européenne ou par l'adoption de règles internes d'entreprise (« Binding Corporate Rules », ou BCR) dont la CNIL a préalablement reconnu qu'elles garantissent un niveau de protection suffisant ;
- 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.

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

La présidente,
I. FALQUE-PIERROTIN