DECLARATION

16/10/2018

AU 54
Lutte contre la fraude externe dans le secteur bancaire et financier

LUTTE CONTRE LA FRAUDE EXTERNE DANS LE SECTEUR BANCAIRE ET FINANCIER

(Déclaration N° 54)

Suite à l'entrée en application du RGPD, les autorisations uniques adoptées par la CNIL n'ont plus de valeur juridique à compter du 25 mai 2018. Dans l'attente de la production de référentiels RGPD, la CNIL a décidé de les maintenir accessibles afin de permettre aux responsables de traitement d'orienter leurs premières actions de mise en conformité.

L'autorisation unique AU-054 encadre les traitements de données ayant pour finalité la lutte contre la fraude externe dans le secteur bancaire et financier.

Cette autorisation unique ne concerne que la fraude externe, c'est-à-dire la fraude commise dans le cadre de contrats portant sur les services bancaires et financiers, de la gestion de la relation commerciale, des relations contractuelles avec les prestataires et en cas de fraude mixte, de la gestion administrative du personnel. Les fraudes internes, commises par le personnel, les collaborateurs ou les administrateurs des entités doivent faire l'objet d'une autorisation spécifique.

Le traitement est limité à la détection d'anomalies, l'analyse et la gestion des alertes, ainsi que la constitution de listes d'auteurs de fraudes avérées, dans le cadre d'activités portant notamment sur les services et produits bancaires et financiers, ainsi que d'activités relatives aux produits et services dits « connexes».

Seules les entités visées au livre V du code monétaire et financier (CMF) ainsi que les filiales contrôlées par ces entités exerçant une activité qualifiée de « connexe » peuvent procéder à un engagement de conformité à cette autorisation unique. Par ailleurs, les responsables de traitements peuvent, dans des conditions strictement énumérées dans l'autorisation unique, opter soit pour un partage ponctuel au sein d'un groupe des données relatives aux soupçons de fraude et aux fraudes avérées, soit pour une mutualisation intra-groupe des données relatives aux fraudes avérées.

Cette autorisation unique fait partie du « pack conformité banque » et a été élaborée en collaboration avec les professionnels du secteur bancaire et financier.

TEXTE OFFICIEL

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)

SECTEURS D'ACTIVITE EXCLUS DU CHAMP DE LA NORME

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.

RESPONSABLES DE TRAITEMENT CONCERNES

Les entités 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 du CMF) ;
- être soumises aux dispositions de l'arrêté du 3 novembre 2014.

Il s'agit des entités suivantes :

- Les établissements de crédit ;
- Les intermédiaires en opérations de banque ;
- 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.

Les filiales contrôlées par les entités susmentionnées, pourvu qu'elles exercent une activité qualifiée de connexe, au sens de l'article L. 311-2 du CMF, et qu'elles relèvent du périmètre consolidé du contrôle interne, au sens de l'article 3 de l'arrêté du 3 novembre 2014.

OBJECTIF(S) POURSUIVI(S) PAR LE TRAITEMENT (FINALITES)

- La détection des actes réalisés dans le cadre des activités présentant une anomalie, une incohérence ou ayant été signalés comme pouvant relever d'une fraude. Ces actes peuvent par exemple consister en la remise d'une fausse fiche de paie, de faux justificatifs d'identité, ou en la communication d'informations contradictoires, ou une incohérence sur le lieu d'une opération, etc.
- Lutte contre la fraude mixte dans le secteur bancaire et financier ;
- La gestion des alertes (qui consiste à procéder à des vérifications, à demander des explications ou des justificatifs) ;
- La constitution de listes de personnes dûment identifiées comme auteurs d'actes qualifiés de fraude ou de tentatives de fraude externe. Cette personne est l'auteur d'un acte présentant une anomalie, qui, après vérification s'avère être une fraude avérée ou une tentative de fraude.

FINALITES EXCLUES DU CHAMP DE LA NORME

La lutte contre la fraude interne. La lutte contre le blanchiment et le financement du terrorisme (AU-003). La gestion des procédures amiables et contentieuses, consécutives à un cas de fraude, mises en œuvre conformément l'autorisation unique AU-046.

DONNEES PERSONNELLES CONCERNEES

Dans le cadre de la passation, la gestion et l'exécution des contrats portant sur les services bancaires et financiers et relativement à la gestion de la relation commerciale :

- les données d'identification des personnes parties au contrat (client, bénéficiaire effectif, etc.) et des 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 » ;
- 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 ;

Dans le cadre de 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 incohérences et 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.

Dans le cadre de la gestion administrative du personnel, s'agissant uniquement de requêtes ponctuelles et individuelles consécutives à la détection d'une fraude mixte :

- noms ;
- prénoms ;
- identifiants ;
- adresse de messagerie ;
- numéro de téléphone ;
- absences ou congés.

DUREE DE CONSERVATION DES DONNEES

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. 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.

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.

DESTINATAIRES DES DONNEES

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 ») ;
- 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.

INFORMATION DES PERSONNES ET RESPECT DES DROITS "INFORMATIQUE ET LIBERTES"

Il existe une obligation d'information générale conformément aux dispositions de l'article 32 de la loi informatique et libertés

L'information se fait à deux niveaux :

1. les personnes concernées 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 des personnes auteurs d'actes qualifiés de fraude ou de tentatives de fraude externe.
2. La personne concernée pourra 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 du contrat.
    - Si, après investigation, une décision produisant des effets juridiques est prise, la personne concernée est informée individuellement de ses conséquences, en particulier en cas de partage des données.

SECURITE ET CONFIDENTIALITE

Le responsable de 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.

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.

Le responsable de traitement doit également prendre 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 doivent prévoir l'existence de systèmes automatiques de traçabilité (journaux, audits, etc.)

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

TRANSFERTS DES DONNES HORS DE L'UNION EUROPEENNE

Les transferts sont possibles dans les conditions prévues par l'AU-054.