

Commission nationale de l'informatique et des libertés

Délibération n° 2015-229 du 9 juillet 2015 portant autorisation unique de traitements de données à caractère personnel aux fins de consultation du répertoire national d'identification des personnes physiques (RNIPP) mis en œuvre par les établissements du secteur bancaire et financier soumis aux obligations relatives aux comptes bancaires inactifs et des coffres inactifs ou par une personne mandatée à cet effet (AU-045)

NOR : CNIL1526006X

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 la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 25-II, 25-1 (6°) et 69 ;

Vu la loi n° 2014-617 du 13 juin 2014 relative aux comptes bancaires inactifs et aux contrats d'assurance vie en déshérence ;

Vu le code civil ;

Vu le code de commerce ;

Vu le code monétaire et financier ;

Vu le code général des impôts ;

Vu le code pénal ;

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 loi n° 2014-617 du 13 juin 2014 relative aux comptes bancaires inactifs et aux contrats d'assurance vie en déshérence renforce l'encadrement légal des comptes et des coffres forts inactifs ouverts dans les livres des établissements visés par la loi précitée. Elle rend notamment obligatoires le recensement annuel des comptes considérés comme inactifs selon les critères définis par cette loi et, sur la base de ce recensement, la recherche des titulaires décédés au moyen d'une consultation annuelle des données figurant au répertoire national d'identification des personnes physiques (ci-après « RNIPP »).

Ces traitements relèvent du 6° du I des articles 25 et 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.

La commission décide :

D'adopter une autorisation unique pour les traitements automatisés ou non de données à caractère personnel relevant de l'article 25-1 (6°). Les organismes mentionnés ci-dessous qui souhaiteront se référer à la présente autorisation unique adresseront à la commission un engagement de conformité pour leurs traitements qui répondent strictement aux conditions définies ci-dessous. Tous les traitements qui ne sont pas strictement conformes à la présente autorisation unique devront faire l'objet d'une demande d'autorisation spécifique présentant et expliquant les différences entre le traitement envisagé et l'autorisation unique.

Sur le champ d'application :

Sont concernés les établissements de crédit mentionnés au titre I^{er} du livre V ainsi que les établissements de monnaie électronique, les établissements de paiement mentionnés au titre II du même livre, les prestataires de services d'investissement ou de services connexes ci-après désignés « les Etablissements » et, le cas échéant, la ou les personnes mandatées à cet effet.

Pour consulter le fichier des personnes décédées issu du RNIPP, les Etablissements peuvent l'acquérir directement ou avoir recours à un tiers mandaté à cet effet selon les conditions fixées par la convention conclue avec l'INSEE, gestionnaire du RNIPP.

Sur la finalité du traitement :

Sont autorisés les seuls traitements de données à caractère personnel ayant pour finalité la recherche des titulaires décédés de comptes ou coffres-forts au moyen d'une consultation des données figurant au répertoire national d'identification des personnes physiques (RNIPP).

Les traitements peuvent être mis en œuvre par les établissements ou un tiers mandaté.

Les traitements mis en œuvre ont pour objet :

- la constitution et la tenue d'une base de données relative aux personnes dont le décès est connu de l'INSEE (ci-après « base de données »). Elle est mise à jour selon une périodicité *a minima* annuelle ;
- la vérification de l'éventuel décès du titulaire d'un compte ou coffre-fort recensé comme inactif par interrogation *a minima* annuelle de la base de données ;
- la mise en place d'une plate-forme sécurisée permettant l'interrogation de la base de données par les seuls établissements concernés ;
- la journalisation des requêtes et la réalisation des analyses statistiques sur l'interrogation de la base de données ;
- la conservation des informations relatives à une interrogation aux fins de preuve.

Les établissements pourront consulter la base de données selon deux modalités :

- par voie d'interrogation ponctuelle sur le titulaire d'un compte ou d'un coffre-fort ;
- par voie d'interrogations groupées, par l'envoi de fichiers portant sur tout ou partie des titulaires de comptes ou coffres inactifs recensés ; ces interrogations groupées pourront porter sur la totalité de la base ou sur les seuls signalements de décès reçus durant la dernière année.

La constitution et la mise à jour de la base de données nécessite la signature d'une licence d'usage entre les établissements ou le tiers mandaté et l'INSEE pour la consultation du RNIPP.

Les Etablissements seront informés de l'éventuel décès du titulaire d'un compte ou coffre-fort inactif. A ce titre, chaque établissement veillera à croiser cette information avec les autres informations dont il dispose déjà dans son dossier, sans collecter de données supplémentaires.

Les personnes mandatées auxquelles ont recours les établissements s'engagent, par voie contractuelle, à ne pas utiliser les données à d'autres fins que celles prévues par la loi du 13 juin 2014, à assurer leur confidentialité, à respecter la durée de conservation limitée des données et à procéder à la destruction ou à la restitution de tous les supports manuels ou informatisés de données à caractère personnel au terme de leurs mandats ou prestations.

Sur la nature des données traitées :

Les données pouvant être collectées dans le cadre de la recherche des titulaires décédés de comptes ou coffres-forts au moyen d'une consultation du RNIPP sont les suivantes :

En ce qui concerne l'interrogation de la base de données relative aux personnes dont le décès est connu de l'INSEE :

- nom de famille ou d'usage, prénoms ;
- sexe ;
- date et lieu de naissance ;

En ce qui concerne les données transmises en retour de l'interrogation de la base de données :

- nom de famille ou d'usage, prénoms ;
- sexe ;
- date et lieu de naissance ;
- date et lieu du décès ;
- numéro d'acte de décès.

En ce qui concerne les données de connexion à la base de données :

- les identifiants de connexion ;
- les informations d'horodatage ;
- les traces des accès aux journaux de connexion ;

Sur la durée de conservation des données :

Si l'information de décès transmise aux établissements est confirmée, les données issues du RNIPP sont archivées par les établissements jusqu'à l'expiration des délais prévus au 2° du III de l'article L 312-20 du code monétaire et financier soit 27 ans suivant la date de dépôt à la Caisse des dépôts et consignation s'agissant des comptes inactifs dont le titulaire est décédé.

Si l'information de décès transmise aux établissements est infirmée, les établissements conservent la preuve des interrogations annuelles du RNIPP permettant de justifier du respect de l'alinéa 3 du 2° du I de l'article L. 312-19 du code monétaire et financier jusqu'au dépôt effectif des comptes inactifs dans les conditions prévues à l'article L. 312-20 du code monétaire et financier soit une durée de dix ans suivant la dernière opération enregistrée permettant de considérer le compte comme inactif.

Pour les coffres-forts inactifs les établissements conservent pendant vingt ans la preuve des interrogations du RNIPP permettant de justifier du respect de l'alinéa 3 du 2° du I de l'article L. 312-19 du code monétaire et financier. Cette durée débute à la date prévue au deuxième alinéa du VI de l'article L. 312-20 du code monétaire et financier.

Les données personnelles enregistrées sont supprimées lorsqu'il apparaît avec certitude qu'elles se rapportent à un homonyme.

Sur les destinataires des données :

Peuvent seuls, dans les limites de leurs attributions respectives, avoir accès aux données à caractère personnel :

a) Dans le cadre des missions habituelles qui leur sont assignées et dont ils doivent répondre :

- les personnes intervenant au titre de la gestion des comptes et coffres forts inactifs ainsi que celles en charge de la gestion et de l'exécution des contrats ;
- les personnes chargées de la gestion des successions ;
- les gestionnaires habilités chargés de l'exploitation des fichiers de réponses issus des interrogations ponctuelles ou par lots de la base de données ;
- les personnels habilités des entités du même groupe auquel appartient le responsable de traitement dans le cadre de l'exercice de leurs missions ;
- les entités d'un même groupe, concernées par le décès de la personne, pour l'exécution et la gestion des contrats, et prestations de services ;
- les personnes en charge de la gestion de l'inactivité des comptes au sein des centres informatiques agissant pour le compte des établissements ;
- les mandataires et les sous-traitants ayant régularisé une convention avec l'établissement ;

b) En qualité de personnes intéressées au contrat :

- s'il y a lieu leurs ayants droit et représentants ;

c) En qualité de personnes habilitées au titre des tiers autorisés, notamment :

- s'il y a lieu les juridictions concernées, les arbitres, les médiateurs ;
- les autorités de tutelle et de contrôle et tous organismes publics habilités à les recevoir ;
- les services chargés du contrôle tels que les commissaires aux comptes et les auditeurs ainsi que les services chargés du contrôle interne ;
- les personnes habilitées de la Caisse des dépôts et consignation.

Les interrogations de la base de données ne peuvent être effectuées que par un nombre de gestionnaires habilités limité et adapté à la taille du portefeuille, disposant de certificats individuels et ayant vérifié la motivation des demandes d'interrogation.

Sur l'information des personnes :

Le responsable du traitement doit, conformément aux dispositions de l'article 32 de la loi du 6 janvier 1978 modifiée, informer les personnes concernées préalablement à la mise en œuvre du traitement.

Les clients sont informés que pour répondre à leurs obligations légales, l'établissement met en œuvre des traitements ayant notamment pour finalité l'identification des comptes et coffres-forts des personnes décédées.

Conformément aux obligations du code monétaire et financier et de la loi du 6 janvier 1978 modifiée, lorsqu'un compte ou un coffre-fort est considéré comme inactif, l'établissement doit en informer par tout moyen le titulaire du compte ou du coffre-fort, son représentant, la personne habilitée par lui ou, le cas échéant, ses ayants droit connus et leur indiquer les conséquences qui y sont attachées.

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

Le droit d'accès défini au chapitre V de la loi du 6 janvier 1978 modifiée s'exerce auprès du ou des services que le responsable du traitement aura désignés.

Sur la sécurité des données et la traçabilité des actions :

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 puissent en prendre connaissance.

Le responsable de traitement définit une politique de sécurité adaptée aux risques présentés par les traitements et à la taille de l'établissement. 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 conditions d'administration du système d'information prévoient l'existence de systèmes automatiques de traçabilité (journaux, audits...).

Tous les envois dématérialisés entre l'INSEE et les établissements ou entre l'INSEE et une personne mandatée font l'objet d'un chiffrement dont la clé est fournie sous pli séparé, en recommandé, avec accusé de réception. Les transmissions de la clé et des données se font successivement, en deux plis distincts, les données n'étant envoyées

qu'après retour à l'INSEE de l'accusé de réception du courrier contenant la clé. (à déterminer et préciser avec l'INSEE).

Les accès individuels à la base de la personne mandatée par les établissements si ces derniers ont choisi cette possibilité s'effectuent après authentification mutuelle du système hébergeant le traitement et de l'utilisateur par le biais de certificats délivrés par la messagerie sécurisée (RADAMESS). L'identification des machines connectées au traitement est également faite par des certificats de même nature.

Le certificat doit être nominatif et les mesures appropriées doivent être prises de manière à garantir qu'il ne sera utilisé que par son titulaire.

Les établissements conservent l'historique des requêtes ponctuelles effectuées sous leur responsabilité et pourront accéder aux interrogations conservées par la personne mandatée. Celle-ci garde une trace de toute interrogation pendant un an.

Toutes les connexions au traitement de données à caractères personnel font l'objet d'un chiffrage.

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
- 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 (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 « BCR », 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