CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Délibération n° 2017-039 du 23 février 2017 portant avis sur un projet de décision de la Caisse nationale des allocations familiales relative au simulateur de droit au RSA et au téléservice de demande de RSA sur le site web caf.fr.

(demande d'avis n° 2028786)

La Commission nationale de l'informatique et des libertés,

Saisie par la Caisse nationale des allocations familiales d'une demande d'avis sur un projet de décision relative au simulateur de droit au RSA et au téléservice de demande de RSA sur le site caf.fr ;

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 de l'action sociale et des familles, notamment ses articles L. 262-29 et R. 262-25-5 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 27-II-4° ;

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 le décret n° 2017-122 du 1er février 2017 relatif à la réforme des minima sociaux ;

Vu la délibération n° 93-056 du 29 juin 1993 relative au traitement CRISTAL de gestion des prestations familiales et de l'aide sociale mis à la disposition des caisses d'allocations familiales ;

Vu la délibération n° 2009-327 du 4 juin 2009 portant avis sur un projet de décret en Conseil d'Etat relatif au revenu de solidarité active (RSA) et un projet d'arrêté relatif à l'échantillon national interrégimes d'allocataires de minima sociaux (ENIAMS) ;

Vu la délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe ;

Après avoir entendu Mme Marie-France MAZARS, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations,

Émet l'avis suivant :

Le décret n° 2017-122 du 1er février 2017 relatif à la réforme des minima sociaux a créé un article R. 262-25-5 dans le code de l'action sociale et des familles (CASF) qui précise que la demande de Revenu de solidarité active (RSA) peut être réalisée soit par téléservice, soit par le dépôt d'un formulaire.

Afin de mettre en application cette disposition, la Caisse nationale des allocations familiales (CNAF) a procédé à la refonte de son site web (caf.fr) et y a intégré un nouveau simulateur de droit au RSA et un téléservice permettant de réaliser une demande de RSA en ligne.

Le projet de décision de la CNAF encadre la mise en œuvre de téléservices impliquant le Numéro d'inscription au Répertoire national d'identification des personnes physiques (NIR) et est donc soumis à l'avis de la Commission sur le fondement de l'article 27-II-4° de la loi du 6 janvier 1978 modifiée.

La Commission note que le site caf.fr a fait l'objet d'une formalité concernant les services suivants :

- dialogue et relation usager/CAF ;
- consultation authentifiée du dossier par l'allocataire ;
- simulation de droits (dans sa version antérieure).

Il résulte de l'instruction de la demande d'avis que la présente demande est limitée à l'encadrement des traitements suivants :

- un simulateur de droit au RSA (nouvelle version) nécessitant le renseignement de données indirectement identifiantes ;
- un téléservice permettant d'effectuer principalement une demande de RSA en ligne mais également une demande de Couverture maladie universelle complémentaire (CMU-C), et permettant de saisir les données socio-professionnelles nécessaires à l'accomplissement, par les conseils départementaux, de leur mission d'accompagnement dans l'insertion sociale et l'orientation professionnelle des bénéficiaires du RSA, en application de l'article L. 262-29 du CASF.

Le présent avis recommande que soient apportées des précisions, dans l'acte réglementaire, sur les catégories de données traitées, les durées de conservation des données, les destinataires des données et les modalités d'information des personnes. L'avis est particulièrement développé sur les mesures de sécurité et de confidentialité prises pour la mise en œuvre du traitement.

Constatant l'essor des téléprocédures, la Commission souhaite insister sur l'importance de prendre en considération les difficultés auxquelles peuvent être confrontés les usagers soumis à l'accomplissement de formalités dématérialisées (difficulté d'accès à internet ou encore insuffisance des connaissances dans le domaine du numérique). C'est pourquoi, elle estime nécessaire d'accompagner les usagers, en les informant notamment des dispositifs leur permettant d'être assistés dans leurs démarches, tels que les espaces publics numériques (EPN). A cet égard, la Commission recommande que cette information soit portée à la connaissance des utilisateurs des services de la CNAF, en renvoyant notamment vers le répertoire des lieux d'accès publics (http://www.netpublic.fr/net-public/espaces-publics-numeriques/repertoire-national/).

Sur la finalité du traitement :

Le traitement a pour finalité la mise en place du simulateur de droits et du téléservice prévu par le décret du 1er février 2017.

S'agissant du simulateur, il convient de noter qu'un usager, ayant obtenu une simulation positive, a la possibilité de continuer ses démarches en réalisant une demande de RSA en ligne. Dans ce cas, les données renseignées dans le simulateur sont reportées dans le téléservice de demande de RSA. De plus, un allocataire connecté sur son espace personnel du site de la CAF et effectuant une demande de RSA en ligne, voit ses données alimenter automatiquement le formulaire de demande de RSA pour lui éviter de devoir les ressaisir.

S'agissant du téléservice, l'objet principal est de permettre la réalisation d'une demande de RSA. Cependant, dans la mesure où certaines données collectées dans le cadre de la demande de RSA sont aussi nécessaires à l'instruction des demandes de CMU-C, il est proposé aux demandeurs de RSA d'effectuer également, via l'outil, une demande de CMUC-C. Les données sont alors adressées aux organismes concernés de la branche Maladie.

Bien que cette transmission d'informations ait déjà fait l'objet d'une formalité distincte auprès de la CNIL, la Commission estime qu'il serait important que cette fonctionnalité, présente dans le téléservice de demande de RSA, soit mentionnée dans le projet de décision de la CNAF.

De même, la Commission estime que la collecte de données socio-professionnelles destinées uniquement aux Conseils départementaux, facilitée par le téléservice de demande de RSA, devrait également être mentionnée dans le projet d'acte réglementaire.

La Commission considère que les finalités du traitement sont déterminées, explicites et légitimes.

Sur la nature des données traitées :

La Commission prend acte de ce que les données collectées dans le cadre du téléservice de demande de RSA sont celles qui sont collectées au moyen des formulaires CERFA correspondants. S'agissant du simulateur, les données collectées sont indirectement identifiantes et sont nécessaires à l'évaluation du droit au RSA.

La Commission note que le projet de décision identifie les catégories de données collectées dans le cadre des traitements mis en œuvre sur le site de la CNAF. Elle considère, s'agissant des traitements effectivement soumis à son étude dans le cadre de la demande d'avis, que les catégories de données listées apparaissent adéquates, pertinentes et non excessives au regard de la finalité poursuivie par le responsable de traitement.

Néanmoins, pour renforcer la clarté et la lisibilité du projet d'acte réglementaire, la Commission recommande, premièrement, que les catégories de données, désignées de manière trop large, soient davantage précisées et, deuxièmement, que soient

distinguées les catégories de données traitées en fonction des services concernées (simulateur de droits, demande de RSA, demande de CMU-C, saisie des données socio-professionnelles).

Sur la durée de conservation des données :

S'agissant du simulateur de droits, la Commission prend acte que les informations renseignées sont conservées pendant trente minutes afin de permettre à l'usager de procéder à une demande de RSA sur la base des informations indirectement identifiantes, déjà renseignées dans le simulateur.

S'agissant du téléservice de demande de RSA, le projet d'acte réglementaire indique que les informations renseignées sont supprimées dès lors qu'elles ont été transmises aux « traitements concernés ». Il est ressorti de l'instruction de la demande d'avis que la notion de « traitements concernés » visait l'outil de paiement des allocations (« Cristal », pour « Conception relationnelle intégrée du système de traitement des allocations ») ainsi que l'outil d'instruction des demandes de RSA (« @RSA »), sur lesquels la Commission a déjà rendu un avis.

La Commission estime que les données enregistrées dans ce téléservice sont conservées pour une durée qui n'excède pas la durée nécessaire à la finalité pour laquelle elles sont collectées et traitées mais recommande que le projet de décision mentionne expressément les « traitements concernés » ayant vocation à recevoir les données.

Sur les destinataires des données :

La Commission prend acte que la création du téléservice de demande de RSA ne vient pas modifier les flux existants des données collectées *via* le formulaire papier de demande de RSA.

S'agissant des données collectées dans le cadre du simulateur de droits, la Commission prend acte qu'elles ne sont adressées à aucun destinataire au sens de la loi du 6 janvier 1978 modifiée.

S'agissant des données collectées dans le cadre de la demande en ligne de RSA, via l'outil @RSA, les destinataires sont les organismes participant à la gestion du RSA :

- les Caisses d'allocations familiales (CAF) ;
- les Caisses de la Mutualité sociale agricole (CMSA) ;
- les Conseils départementaux (ou métropoles) et les Centres communaux d'action sociale (CCAS).

La Commission considère que ces destinataires présentent un intérêt légitime à accéder aux données du présent traitement, dans la limite de leurs attributions et sous réserve que les données effectivement accessibles présentent un lien direct et nécessaire avec leurs fonctions. Elle estime que devraient également être mentionnés, dans l'acte réglementaire, les destinataires des données relatives à la demande de CMU-C et des données socio-professionnelles qui disposent des données *via* l'outil @RSA.

Sur l'information des personnes :

Il ressort du dossier descriptif du traitement que les personnes concernées sont informées des mentions de l'article 32 de la loi du 6 janvier 1978 modifiée *via* :

- le site web de la CNAF ;
- le formulaire papier CERFA n° 15481*01 et 15482*01;
- les écrans du téléservice de demande du RSA ;
- les courriers de notification adressés par leur CAF de rattachement (notification d'ouverture de droit ou de fin de droit).

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

Les personnes peuvent exercer leurs droits d'accès et de rectification, prévus aux articles 39 et 40 de la loi du 6 janvier 1978 modifiée, auprès du directeur de la CAF de rattachement.

La Commission note qu'en revanche, le droit d'opposition est écarté par le projet d'acte réglementaire.

Sur la sécurité des données et la traçabilité des actions :

Afin de déterminer si la personne est éligible au RSA et de calculer les droits associés le cas échéant, la CNAF utilise un premier module développé par un prestataire, hébergé au sein de l'Union européenne, qui exécute les règles de calculs du simulateur. Un second module est mis à disposition par le prestataire et sert d'intermédiaire entre le système d'information (SI) de la CNAF et le premier module.

La Commission note tout d'abord que l'ensemble des écrans du téléservice est en HTTPS. Dans sa démarche d'engagement responsable, visant à mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données (*accountability*), la CNAF a initié une procédure d'homologation RGS du téléservice, laquelle devrait être prononcée avant la fin du premier semestre 2017 et affichée sur l'écran d'ouverture de la téléprocédure. Par ailleurs, une analyse de risque et d'impacts pour les personnes concernées, une des composantes du dossier d'homologation RGS précité, a été menée. La Commission prend cependant acte que le téléservice n'entre pas dans le cadre du plan de gestion d'incidents de la CNAF et recommande de l'y faire figurer.

La Commission souligne que les échanges entre le téléservice et le premier module s'effectuent via une liaison HTTPS avec authentification mutuelle. Par ailleurs, afin de renforcer la sécurité des communications, un canal de communication pérenne chiffré a été établi entre le SI CNAF à Sophia Antipolis et l'un des sites européens du prestataire.

La Commission prend acte que le téléservice et les modules du prestataire ne conservent pas les données traitées en dehors du temps nécessaire à la réalisation de leurs tâches. Les données ne sont conservées qu'en cas de simulation de droits positive, et ce pendant une durée de 30 minutes, afin que l'utilisateur puisse, à la suite de la simulation, effectuer une demande de RSA en ligne. Les données ne sont alors accessibles que par la téléprocédure de demande et il est nécessaire que l'utilisateur

continue et finalise sa démarche afin que l'information soit enregistrée, par la CNAF, dans son SI, et que la prestation se mette en place.

Les modules du prestataire ne conservent, quant à eux, aucune donnée, en dehors de journaux techniques. La Commission rappelle, à toutes fins utiles, qu'en dehors de dispositions légales particulières, les journaux doivent être conservés sur une période glissante ne pouvant excéder 6 mois.

Afin de réaliser la demande de RSA et s'il souhaite voir la simulation pré-remplie en partie, l'allocataire doit se connecter sur son espace personnel « Mon Compte ». L'utilisateur s'authentifie avec son numéro d'allocataire, code poste de résidence, date de naissance et mot de passe sur un clavier virtuel. Le primo demandeur, n'étant pas connu des services de la CAF, ne dispose pas d'un espace personnel et a librement accès au téléservice de demande de RSA. Une fois la demande réalisée, il se voit attribuer un matricule ainsi qu'un mot de passe provisoire pour accéder à l'espace personnel que lui aura alors créé la CAF. Le mot de passe est envoyé par SMS si l'utilisateur a renseigné un numéro de téléphone portable ou par courrier postal à défaut. Le mot de passe initial doit être changé lors du premier accès à l'espace personnel.

La Commission note que le mot de passe de l'utilisateur doit être composé de 8 chiffres, que ces chiffres ne doivent pas correspondre à certains schémas, que le mot de passe a une durée de vie de 2 ans. Par ailleurs le compte de l'utilisateur se bloque pour une durée déterminée après 5 tentatives infructueuses. La Commission rappelle que, dans sa recommandation n° 2017-012 du 19 janvier 2017, il est souhaité qu'une temporisation d'accès au compte après plusieurs échecs, dont la durée augmente exponentiellement dans le temps, soit mise en œuvre.

La Commission relève que chaque mot de passe précité est stocké haché au sein de la base de données. Chaque condensat est calculé avec injection d'un sel distinct, sel lui-même stocké dans la même base de données mais chiffré. Les clés de chiffrement sont stockées en interne, sur des équipements de sécurité à accès restreint.

La Commission prend acte que les administrateurs du système s'authentifient sur les ressources du SI à l'aide de couples identifiants et mots de passe :

- S'agissant des postes de travail, la Commission note que les mots de passe doivent comporter 8 caractères, être complexes (3 types de caractères parmi les 4), être différents des 2 mots de passe précédents et changés tous les 90 jours. Après 5 tentatives infructueuses, le compte de l'utilisateur est bloqué et il est nécessaire que le service support intervienne afin de le débloquer.
- S'agissant des comptes du SaaS (s*oftware as a service*) du prestataire, le Commission relève que les mots de passe doivent comporter 8 caractères, être complexes (a minima un chiffre, une lettre majuscule et une lettre minuscule) et être renouvelés tous les 4 mois. Les comptes sont nominatifs individuels, non partagés. Le dispositif ne prévoit pas de mesures de restriction en cas d'erreurs successives d'authentification.
- S'agissant des comptes d'administration de caf.fr, la Commission note que les mots de passe ne sont contraints par aucune modalité particulière, ni longueur, ni complexité, ni durée de vie.

La Commission rappelle qu'elle recommande, pour ces deux derniers cas, que les mots de passe fassent une longueur minimale de 12 caractères et soient composés de lettres

majuscules, minuscules, chiffres et symboles ou qu'ils fassent entre 8 et 11 caractères, soient composés de trois des quatre possibilités précitées et associés à une restriction d'accès en cas d'erreurs successives (blocage de compte temporaire, possibilité de tentatives après une durée incrémentielle, etc.).

La Commission note qu'aucune revue des droits d'accès des agents n'est effectuée et suggère fortement qu'une revue soit réalisée a minima une fois par an, mais relève que des analyses de vulnérabilités mensuelles sont effectuées par une équipe interne et que des tests d'intrusion sont effectués par des prestataires extérieurs spécialisés a minima tous les deux ans.

La Commission prend acte que le site de la CNAF situé à Sophia Antipolis met en œuvre un dispositif de vidéo-surveillance, un gardiennage sur site en 24/24, un contrôle d'accès individuel par badge ainsi qu'un dispositif de détection d'intrusion et d'incendie. Par ailleurs, les salles machines voient leur circuit d'alimentation électrique redondés (onduleurs et groupes électrogènes) et disposent d'un groupe de climatisation. La Commission recommande de redonder également le système de refroidissement. Enfin, votre rapporteur note que des sauvegardes sont effectuées, un jeu étant gardé sur site en interne, un autre étant externalisé.

Sous réserve de l'effectivité de l'ensemble des éléments précités, la Commission considère que la sécurité du dispositif est assurée de façon adéquate, conformément aux prescriptions de l'article 34 de la loi du 6 janvier 1978 modifiée

La Commission rappelle toutefois que cette obligation de sécurité nécessite la mise à jour des mesures de sécurité au regard de la réévaluation régulière des risques.

La Présidente

I. FALQUE-PIERROTIN