PROJET DE RÉFÉRENTIEL

CONCERNANT L'EVALUATION DE LA SOLVABILITE DANS LE CADRE DE L'OCTROI DE CREDIT

Version soumise à consultation publique jusqu'au 18 juillet 2025

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table des matières

1. A qui s'adresse ce référentiel ?

Ce référentiel s'adresse aux organismes privés habilités à octroyer des prêts au titre des articles L. 511-5, L. 511-6 et L. 518-1 du code monétaire et financier (CMF).

Le référentiel s'applique aux traitements mis en œuvre à des fins d'évaluation de la solvabilité des personnes concernées exclusivement dans le cadre des crédits encadrés par les dispositions des chapitres II et III du titre I du livre 1 de la partie législative du code de la consommation (articles L. 312-1 à L. 312-95 et L. 313-1 à L. 313-64).

Le référentiel ne s'applique pas aux traitements mis en œuvre par les intermédiaires en opérations de banque et en services de paiement (IOBSP) visés à l'article L. 519-1 du CMF, compte tenu de la nature particulière de leurs activités.

Le référentiel ne s'applique pas aux traitements mis en œuvre en vue de la conclusion d'un contrat d'assurance garantissant les risques liés au contrat de crédit.

2. Portée du référentiel

2.1. Champ d'application matériel

Le référentiel a pour objectif de fournir aux responsables du traitement un outil d'aide à la mise en conformité aux dispositions du règlement général sur la protection des données (RGPD) et à celles de la loi du 6 janvier 1978 modifiée (loi « informatique et libertés »). Il peut également guider les acteurs qui n'entrent pas explicitement dans son périmètre mais dont les activités de traitement sont similaires.

Ce référentiel n'ayant pas de valeur contraignante, les responsables du traitement peuvent s'en écarter. Il leur appartient alors de justifier et de documenter les mesures mises en œuvre afin de garantir la conformité des traitements à la réglementation en matière de protection des données à caractère personnel.

2.2. Champ d'application territorial

Le référentiel a vocation à accompagner :

- les responsables du traitement soumis à la compétence de la CNIL ;
- plus généralement tout responsable du traitement exerçant son activité sur le territoire français, ou ciblant ce territoire dès lors que le contrat de crédit le lie à un consommateur sur le territoire français.

3. Objectif poursuivi par le traitement (finalité)

Les traitements mis en œuvre aux fins d'évaluation de la solvabilité incluront la collecte, l'enregistrement et l'utilisation de :

- données à caractère personnel apportées par les demandeurs (documents, informations, etc.) ;
- informations internes et externes relatives aux demandeurs qui ont rencontré des difficultés dans le remboursement de précédents crédits.

Le référentiel n'a pas vocation à s'appliquer :

- au traitement des mentions associées aux personnes qui ont rencontré des difficultés dans le remboursement de précédents crédits à d'autres fins que l'évaluation de la solvabilité (par exemple, en vue du recouvrement des sommes dues ou encore à des fins d'identification des clients visés par l'article L. 312-1-3 du CMF) ;

- aux traitements d'élaboration, d'actualisation et d'estimation de la pertinence des « modèles de score » pris pour référence dans l'évaluation du risque de défaillance de paiement que présentent les demandeurs de crédits.

Point d'information

Les modèles de score développés, actualisés et mis en œuvre par les organismes sont susceptibles de constituer des systèmes d'intelligence artificielle (IA) au sens du règlement (UE) 2024/1689 sur l'intelligence artificielle (RIA).

Les organismes pourront utilement se référer aux recommandations de la CNIL sur l'application du RGPD aux modèles et systèmes d'IA, ainsi qu'aux recommandations de l'autorité de surveillance de marché compétente au titre du RIA.

Les informations recueillies ne peuvent pas être réutilisées pour poursuivre un autre objectif qui serait incompatible avec la finalité initiale. Tout nouvel usage des données doit respecter les principes de protection des données personnelles. Les traitements mis en œuvre ne doivent pas donner lieu à des interconnexions ou échanges autres que ceux nécessaires à l'accomplissement des finalités ci-dessus énoncées.

4. Base légale du traitement

Lorsqu'un traitement poursuit plusieurs finalités, le responsable du traitement doit déterminer la base légale la plus appropriée pour chacune d'elles (art. 6.1 du RGPD).

Il appartient au responsable du traitement de déterminer cette base légale avant toute opération de traitement, après avoir mené une réflexion, qu'il pourra documenter, au regard de sa situation spécifique et du contexte.

Le référentiel propose à titre indicatif la base légale de **l'exécution de mesures précontractuelles prises à la demande de la personne concernée (article 6.1.b du RGPD) s'agissant des traitements mis en œuvre à des fins d'évaluation de la solvabilité** d'une personne concernée.

La consultation des fichiers de la Banque de France

- **Le fichier national des incidents de remboursement des crédits aux particuliers (FICP)**

L'article 2 de l'arrêté du 26 octobre 2010 relatif au FICP impose aux responsables du traitement de consulter le FICP avant toute décision effective d'octroyer un crédit encadré par les dispositions des chapitres II et III du titre I du livre 1 de la partie législative du code de la consommation.

Conformément aux dispositions de l'article L. 751-2 du code de la consommation, ce fichier a vocation à fournir un élément d'appréciation de la solvabilité des personnes qui sollicitent un crédit. L'inscription d'une personne concernée au sein du FICP n'emporte pas interdiction de délivrer un crédit.

Pour être licites, la consultation du FICP et le traitement des informations extraites de ce fichier doivent respecter les règles sectorielles, et notamment les conditions fixées par l'arrêté du 26 octobre 2010.

- **Le Fichier Central des Chèques (FCC)**

Les organismes ont la possibilité de consulter le FCC dans le cadre de l'évaluation de la solvabilité. Cependant, cette consultation ne revêt aucun caractère obligatoire.

5. Données personnelles concernées

La liste des données mentionnées a un caractère facultatif et n'a pas vocation à l'exhaustivité.

Afin de respecter le principe de minimisation (article 5.1.c du RGPD), **le responsable du traitement ne doit collecter et traiter que les données pertinentes et strictement nécessaires** aux fins d'évaluation de la solvabilité.

5.1 Données susceptibles d'être traitées dans le cadre de l'octroi de crédit

Les données suivantes peuvent être traitées :

- **Situation personnelle des demandeurs :** âge, nationalité (sous la forme : « français », « ressortissant d'un autre État de l'Union européenne », « autre nationalité »), capacité juridique, situation maritale (sous la forme « célibataire », « veuf », « marié », « autre vie de couple »), régime matrimonial ou afférent au PACS, nombre d'enfants, situation de logement (sous la forme « propriétaire », « locataire », « hébergé à titre gracieux », « logé par l'employeur », « accédant à la propriété »), ancienneté dans le logement, nature des relations entre les codemandeurs (sous la forme « vie de couple », « relations amicales », « relations familiales », « relations professionnelles »). Les informations peuvent être collectées directement sur des justificatifs de résidence et d'identité fournis par les demandeurs.
- **Sur les autres membres du foyer fiscal des demandeurs de crédit :** situation de la personne dans le foyer (conjoint, personne vivant maritalement, enfant, parent, autre personne à charge), situation maritale (sous la forme « célibataire », « veuf », « marié », « autre vie de couple »), régime matrimonial ou afférent au PACS.
- **Caractéristiques de l'opération de crédit et de l'objet du prêt :** canal d'acquisition du client, type de crédit, primo-accession, vente en l'état futur d'achèvement, montant, durée, taux, bien financé, type de vente, apport personnel, garanties, date de mise à disposition des fonds, assurance, autres prestations, estimation des coûts pour les prêts à la construction et à l'amélioration des biens immobiliers. Les informations peuvent être collectées sur des justificatifs relatifs aux sûretés et garanties dont disposent les demandeurs et qui permettent de réduire le risque de crédit.
- **Situation professionnelle des demandeurs :** catégorie socioprofessionnelle, situation professionnelle (sous la forme « activité », « retraite », « chômage »), ancienneté au poste occupé, durée écoulée depuis l'éventuel début de la période de chômage, secteur d'activité, statut (par exemple : temps plein, temps partiel, entrepreneur, travailleur indépendant). Le responsable du traitement peut, si nécessaire, collecter auprès des personnes concernées un justificatif de l'emploi sous la forme d'une attestation de l'employeur.
- **Situation bancaire, économique et financière des demandeurs :** nature et montant des revenus (y compris, par exemple, primes annuelles, commissions, heures supplémentaires, loyers perçus et revenus locatifs, revenus financiers), des charges (y compris pensions alimentaires), et du patrimoine, dont l'assurance vie, analyse des ratios et bilans financiers, domiciliation bancaire, ancienneté de la relation client, montant du solde des comptes détenus, encours de l'épargne, nature et montant des produits financiers détenus, mouvements financiers sur les trois derniers mois, moyens de paiement et de crédit détenus, fréquence d'utilisation, autres crédits en cours, incidents de paiement, respect des échéances, nombre de produits d'assurance souscrits auprès du groupe, ancienneté de la relation avec le groupe. Les informations peuvent être collectées directement sur des justificatifs adéquats tels que des avis d'impôts, des fiches de paie, des relevés de comptes, courants ou d'épargne, ou des relevés de prêts indiquant les soldes de prêts en cours, ou contrôlées / vérifiées par d'autres biais, notamment pour les indépendants.
- **Sur les garants :** âge, nationalité (sous la forme « français », « ressortissant d'un autre Etat de l'Union européenne », « autre nationalité »), situation maritale (sous la forme « célibataire », « veuf », « marié », « autre vie de couple »), régime matrimonial ou afférent au PACS, nombre d'enfants, situation de logement (sous la forme « propriétaire », « locataire », « hébergé à titre gracieux », « logé par l'employeur », « accédant à la propriété »), catégorie socioprofessionnelle, situation professionnelle, ancienneté dans l'emploi, chômage, nature et montant des revenus et des charges, domiciliation bancaire, incidents de paiement, analyse des ratios et bilans financiers.
- **Sur le résultat de l'application du score :** message relatif à l'acceptation ou au rejet de la demande de crédit par l'outil de score ou à la nécessité de procéder à un examen approfondi, le cas échéant, note.

Lorsque la collecte d'informations intervient directement sur un justificatif ou un autre document produit par les personnes concernées (avis d'imposition ou fiche de paie), le responsable du traitement doit expressément inviter ces dernières, le cas échéant, à occulter les informations qui ne sont pas nécessaires à l'objectif poursuivi. Le responsable du traitement ne doit traiter que les informations nécessaires à la prise de décision et non à l'ensemble des informations accessibles sur le document justificatif, en particulier lorsque les personnes concernées auraient oublié d'occulter certains éléments.

5.2 Cas particulier des données susceptibles d'être traitées dans le cadre de la prise en compte des défaillances contractuelles passées à des fins d'analyse de la solvabilité

Seules des défaillances contractuelles répondant à des conditions objectives, définies préalablement par le responsable du traitement, devraient être prises en compte en vue d'évaluer la solvabilité d'une personne concernée, dans la limite des durées de conservation mentionnées au point 7.2.

Dans ce cadre, les données suivantes peuvent être traitées :

- **Concernant les manquements contractuels supposés :** numéro de contrat, intitulé et date de conclusion de contrat, obligations contractuelles inexécutées (éventuellement, sous la forme de code interne), date de la ou des défaillance(s) de paiement et montant du ou des paiement(s) inexécuté(s).
- **Concernant le contexte :** envoi de courrier en précisant les modalités (courriel, lettre de mise en demeure, assignation en justice), réponses adressées ou actions menées par le client (paiement de la dette, demande de délai de paiement, renégociation du contrat, etc.), état de la procédure en cours (précontentieux, première instance, appel, etc.), résultat des décisions de justice intervenues et des autres étapes procédurales telles que les tentatives de conciliation, en précisant si la décision est favorable au responsable du traitement ou au client.
- **Concernant l'identité de la personne concernée (par exemple, en cas d'inscription d'une mention sur une liste ou un support distinct de son dossier) :** nom de famille, nom marital, prénoms dans l'ordre de l'état civil, date de naissance, lieu de naissance, département, code géographique (INSEE) du lieu de naissance pour les personnes nées en France (métropole, DROM-COM), code pays ISO et la localité de naissance pour les personnes nées à l'étranger et le sexe, ou tout autre élément dont le responsable du traitement pourra démontrer qu'il est nécessaire pour éviter une erreur d'identification due, par exemple, à une homonymie.

Sur le caractère objectif des mentions relatives aux défaillances et la définition d'un seuil de prise en compte des défaillances contractuelles

Afin d'éviter aux personnes de subir indéfiniment les conséquences de situations antérieures et révolues lors de l'évaluation de leur solvabilité, le responsable du traitement doit s'assurer de la pertinence et de l'exactitude des données qu'il traite, ce qui doit le conduire à prendre les mesures raisonnables nécessaires pendant toute la durée du traitement. A cet égard :

- Les mentions doivent correspondre à des descriptions factuelles des inexécutions contractuelles. Par exemple, la CNIL recommande d'exclure les commentaires ou intitulés qui ne permettent pas au gestionnaire du contrat d'apprécier la situation actuelle du demandeur dans son intégralité, tels que « ***client refusable*** » ou « ***non éligible à nos offres*** ».
- Les mentions défavorables doivent être limitées à des incidents pertinents pour l'évaluation. Par conséquent, le responsable du traitement doit définir un seuil adapté à partir duquel il est procédé à l'enregistrement d'informations en lien avec les défaillances contractuelles des personnes concernées (critères factuels tels que la répétition des incidents, leur montant financier, leur montant rapporté à celui du crédit concerné, etc.) ;
- Les informations traitées ne doivent prendre en compte que les inexécutions contractuelles qui conduisent ou ont conduit à placer le client en situation de débiteur à leur égard.

5.3 Cas particulier des catégories particulières de données à caractère personnel

Le responsable du traitement doit veiller à ne pas traiter de catégories particulières de données à caractère personnel. Cela nécessite de ne pas traiter le libellé des transactions à des fins d'évaluation de la solvabilité puisque ces informations sont susceptibles de contenir des catégories particulières de données. A défaut, il devra en justifier la pertinence et la possibilité de se fonder sur une des exemptions prévues à l'article 9 du RGPD.

6. Accédants et destinataires des informations

Les données à caractère personnel doivent uniquement être rendues accessibles aux personnes habilitées à en connaitre au regard de leurs attributions, dans le respect des dispositions relatives au secret professionnel.

Des profils d'habilitation, rôles et privilèges doivent être mis en œuvre et actualisés régulièrement, conformément aux préconisations de la CNIL en matière de sécurité.

Des règles de confidentialité doivent être imposées aux prestataires, qui doivent (i) être sélectionnés sur la base des garanties qu'ils sont en mesure de proposer et (ii) voir leurs modalités d'intervention encadrées par un contrat spécifique et adapté (articles 26 ou 28 du RGPD).

6.1 Personnes accédant aux données pour le compte du responsable du traitement

Les personnels chargés de la définition des modèles de score ou du contrôle interne peuvent accéder aux données nécessaires à l'élaboration et à l'actualisation de ces modèles.

En ce qui concerne le résultat de l'application du score, les personnels suivants peuvent accéder aux informations :

- Les personnels des services chargés de l'octroi de crédit et de la sélection des risques.
- Les commerciaux, gestionnaires et chargés de clientèle ayant recueillis les données, pour les dossiers qui leur sont attribués.

Peuvent accéder aux mentions des défaillances passées :

- Les personnels habilités à en connaître au regard de leurs attributions et des dossiers qui leur sont attribués.
- Les personnels des services chargés des contrôles.

6.2 Destinataires des données

En cas de recours à un apporteur d'affaires, une fois terminée la saisie des données, les personnels habilités de l'apporteur d'affaires ne doivent pouvoir accéder qu'à un message indiquant l'acceptation immédiate ou non de la demande de crédit après application du score.

Il convient par ailleurs de veiller à ce que le message ne soit plus consultable par ces personnels après la communication au demandeur et à l'apporteur d'affaires de la décision définitive de l'établissement de crédit.

Sur le partage d'informations concernant les défaillances passées (en-dehors des fichiers tenus par la Banque de France)

La CNIL rappelle aux responsables du traitement qu'il leur appartient d'être en capacité de démontrer :

- qu'une telle transmission ne remet pas en cause le secret professionnel défini par l'article L. 511-33 du CMF, lequel 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 ces mêmes dispositions ;
- qu'une telle transmission est nécessaire, notamment au regard des informations figurant déjà dans les fichiers tenus par la Banque de France, et proportionnée.

7. Durées de conservation

Les données à caractère personnel ne doivent être conservées sous une forme permettant l'identification des personnes que le temps strictement nécessaire à la réalisation des finalités poursuivies (article 5.1.e du RGPD).

7.1 Durées de conservation relatives aux données recueillies au titre de la demande de crédit

Lorsque le demandeur n'est pas un client, les données à caractère personnel collectées pour l'instruction d'une demande de crédit ne devraient, en cas de rejet de la demande, être conservées qu'au maximum **six mois à compter du dépôt de la demande**. Elles ne peuvent être utilisées qu'aux fins de l'instruction de la demande de crédit, ainsi que d'éventuelles nouvelles demandes de crédit, à l'exclusion de toute autre finalité.

Lorsque le demandeur est client de l'établissement, les données recueillies au titre de la demande de crédit peuvent servir à actualiser les données déjà détenues et être utilisées à d'autres fins lorsque le client concerné en a été préalablement informé, sous réserve du respect de ses droits.

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.

7.2 Durées de conservation relatives aux défaillances contractuelles passées du demandeur déjà client

Les données concernant des défaillances contractuelles passées des personnes déjà clientes :

- ne devraient être traitées dans le cadre de l'instruction de nouvelles demandes de crédit à des fins d'évaluation de la solvabilité que, en l'absence de régularisation, **pendant 5 ans à compter de la date de la défaillance de paiement ;** la CNIL recommande de ne traiter ces données à cette fin que **pendant un délai raisonnable ne dépassant pas six mois à compter de la régularisation intégrale de la défaillance contractuelle** ;
- en cas de procédure judiciaire, doivent immédiatement cesser d'être traitées dans le cadre de l'instruction de nouvelles demandes de crédit, dès réception d'une décision judiciaire définitive ne reconnaissant pas l'existence d'une défaillance contractuelle du demandeur.

8. Recours à la prise de décision individuelle fondée exclusivement sur un traitement automatisé

8.1 Application de l'article 22 du RGPD à l'évaluation de la solvabilité

L'article 22 du RGPD encadre le fait de soumettre une personne à une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

Il s'applique aux traitements mis en œuvre à des fins d'évaluation de la solvabilité du demandeur quand ces traitements intègrent des outils d'évaluation automatisée de la solvabilité du demandeur aboutissant à l'acceptation ou au refus de la demande sans intervention humaine significative (sur ce point, voir l'arrêt du 7 décembre 2023, SCHUFA Holding e.a. (Scoring) (C-634/21, EU:C:2023:957)).

La décision d'octroyer ou de refuser un crédit peut être fondée exclusivement sur un traitement automatisé lorsque celui-ci est **nécessaire pour conclure le contrat de crédit, au vu notamment des obligations précontractuelles imposées par les articles L. 312-16 et L. 313-16 du code de la consommation (article 22.2.b du RGPD)**. Le responsable du traitement doit être en capacité de faire la démonstration de cette nécessité.

8.2 Existence de droits spécifiques à la prise de décision individuelle exclusivement fondée sur un traitement automatisé

Le responsable du traitement met en œuvre des mesures appropriées pour protéger les droits, libertés et intérêts légitimes des personnes concernées, tels que les droits d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer un point de vue et de contester la décision (article 22.3 du RGPD).

Les personnes concernées devraient, en particulier, être informées, dès la réception de leur demande de crédit, qu'elles pourront solliciter un réexamen de leur dossier en cas de rejet de leur demande initiale. Elles devront pouvoir présenter leurs observations sur leur situation financière personnelle. Cet échange pourra prendre la forme d'un entretien. Cet entretien pourra être organisé à distance, le cas échéant, par exemple pour les responsables du traitement qui ne sont pas organisés sous la forme d'un réseau d'agences.

Recours à l'intelligence artificielle

Les outils d'automatisation utilisés par les responsables du traitement, qu'ils entrent dans le périmètre de l'article 22 du RGPD ou non, sont susceptibles de constituer des systèmes d'IA à haut risque au sens du RIA.

Cette qualification serait susceptible de s'assortir de garanties et d'exigences venant compléter celles décrites dans le présent référentiel. L'autorité de surveillance de marché compétente est seule compétente pour interpréter le RIA et l'appliquer aux outils en question.

9. Information et droits des personnes

9.1 Information des personnes

9.1.1. Rappels généraux en matière d'information des personnes

Le responsable du traitement doit s'assurer du respect des principes de transparence et de loyauté à l'égard des personnes dont les données peuvent être traitées dans les conditions prévues par les articles 12, 13 et 14 du RGPD (demandeurs de crédit et garants).

Lorsque l'évaluation de la solvabilité implique le traitement de données qui n'ont pas été collectées auprès de la personne concernée (par exemple, des données collectées par d'autres établissements du groupe auquel ils appartiennent), le responsable du traitement doit généralement informer les personnes concernées du traitement de ces catégories de données (article 14.1.d du RGPD), ainsi que de la source des données (article 14.2.f du RGPD).

En cas d'intervention d'un prestataire dans le processus d'octroi de crédit, celui-ci doit si nécessaire participer à l'élaboration des mentions d'informations destinées à être communiquées aux personnes concernées. La CNIL considère qu'il est de bonne pratique d'associer étroitement les prestataires à la rédaction des mentions d'informations qu'il est envisagé d'utiliser dès lors que ces derniers ont souvent une meilleure connaissance des outils utilisés et sont dans ce cas plus à même d'en expliquer le fonctionnement.

9.1.2. Information des personnes concernant les mentions défavorables

L'utilisation de mentions défavorables liées aux défaillances contractuelles passées des personnes concernées ne devrait pas dépasser les attentes mutuelles des parties, compte tenu des efforts de transparence réalisés afin d'être fondée sur l'exécution de mesures précontractuelles (article 6.1.b du RGPD). A cet égard, la CNIL recommande que les personnes concernées soient informées :

- **au moment de la survenance de l'incident de paiement :** des moyens dont elles disposent pour régulariser leur paiement, de la possibilité de présenter des observations ou, le cas échéant, de demander un réexamen de la situation ;
- **en l'absence de régularisation :** de l'inscription d'une mention défavorable au sein de leur dossier ainsi que des conséquences de cette mention (notamment de leur prise en compte dans le cadre de l'évaluation de leur solvabilité dans l'hypothèse d'une nouvelle demande de crédit) ;

- **préalablement à l'évaluation de la solvabilité justifiée pour chaque nouvelle demande de crédit :** de la consultation de ces mentions passées à des fins d'évaluation de la solvabilité de la personne concernée.

9.2 Droits des personnes concernées

Les personnes concernées bénéficient également des droits suivants, qui s'exercent dans les conditions prévues par le RGPD (articles 15 à 20 du RGPD) :

- **Le droit à la limitation du traitement** (article 18 du RGPD).

Par exemple, lorsqu'une personne concernée conteste l'exactitude de ses données, elle peut demander à l'organisme le gel temporaire du traitement de ses données, le temps que celui-ci procède aux vérifications nécessaires.

- **Le droit à la portabilité** (article 20 du RGPD).

Ne sont concernées que les données fournies par la personne sur la base de l'exécution des mesures précontractuelles. Les personnes doivent être informés des traitements concernés par ce droit.

- **Le droit d'accès, de rectification** et, dans des conditions particulières, **d'effacement des données** qui les concernent (articles 15 à 17 du RGPD).

Dans le cadre de l'exercice du droit d'accès :

- les personnes concernées doivent être informées du score qu'elles ont obtenu ainsi que des notes minimales et maximales pour obtenir le crédit, afin qu'elles puissent comprendre où elles se situent vis-à-vis des exigences du responsable du traitement ;
- les différentes informations fournies aux personnes concernées au titre de l'article 15.1.a à h ne peuvent pas consister en un simple rappel de celles qui ont été communiquées en amont de la collecte et du traitement des données à caractère personnel, en application des articles 13 et 14 du RGPD et préalablement à la prise de décision.

Le droit d'accès s'applique aux informations contenues dans les zones de commentaires libres.

L'articulation entre le droit d'accès et le droit des tiers

Le droit d'accès ne doit pas porter atteinte aux droits des tiers, au nombre desquels figurent les droits du responsable du traitement lui-même (par exemple, le droit au secret des affaires).

En cas de doute, le responsable du traitement ne doit pas opposer un refus global à la personne concernée et doit, dans la mesure du possible, répondre à la demande reçue en fournissant tout élément susceptible de satisfaire la demande et, le cas échéant, en transmettant les éléments susceptibles de porter atteinte aux droits des tiers identifiés à la CNIL ou à la juridiction compétente, afin que celles-ci se prononcent sur l'étendue du droit d'accès des personnes.

Voir en ce sens, CJUE, n° C-203/22, Arrêt de la Cour, CK contre Dun & Bradstreet Austria GmbH et Magistrat der Stadt Wien, 27 février 2025.

9.3 Informations complémentaires à fournir en cas de refus de la demande de crédit

Les personnes concernées doivent, conformément aux textes applicables, être informées lorsque le refus opposé à leur demande de crédit résulte de la consultation du FICP ou du FCC (article L. 313-6 du code de la consommation et article 19.6 de la directive (UE) 2023/2225 relative aux contrats de crédits aux consommateurs, en cours de transposition).

Dans les situations dans lesquelles une telle information n'est pas imposée par la règlementation sectorielle, la CNIL l'encourage à titre de bonne pratique.

La CNIL recommande également, à titre de bonne pratique, que les personnes concernées soient informées lorsque le refus de leur demande de crédit est fondé sur la consultation d'un fichier interne, tel qu'un fichier recensant des évènements concernant des impayés.

9.4 Informations à fournir en cas de prise de décision fondée exclusivement sur un traitement automatisé, au sens de l'article 22 du RGPD[1]

Le responsable du traitement doit informer les personnes concernées de l'existence d'une prise de décision entièrement automatisée, au sens de l'article 22 du RGPD y compris un profilage et, au moins en pareil cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée (articles 13.2.f, 14.2.g et 15.1.h du RGPD).

S'agissant des informations utiles concernant la logique sous-jacente, les personnes concernées doivent recevoir toute information pertinente concernant notamment la procédure et les principes concrètement appliqués pour exploiter, par voie automatisée, leurs données à caractère personnel aux fins d'obtenir le résultat déterminé.

Au titre, plus spécifiquement, du droit d'accès, informer les personnes concernées de la mesure dans laquelle une variation des données à caractère personnel prises en compte aurait conduit à un résultat différent peut constituer une information suffisamment transparente et intelligible.

Par exemple, le responsable du traitement pourrait mettre à disposition des personnes concernées un outil de calcul leur permettant de renseigner elles-mêmes leurs données à caractère personnel (revenus, charges, etc.), de les modifier et de voir l'effet de cette modification sur le résultat de leur demande de crédit.

Par ailleurs, **les informations relatives à l'importance et aux conséquences prévues de ce traitement pour la personne concernée** doivent être complétées d'exemples réels et tangibles pour être utiles et compréhensibles.

Le responsable du traitement doit fournir aux personnes concernées :

- ces informations avant toute mise en œuvre des traitements (articles 13.2.f, 14.2.g du RGPD) ;
- de nouvelles informations, plus précises et adaptées à la situation particulière d'une personne, lorsque cette dernière exerce son droit d'accès (article 15.1.h du RGPD).

En effet, le « droit à l'explication » que constitue le droit d'accès doit permettre aux personnes concernées :

- de comprendre la situation dans laquelle elles se trouvent individuellement ;
- d'exercer les autres droits garantis par le RGPD.

Ces informations doivent être fournies de manière concise, transparente, compréhensible et aisément accessible. Une formule mathématique complexe, telle qu'un algorithme, ou une description détaillée de toutes les étapes d'une prise de décision entièrement automatisée ne suffisent donc pas dans la mesure où aucune de ces modalités ne constituerait une explication suffisamment concise et compréhensible.

10. Analyse d'impact sur la protection des données (AIPD)

Le responsable du traitement doit réaliser une analyse d'impact lorsque les traitements qu'il met en œuvre sont susceptibles de présenter un risque élevé pour les droits et les libertés des personnes concernées (article 35 du RGPD).

Les traitements impliquant le profilage des personnes et pouvant aboutir à leur exclusion du bénéfice d'un contrat ou à la suspension voire à la rupture de celui-ci figurent dans la liste des types d'opérations de traitement pour lesquelles une AIPD est requise. **Ces traitements incluent notamment ceux qui établissent un score pour l'octroi de crédit.**

Le responsable du traitement documentera dans l'AIPD ou en annexe de celle-ci les mesures mises en œuvre pour réduire les risques propres aux outils automatisés utilisés pour les droits et libertés des personnes concernées, notamment les risques liés à d'éventuels biais discriminatoires de ces outils.

[1] Sur l'interprétation de l'article 15.1.h du RGPD, voir CJUE, 27 février 2025, CK contre Magistrat der Stadt Wien en présence de Dun & Bradstreet Austria GmbH, C-203/22. Disponible ici :

https://curia.europa.eu/juris/document/document.jsf?text=&docid=295841&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=15430049.

Lorsque le responsable du traitement utilise ces outils comme aides à la prise de décision pour évaluer la solvabilité, sans prise de décision fondée exclusivement sur un traitement automatisé au sens de l'article 22 du RGPD, la Commission recommande de **documenter, dans l'AIPD ou en annexe, le caractère significatif de l'intervention humaine assurée dans l'octroi ou le refus de chaque demande de crédit**. L'analyse peut notamment prendre en compte les axes suivants :

L'évaluation de l'intelligibilité de l'outil d'automatisation utilisé

- Les sorties (résultats de l'outil) sont-elles opérationnelles, c'est-à-dire fournies dans un format clair et manipulable ?

Les sorties peuvent par exemple s'accompagner d'une explication sous forme de graphique ou de texte.

- L'outil est-il accompagné d'une documentation contenant des informations sur son fonctionnement permettant d'interpréter ses réponses ?

Cette documentation pourra préciser, en plus de la performance de l'outil, ses marges d'erreur et les types de cas sur lesquels il est en difficulté. Si le responsable du traitement a développé lui-même l'outil, il peut avoir produit cette documentation. Si le développement a été externalisé, elle peut avoir été fournie par le développeur.

- Si l'outil utilise des données sur la personne concernée pour fournir une sortie, cette sortie s'accompagne-t-elle de données permettant à l'agent humain de contrebalancer ou d'évaluer la sortie ?

L'évaluation de la gouvernance de la procédure de prise de décision

- Le responsable du traitement met-il en œuvre une procédure de gestion du risque et un contrôle qualité de l'intervention humaine afin d'identifier et de corriger (par exemple par de la formation) les biais éventuels de l'agent humain ou le caractère superficiel de son intervention face à la décision proposée par l'outil d'analyse ?

Ce contrôle pourra par exemple inclure un contrôle des sorties de l'outil sur la base de demandes fictives, une analyse des réclamations clients ou un contrôle statistique des cas où les agents humains vont à l'encontre de l'évaluation par l'outil.

- Le responsable du traitement s'est-il doté de procédures claires sur l'exécution de l'intervention humaine dans la prise de décision ? Ces procédures clarifient-elles les rôles respectifs de l'outil et de l'agent humain, les éléments que peut prendre en compte ce dernier pour faire fi de l'évaluation par l'outil et les modalités dont il dispose pour demander des éléments complémentaires ou adapter la décision à des situations particulières ?

L'évaluation des éléments relatifs à l'agent humain

- L'agent a-t-il le pouvoir, l'indépendance et la liberté de ne pas suivre le résultat de l'évaluation par l'outil ? En particulier, l'agent est-il susceptible d'être dissuadé d'exercer un contrôle effectif par sa hiérarchie, par la procédure à suivre, par une interface mal-adaptée ou par la menace d'éventuelles conséquences négatives pour lui ?
- L'agent a-t-il la compétence et les moyens de former sa propre opinion indépendamment de l'évaluation par l'outil ? En particulier a-t-il accès ou peut-il se procurer en temps utile toutes les données pertinentes, y compris au moins les données utilisées par l'outil pour mener son évaluation et a-t-il le temps d'examiner effectivement ses dossiers ?
- L'agent est-il formé au fonctionnement de l'outil d'évaluation comme un simple outil d'aide à la décision, c'est-à-dire :
  - En comprend-il le fonctionnement et les limites ?
  - Comprend-il les biais d'acceptation et d'aversion qui peuvent guider son utilisation de l'outil ?
  - Sait-il sous quelles conditions il peut s'écarter du résultat de l'évaluation par l'outil et est-il capable de mener l'analyse sans le secours de l'outil ?
  - Bénéficie-t-il d'actions de sensibilisation régulières ?

L'évaluation des évolutions du contrôle humain dans le temps

- Le responsable du traitement recense-t-il les situations dans lesquelles la décision finale a suivi le résultat proposé par le système utilisé, ou s'en est écartée ? Une agrégation statistique de ces éléments confirme-t-elle la réalité de l'intervention humaine et le niveau de suivi et de contrôle appliqués à l'outil ?

Si le responsable du traitement estime que la décision est prise de manière entièrement automatisée, au sens de l'article 22 du RGPD, il leur est recommandé de **documenter dans l'AIPD ou, en annexe à celle-ci, la nécessité objective d'une telle automatisation**. Il devra notamment expliquer en quoi une intervention humaine significative et systématique ne peut raisonnablement être mise en œuvre dans le processus décisionnel.

11. Sécurité

Le responsable du traitement et ses éventuels sous-traitants doivent s'assurer que les mesures techniques et organisationnelles appropriées sont mises en œuvre afin de garantir un niveau de sécurité adapté aux risques spécifiques des traitements concernés (article 32 du RGPD).

L'analyse de ces risques ainsi que les mesures mises en œuvre et envisagées pour faire face à ces risques, y compris par les éventuels sous-traitants, doivent être documentées au sein de l'AIPD.

Afin de garantir un niveau élevé de confidentialité et d'intégrité pour les données à caractère personnel concernées, des canaux et de supports chiffrés, respectivement pour le transport et la conservation des données collectées devraient systématiquement être utilisés. La CNIL recommande que les méthodes de chiffrement utilisées ainsi que l'authentification des personnes accédant aux données respectent les règles définies dans le référentiel général de sécurité de l'ANSSI.

De plus, afin de limiter l'impact d'une violation de données sur les personnes concernées, notamment les risques de fraude documentaire ou d'usurpation d'identité, le responsable du traitement peut notamment sécuriser les documents collectés par des filigranes numériques.

Enfin, la CNIL rappelle que toute violation de données engendrant un risque pour les personnes concernées doit faire l'objet d'une notification à la CNIL dans un délai maximal de 72 heures (article 33 du RGPD). En cas de risque élevé, une notification des personnes concernées doit également être réalisée (article 34 du RGPD).