

Macssi

Paris, le 22 février 2022

Conformité Informatique et
Libertés, Sécurité du SI



Destinataire(s) : Mesdames les directrices et Messieurs les directeurs des Caisses d'allocations familiales, Mesdames les directrices et Messieurs les directeurs de la Caisse nationale d'allocations familiales, Relais Informatique et Libertés des Caf, MSSSI

Objet : **Utilisation du NIR dans les traitements de données à caractère personnel**

Référence : Information technique 2022-030 du 22 février 2022

Périmètre d'application : Immédiate, Métropole et DROM

Textes de référence : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD – Règlement Général sur la Protection des Données) – Loi Informatique et Libertés

Mots clés : NIR, numéro de sécurité sociale, NIRPP, RNIPP, Données personnelles, RGPD, Règlement Général sur la Protection des Données, Loi Informatique et Libertés, CNIL, Commission Nationale de l'Informatique et des Libertés



Les contraintes qui pesaient sur le traitement du NIR (Numéro d'Inscription au Répertoire, plus connu sous l'appellation « numéro de sécurité sociale ») depuis la première version de la loi du 7 janvier 1978 (dite « Loi Informatique et Libertés ») ont été considérablement allégées pour la branche Famille.

Toutefois la CNIL reste vigilante et exige que le traitement de cette donnée hautement personnelle fasse l'objet d'une réflexion spécifique et documentée.

La présente instruction a pour but de clarifier cela de façon synthétique.

L'annexe fournit des éléments de contexte.

Le présent document s'applique également au NIA (NIR d'Attente).

1. Quelles sont les règles actuelles de traitement du NIR pour la branche Famille ?

Le décret n° 2019-341 du 19 avril 2019 « *relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire* », dans le 1. de son article 2.A, permet le traitement du NIR par les « *organismes chargés de la gestion d'un régime de base de sécurité sociale légalement obligatoire ou du service des allocations, prestations et aides mentionnés dans le code de la sécurité sociale et le code de l'action sociale et des familles* » – dont la branche Famille- « **Pour l'accomplissement de leurs missions en matière de protection sociale** ».

Cette rédaction très générique est favorable à la Branche.

De même, la Branche peut recourir à un prestataire extérieur (un sous-traitant au sens de l'article 4.8 du RGPD) pour que celui-ci assure la collecte et le traitement du NIR pour son compte, dans le strict respect des dispositions de l'article 28 du RGPD (Cf. l'IT 2020-027 sur les clauses RGPD qui doivent être imposées au sous-traitant).

Pour les traitements ayant pour finalité la recherche et la statistique publique et impliquant plusieurs acteurs, se reporter au chapitre 6. du présent document.

2. Quelles précautions doivent être prises quant au traitement du NIR par la branche Famille ?

Le principe général édicté dans l'article 5.1 du RGPD vient à s'appliquer : « *Les données à caractère personnel doivent être [...] c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données).* »

C'est pourquoi, dans sa délibération n° 2019-029 du 14 mars 2019 (portant avis sur le projet de décret cité *supra*), la CNIL exprime son souhait de ne pas voir traité le NIR par « facilité ».

Il revient donc au responsable de traitement (la Cnaf, la Caf) de documenter le fait que **le traitement de cette donnée est indispensable à l'atteinte de la finalité visée** (qu'il n'est pas possible de faire autrement) et d'être en mesure de le prouver :

« Elle [la CNIL] insiste sur le fait que chaque traitement mis en œuvre devra respecter ces principes et notamment celui relatif à la minimisation des données qui doit conduire à ne traiter le NIR qu'en cas de besoin justifié par la finalité du traitement concerné. »

« La CNIL n'est pas favorable à une utilisation systématique du NIR dans les dossiers des bénéficiaires. Ce numéro ne doit donc être demandé que si son enregistrement est pertinent ou justifié par un texte¹. »

¹ <https://www.cnil.fr/fr/cnil-direct/question/numero-de-securite-sociale-nir-dans-quels-cas-les-communes-et-les-departements>

La CNIL rappelle également qu'il faut veiller à la conformité de tout traitement portant sur le NIR, considérant qu'il s'agit d'une « donnée à caractère hautement personnel » :

« L'organisme doit s'assurer, avant de mettre en œuvre son traitement, que celui-ci respecte l'ensemble des principes et obligations du règlement général sur la protection des données (RGPD) et de la loi « Informatique et Libertés » (principe de minimisation, transparence vis à vis des personnes concernées, obligation de sécurité, etc.). ».

Ces points sont traités dans le cadre de chaque projet et documentés au sein du Dossier Informatique et Libertés formalisé par le RIL (au sein d'une Caf) / par la Macssi (au sein de la Cnaf) avec l'aide principale du chef de projet MOA Métier concerné.

Pour les projets initiés au niveau de la Cnaf, une case permet au créateur d'une Feb (Fiche d'expression de besoins) d'indiquer qu'une analyse informatique et libertés et/ou de sécurité informatique est requise « notamment en présence de données personnelles, de NIR, ou de leur transmission ».

3. Quels sont les points principaux de vigilance de la CNIL en cas de traitement du NIR ?

Au fil de ses délibérations, **la CNIL revient régulièrement sur des « écueils fréquents » qu'elle a identifiés en cas de traitement du NIR**, tels que la transmission du NIR à un tiers qui n'a pas légitimité à traiter cette donnée ou une conservation excessive de cette donnée dès lors que l'objectif visé a été atteint.

Elle est également vigilante à la bonne sécurisation de cette donnée et à l'information des personnes :

« Outre la nécessité de figurer dans le décret pour ce qui concerne la collecte et le traitement du NIR, l'organisme doit s'assurer, avant de mettre en œuvre son traitement, que celui-ci respecte l'ensemble des principes et obligations du RGPD et de la loi Informatique et Libertés (principe de minimisation, transparence vis à vis des personnes concernées, obligation de sécurité, etc.)². »

Dans le cadre de chaque projet, ces points sont étudiés et documentés dans le « Dossier Informatique et Libertés » établi par le RIL en Caf (et la Macssi au sein de la Cnaf) avec l'aide principale du chef de projet MOA Métier, préalable à une inscription au registre des traitements au titre de l'article 30 du RGPD.

Selon le niveau de risque qu'est susceptible de faire courir le traitement projeté pour les personnes concernées, une analyse d'impact peut être formalisée en sus au titre de l'article 35 du RGPD. Dans ces deux documents (Dossier Informatique et Libertés et Analyse d'impact) dont la CNIL peut demander communication à tout moment, sont décrites a) la raison impérieuse qui oblige à traiter le NIR ; b) sa durée de conservation et l'objectivation de celle-ci ; c) les mesures de sécurité prises pour en assurer la protection.

Les bonnes questions à se poser :

- Avons-nous vraiment besoin de traiter le NIR pour atteindre l'objectif fixé ?
- Saurions-nous le justifier en cas de contrôle de la CNIL ?
- Avons-nous mis en œuvre les mesures de protection adéquates ?

² Source : « Numéro d'inscription des personnes dans le secteur social : le décret « cadre NIR » en question », site Web de la CNIL

4. Quelques exemples concrets

Conforme : Consultée, la CNIL a accepté que le NIR soit utilisé par la branche Famille comme identifiant donnant accès aux espaces personnels dans le cadre de la gestion à la personne (dispositif CALP)., en remplacement de l'ensemble « numéro matricule + numéro du département + MM/AA de naissance » .

Conforme : Dans le cadre de l'enregistrement des assistants maternels sur un nouvelle version du site mon-enfant.fr, le NIR est collecté uniquement pour pouvoir interroger en temps réel le SNGI³ afin de vérifier la concordance entre les prénoms saisis par l'internaute et ceux figurant au fichier géré par la Cnav. Aussitôt l'assurance raisonnable obtenue que l'internaute est bien la personne qu'il prétend être, le NIR est purgé (il n'est pas mémorisé dans le système d'information de la Branche).

Conforme : Afin de traiter les impacts du Brexit sur les dossiers des citoyens du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, une interaction a été réalisée avec la totalité des responsables des dossiers dans lesquels ce dernier ou son conjoint présentant un code de nationalité « C » nés dans les pays concernés. Cette dernière information a été obtenue par lecture du NIR.

Non conforme : Le NIR ne doit pas être collecté et traité durant la phase de recrutement. *« De manière générale, l'employeur ne doit collecter que les données dont il a réellement besoin, et ne doit le faire qu'à partir du moment où ce besoin se concrétise. Exemple : lors de la conclusion d'un contrat de travail, l'employeur a l'obligation d'accomplir certaines formalités déclaratives qui requièrent le traitement du numéro de sécurité sociale (NIR) des salariés. Si cette utilisation est alors justifiée, elle ne saurait être demandée à un candidat avant la validation définitive de sa candidature⁴. »*. En revanche, le traitement du NIR par les employeurs est légitime pour la gestion de la paie, le calcul des cotisations versées aux organismes de protection sociale et la gestion des dispositifs d'épargne salariale.

Non conforme : Le numéro de sécurité sociale n'est pas utile pour l'inscription à l'école ou aux activités périscolaires (*« Les communes ne doivent pas enregistrer le numéro de sécurité sociale ni l'utiliser comme identifiant de l'élève. Elles ne sont pas autorisées non plus à demander la copie de l'attestation de sécurité sociale. »*).

Non conforme : Une agence immobilière ne peut pas exiger la communication du NIR à une personne qui recherche à louer un appartement.

À étudier et à justifier : Le traitement du NIR est parfois envisagé uniquement pour limiter le risque d'homonymie. Cela ne peut être envisagé que pour un ensemble qui concerne un grand nombre de personnes et dans le cadre d'un traitement pour lequel il est démontré qu'il n'est pas possible de limiter le risque en traitant un ensemble de données jugées plus « anodines » comme les nom, prénom, lieu et date de naissance.

En cas de doute, ne pas hésiter à solliciter le RIL (au sein d'une Caf) ou la Macssi (au sein de la Cnaf).

³ Le Système national de gestion des identités (SNGI) est un système de traitement automatisé français mis en œuvre par la Caisse nationale d'assurance vieillesse (CNAV). Situé sur le site informatique de Tours, ce fichier contient l'identité des personnes nées en France et les personnes nées à l'étranger qui viennent travailler en France à partir du simple numéro de sécurité sociale (NIR).

⁴ Source : « Référentiel relatif à la gestion des ressources humaines », CNIL, avril 2020

5. Faut-il sécuriser les NIR d'une façon spécifique ?

Le NIR n'est pas identifié par le RGPD comme une donnée relevant de son article 9 (« catégories particulières de données à caractère personnel »), c'est-à-dire comme une donnée dite « sensible ».

Il n'existe donc pas de règle imposant la mise en œuvre d'une sécurisation particulière du NIR. Ceci est étudié au cas par cas, dans le cadre de la formalisation du « Dossier Informatique et Libertés » et des risques que le traitement est susceptible de faire peser sur les personnes concernées.

Notons qu'il n'est pas possible de changer de NIR si celui-ci a été exposé. Ainsi, en février 2021, un fichier contenant près de 500.000 numéros de sécurité sociale de citoyens français provenant de 27 laboratoires médicaux a « fuité », avec l'identité des personnes et leur adresse. Cette base de données a circulé gratuitement et massivement pendant plusieurs jours, à la fois dans les milieux cybercriminels et parmi les experts en cybersécurité. Si les autorités ont pris quelques mesures pour limiter sa diffusion, il n'est plus possible de l'empêcher. Le fichier a été téléchargé et copié des milliers de fois et continuera de s'échanger. De même, l'AP-HP a porté plainte en septembre 2021 à la suite du vol de 1,4 million de NIR associés aux noms et coordonnées de personnes ayant subi un test de détection de la COVID-19.

Il est donc relativement facile de se procurer, dans le *Darknet*⁵, des ensembles « Nom/Prénom/NIR/Date de naissance/Lieu de naissance ». C'est la raison pour laquelle la simple consultation du SNGI ne peut pas être considérée à elle seule comme l'obtention d'une assurance absolue de l'identité réelle d'un internaute (s'agit-il bien de la personne que l'internaute prétend être ?) mais seulement d'une assurance « raisonnable » et qu'a été mis œuvre en sus un appel au service DocVérif qui permet de vérifier le statut d'un titre d'identité auprès du Ministère de l'intérieur.

6. Le « NIR statistique » ou CSNS (Code Statistique Non Signifiant)

L'article 30 de la Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés prévoit deux cas d'usage qui dérogent au « décret NIR » : Les traitements qui ont exclusivement des finalités de statistique publique et sont mis en œuvre par le Service Statistique Public (SSP)⁶ ; Les traitements qui ont exclusivement des finalités de recherche scientifique ou historique.

Cette dérogation n'est applicable que si le NIR fait préalablement l'objet d'une opération cryptographique lui substituant un code statistique non signifiant (c'est à dire l'application d'un *hash*⁷, d'une empreinte).

Pour les traitements qui ont exclusivement des finalités de recherche scientifique ou historique, l'opération cryptographique et, le cas échéant, l'interconnexion de deux fichiers par l'utilisation du code spécifique non signifiant qui en est issu ne peuvent être assurées par la même personne ni par le responsable de

⁵ Le *Darknet* est un réseau présent dans internet qui utilise des protocoles spécifiques intégrant des fonctions d'anonymat de façon à permettre à ses utilisateurs de communiquer sans grande crainte d'immixtion de la part de gouvernements. Pour ces raisons, les darknets sont souvent associés à la communication de type dissidence politique et aux activités illégales.

⁶ Le service statistique public comprend l'Institut national de la statistique et des études économiques et les Services Statistiques Ministériels (SSM) (Cf. Article 1er de la loi n°51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques.

⁷ On nomme fonction de hachage (ou *hash function*) une fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte numérique servant à identifier rapidement la donnée initiale.

traitement. L'article 30 précise que « Cette opération est renouvelée à une fréquence définie par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés. ».

Un arrêté a été publié le 28 septembre 2020 relatif au CSNS (Code Statistique Non Signifiant), calculé à partir du NIR, pris en application du décret n° 2016-1930 du 28 décembre 2016 portant simplification des formalités préalables relatives à des traitements à finalité statistique ou de recherche.

Il précise que « La solution mobilisée pour l'opération cryptographique en vue de la production d'un code statistique non signifiant (CSNS) s'appuie sur des algorithmes de chiffrement éprouvés, conformes à la politique de sécurité des systèmes d'information de l'Etat (PSSIE) et aux standards de sécurité produits par le fonctionnaire de sécurité des systèmes d'information des ministères économiques et financiers. Cette solution inclut l'enregistrement des accès à toutes les fonctions mobilisées pour les besoins de sa mise en œuvre ainsi qu'aux clés de chiffrement. L'opération cryptographique citée est placée sous l'autorité du directeur général de l'INSEE. ».

Il convient toutefois de noter que le CSNS, qui facilite les appariements entre plusieurs acteurs, est réservé au seul SSP.

Une telle disposition permet le traitement par l'INSEE ou des SSM de données relatives à un ensemble de personnes identiques, par plusieurs responsables de traitements différents qui visent une même finalité de recherche scientifique ou historique, sans que jamais le NIR soit utilisé (il serait remplacé par le CSNS).

Il est espéré une évolution des textes qui permettrait à la Cnaf d'utiliser le CSNS.

7. Quels sont les risques à traiter le NIR d'une façon non conforme ?

Aux risques de voir la CNIL utiliser ses pouvoirs (contrôle, avertissement - dont publics-, mises en demeure, sanctions), s'ajoutent ceux de l'article 226-16-1 du Code pénal :

« Le fait, hors les cas où le traitement a été autorisé dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 précitée, de procéder ou faire procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. »

Annexe

- Note Macssi « Le NIR : une donnée hautement identifiante, du berceau au tombeau »

Pour aller plus loin

- [Décret n° 2019-341 du 19 avril 2019](#) relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire

- [Délibération n° 2019-029 du 14 mars 2019](#) portant avis sur un projet de décret pris pour application de l'article 22 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Page « [Tout savoir sur le décret « cadre NIR » dans le champ de la protection sociale](#) » sur le site web de la CNIL