

# Commission nationale de l'informatique et des libertés

**Délibération n° 2008-198 du 9 juillet 2008 modifiant l'autorisation unique n° AU-005 relative à certains traitements de données à caractère personnel mis en œuvre par les établissements de crédit pour aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit**

NOR : CNIA0800007X

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 par la loi n° 2004-801 du 6 août 2004, relative à l'informatique, aux fichiers et aux libertés, notamment le 4° du I et le II de l'article 25 ;

Vu le code monétaire et financier, notamment ses articles L. 311-1, L. 313-1 et L. 511-1 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978, modifiée par la loi n° 2004-810 du 6 août 2004 ;

Sur le rapport de M. Philippe Nogrix, commissaire, en son rapport, et Mme Catherine Pozzo di Borgo, commissaire du Gouvernement adjoint, en ses observations ;

Formule les observations suivantes :

Les établissements de crédit recourent fréquemment, en matière d'octroi de crédit, à des traitements automatisés d'aide à la décision qui s'appuient sur des modèles de score.

L'objectif de ces modèles est d'identifier les caractéristiques personnelles des clients qui paraissent différencier le mieux la population des emprunteurs défaillants de ceux qui ne font pas défaut. Les établissements de crédit les construisent sur la base de techniques statistiques, à partir des données relatives aux contrats de crédit qu'ils ont précédemment conclus, des caractéristiques personnelles des emprunteurs et des défauts de remboursement constatés.

Ces traitements automatisés de données à caractère personnel ont pour objet, d'une part, d'évaluer, pour chaque personne qui présente une demande de crédit ou souhaite disposer d'un moyen de paiement adossé à un contrat de crédit, le risque statistique de défaillance qui lui est attaché et, d'autre part, de sélectionner les demandes qui correspondent à un niveau de risque de défaillance jugé satisfaisant. Ils sont, par voie de conséquence, susceptibles d'exclure, au moins de façon temporaire, une personne du bénéfice d'un contrat de crédit là où aucun texte législatif ou réglementaire ne prévoit une telle exclusion.

Dès lors, ces traitements automatisés relèvent du 4° du I de l'article 25 de la loi du 6 janvier 1978 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, la commission peut autoriser par une décision unique une catégorie de traitements qui répondent aux mêmes finalités, portent sur des catégories de données identiques et ont les mêmes catégories de destinataires. Il en résulte que le responsable d'un traitement conforme à cette décision unique d'autorisation pourra déclarer son traitement en adressant à la commission un engagement de conformité par lequel il s'engage à respecter les termes de la décision de la CNIL.

La délibération n° 2006-019 du 2 février 2006 portant autorisation unique de certains traitements mis en œuvre par les établissements de crédit pour aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit (décision d'autorisation unique n° AU-009) doit être modifiée pour en étendre le domaine d'application, en favoriser l'utilisation par les établissements de crédit et préciser les obligations à la charge des responsables de traitement.

Décide de remplacer les articles 1<sup>er</sup> à 9 de la délibération précitée par le tableau mis en annexe.

Décide que les établissements de crédit qui souhaitent se référer à l'autorisation unique n° AU-005 adressent, à cette fin, à la CNIL un engagement de conformité pour ceux de leurs traitements automatisés qui répondent aux conditions définies dans le tableau susmentionné seront autorisés à les mettre en œuvre.

Décide que tout projet de traitement automatisé dont les finalités ou les catégories de données ou de destinataires excéderaient le cadre défini par la présente autorisation unique ou qui ne respecterait pas les exigences qui y sont définies devra faire l'objet d'une demande d'autorisation spécifique présentant et expliquant les différences entre le traitement envisagé et l'autorisation unique.

La présente délibération sera publiée au *Journal officiel* de la République française.

Le président,  
A. TÜRK

## A N N E X E

## CHAMP D'APPLICATION DE L'AUTORISATION UNIQUE ET CONDITIONS AUXQUELLES DOIVENT RÉPONDRE LES TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL POUR BÉNÉFICIER DE L'AUTORISATION UNIQUE

SECTEUR CONCERNÉ	BANQUE - FINANCE - CRÉDIT
Responsable du traitement.	Tout établissement de crédit.
Finalités des traitements.	<p>Seuls peuvent faire l'objet d'un engagement de conformité à la présente autorisation unique les traitements automatisés relatifs à l'élaboration, à l'actualisation et à l'utilisation de modèles de score pour l'attribution de prêts personnels, de crédits à la consommation, de crédits immobiliers ou professionnels, lorsque ceux-ci visent à :</p> <ul style="list-style-type: none"> <li>- mesurer le risque statistique de défaut de remboursement qui correspond aux demandes de crédit (ou de moyen de paiement adossé à un contrat de crédit) présentées par des clients personnes physiques ;</li> <li>- apporter une aide à la sélection des demandes dont le niveau de risque, ainsi évalué, permet la conclusion d'un contrat de crédit, sous la seule réserve de la production de pièces justificatives.</li> </ul> <p>Ces traitements ne peuvent avoir que les finalités suivantes :</p> <ul style="list-style-type: none"> <li>- la constitution des modèles de score à partir de l'analyse statistique de données, rendues indirectement nominatives, relatives à la situation personnelle, familiale, économique et financière des clients de l'établissement de crédit, éventuellement à l'historique du fonctionnement de leurs comptes bancaires, ainsi qu'aux modalités de remboursement des crédits octroyés (définition des populations homogènes d'emprunteurs correspondant à des modèles spécifiques de score, des variables à retenir et des pondérations qui leur sont attachées) ;</li> <li>- la vérification de la pertinence des modèles de score mis en œuvre et leur actualisation, en utilisant les mêmes catégories de données ;</li> <li>- l'évaluation du risque de défaut de remboursement qui est attaché à chaque demande de crédit en vue d'apporter une aide à l'instruction de la demande.</li> </ul> <p>Conformément à l'article 10 de la loi du 6 janvier 1978, le résultat du score ne peut, en toute hypothèse, avoir qu'un caractère indicatif lorsqu'il ne conclut pas à l'attribution du crédit sous la seule réserve de la production de pièces justificatives.</p> <p>Les traitements d'aide à la décision ne peuvent être mis en œuvre par les établissements de crédit que selon l'une des modalités suivantes :</p> <ul style="list-style-type: none"> <li>- dans leurs agences commerciales ou autres services chargés de l'instruction des demandes de crédit ;</li> <li>- directement à partir de leur site internet ou d'un site internet marchand, sur l'initiative du client ;</li> <li>- dans les locaux d'un apporteur d'affaires ;</li> <li>- par voie de démarchage à domicile.</li> </ul>
Données susceptibles d'être traitées.	<p>a) Sur la situation personnelle des demandeurs de crédit (les futurs signataires du contrat de crédit) : âge, nationalité (sous la forme : français, ressortissant d'un autre Etat 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, département de résidence, type d'habitation, situation de logement (sous la forme : propriétaire, locataire, hébergé à titre gracieux, logé par l'employeur, accédant à la propriété), ancienneté dans le logement, catégorie socioprofessionnelle, situation professionnelle, ancienneté dans l'emploi, chômage, types de téléphone, existence d'une adresse électronique, nature des relations entre les codemandeurs (sous la forme : vie de couple, relations amicales, relations familiales, relations professionnelles).</p> <p>b) Sur la situation économique et financière des demandeurs de crédit : nature et montant des revenus, des charges et du patrimoine ; analyse des ratios et bilans financiers.</p> <p>c) Sur la situation bancaire des demandeurs de crédit : domiciliation bancaire, ancienneté bancaire, type de banque, montant du solde des comptes et des flux financiers, encours de l'épargne, nature et montant des produits financiers détenus, mouvements financiers, moyens de paiement et de crédit détenus, fréquence d'utilisation, autres crédits en cours, incidents de paiement, respect des échéances. Ces données peuvent être prises en compte tant qu'elles n'ont pas été archivées par l'établissement de crédit, dans le respect des durées de conservation déclarées à la CNIL.</p> <p>d) Sur les autres membres du (des) foyer(s) des demandeurs de crédit et les personnes qui leur sont économiquement liées : âge, catégorie socioprofessionnelle, situation de la personne dans le foyer (conjoint, personne vivant maritalement, enfant, parent, autre personne à charge), nature et montant des revenus et des charges.</p> <p>e) 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.</p> <p>f) Sur les caractéristiques de l'opération de crédit : 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.</p> <p>Les données visées aux paragraphes a) à f) peuvent être utilisées par le système de score. Elles peuvent avoir été spécialement transmises par les demandeurs de crédit lors de la constitution du dossier de crédit ou provenir des fichiers internes de l'établissement de crédit, à condition qu'elles aient été communiquées par la personne concernée ou qu'elles se rapportent à des contrats en vigueur conclus avec l'établissement prêteur (ouverture et fonctionnement d'un compte bancaire, demandes de crédit en cours et état de leur remboursement...).</p> <p>g) 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.</p>

SECTEUR CONCERNÉ	BANQUE - FINANCE - CRÉDIT
	<p>h) Pour les demandes de crédit transmises en ligne, un cookie ne comportant aucune autre donnée personnelle qu'un identifiant non signifiant peut être utilisé par l'organisme de crédit pour faciliter la navigation sur le site.</p>
Modalités de conservation et de réutilisation des données.	<p>Le résultat de l'application du score aux données se rapportant à une demande de crédit ne peut pas être utilisé sous forme nominative, notamment dans le cadre de l'instruction d'autres demandes.</p> <p>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 et des règles relatives aux formalités préalables.</p> <p>L'information des autres membres des foyers des demandeurs de crédit et des personnes qui leur sont économiquement liées est à la charge du responsable du traitement lorsqu'il envisage d'utiliser les données à d'autres fins que la mise en œuvre du système de score, conformément au III de l'article 32 de la loi du 6 janvier 1978.</p> <p>En cas de rejet de la demande de crédit, les informations spécialement collectées pour son instruction sont conservées sous forme nominative au maximum pendant une durée de six mois à compter du dépôt de la demande, lorsque le demandeur n'est pas par ailleurs client de l'établissement de crédit. Elles ne peuvent être utilisées qu'aux fins de l'instruction de nouvelles demandes de crédit.</p> <p>Pour les demandes de crédit transmises en ligne, les cookies installés sur l'ordinateur du client ne sont pas conservés après que le demandeur a pris connaissance de la décision définitive de l'établissement de crédit.</p> <p>Les données prises en compte lors de l'application du score à une demande de crédit peuvent également être conservées sous une forme indirectement nominative dans des bases de données dont la finalité, statistique, est d'établir les modèles de score et de vérifier et maintenir leur qualité.</p> <p>Lorsque ces bases regroupent des données provenant de plusieurs applications commerciales de gestion des opérations de crédit, notamment de plusieurs établissements de crédit, ou lorsqu'elles conservent ces données pendant une durée plus longue que dans leurs applications d'origine, les éléments d'identification des demandeurs de crédit sont remplacés par des éléments non signifiants et propres à ces bases.</p> <p>Le lien entre les éléments d'identification d'un demandeur de crédit et les éléments non signifiants correspondants est confidentiel. La confidentialité de ce lien est directement assurée par un mécanisme cryptographique à clés secrètes. Les clés secrètes sont gérées selon les usages établis dans le domaine de la cryptographie bancaire en appliquant le principe du double contrôle qui assure qu'une personne ou un service ne peut pas, seul, autoriser l'identification ponctuelle des personnes concernées par les données enregistrées.</p>
Destinataires des données.	<p>Seuls peuvent être habilités à avoir communication des données précitées, sous réserve qu'elles soient nécessaires pour l'exercice de leurs compétences :</p> <p>a) Pour l'ensemble des données nécessaires à l'élaboration et à l'actualisation des modèles de score : les personnels de l'établissement de crédit ou, en cas d'appartenance à un groupe, de l'entité du groupe qui sont chargés :</p> <ul style="list-style-type: none"> <li>- de la définition de ces modèles ;</li> <li>- du contrôle interne.</li> </ul> <p>b) Pour le seul résultat de l'application du score :</p> <ul style="list-style-type: none"> <li>- les personnels des services chargés de l'octroi de crédit et de la sélection des risques ;</li> <li>- les commerciaux et chargés de clientèle ayant recueilli les données ;</li> <li>- les personnels habilités de l'apporteur d'affaires qui, une fois terminée la saisie des données demandées par le traitement, ne peuvent accéder qu'à un message indiquant l'acceptation immédiate ou non de la demande de crédit après application du score.</li> </ul> <p>Ce message ne doit plus être consultable par les personnels de l'apporteur d'affaires après la communication au demandeur et à l'apporteur de la décision définitive de l'établissement de crédit. Il ne doit être conservé sur aucun support.</p>
Transferts de données hors de l'Union européenne.	<p>Lorsque des données sont transmises vers un Etat qui n'assure pas un niveau de protection suffisant ou reconnu comme tel par une décision de la Commission européenne, le transfert ne peut être effectué que sous réserve du respect par le responsable du traitement des dispositions des articles 68 et 69 de la loi du 6 janvier 1978.</p> <p>Tout contrat conclu avec les personnes habilitées à avoir communication des données devra respecter les décisions de la Commission européenne relatives aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers ou des sous-traitants établis dans des pays tiers en vertu de la directive du 24 octobre 1995 susvisée.</p>
Information et droits des personnes.	<p>L'article 10 de la loi du 6 janvier 1978 dispose que :</p> <ul style="list-style-type: none"> <li>- « aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé » ;</li> <li>- les décisions relatives notamment à la conclusion d'un contrat ne sont pas regardées comme prises sur le seul fondement d'un traitement automatisé, si, et seulement si, les personnes concernées ont été mises en mesure de présenter leurs observations. Ce dispositif ne concerne pas les décisions ayant satisfait les demandes des personnes concernées.</li> </ul> <p>Le respect de ces obligations légales est garanti, en cas d'utilisation d'un système de score, par la mise en place des règles suivantes dès lors que la demande de crédit a fait l'objet d'un refus : les demandeurs ont le droit de solliciter un entretien avec un agent habilité à procéder à un réexamen de leur dossier, au cours duquel ils pourront présenter leurs observations sur leur situation financière personnelle. Ils sont informés de ce droit dès le dépôt de leur demande.</p> <p>En l'absence de guichet situé à proximité du demandeur, l'entretien peut s'effectuer à distance et être complété par un échange de courriers ou courriels.</p> <p>Il en va notamment ainsi lorsque le résultat de l'application du score n'est pas directement opposé aux demandeurs ou lorsque le traitement automatisé n'est pas mis en œuvre en leur présence.</p>

SECTEUR CONCERNÉ	BANQUE - FINANCE - CRÉDIT
	<p>Les demandeurs de crédit et leurs garants qui transmettent des informations pour l'instruction d'un dossier sont informés, par écrit, des finalités des traitements dont ces informations peuvent faire l'objet, notamment du traitement d'aide à la décision en matière d'octroi de crédit, du caractère obligatoire ou facultatif des données collectées, de leur transmission à un traitement statistique aux fins de constitution des modèles de score, ainsi que des différents droits qui leur sont reconnus par ladite loi.</p> <p>Ils sont également informés, s'il y a lieu, des grandes catégories de données, déjà connues de l'établissement de crédit, qui peuvent être utilisées pour le traitement de la demande de crédit.</p>
Mesures de sécurité.	<p>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.</p> <p>Les accès individuels au traitement s'effectuent par un identifiant et un mot de passe individuels, régulièrement renouvelés, ou par tout autre moyen d'authentification.</p> <p>Les demandes de crédit en ligne donnent lieu à la création par l'établissement de crédit d'un compte informatique, individuel et provisoire, dont l'accès est sécurisé grâce à l'attribution au client d'un code d'accès et d'un mot de passe personnel ou de toute mesure offrant un niveau de sécurité supérieur.</p> <p>Les mesures prises pour sécuriser l'accès aux données sont indiquées sur le premier écran de saisie.</p> <p>Ce compte informatique, individuel et provisoire, est clôturé lors du rejet définitif de la demande de crédit ou de l'ouverture d'un compte client informatique définitif. Aucun document ne pourra être communiqué via le compte provisoire informatique.</p> <p>Les demandes de crédit en ligne sont sécurisées dès l'affichage du premier écran de saisie (exemple : en https).</p>
Recours à des prestataires externes.	<p>La réalisation des opérations visées par la présente autorisation unique peut être confiée par le responsable du traitement, sous sa seule responsabilité, à un tiers prestataire de services.</p> <p>Les établissements liés contractuellement au responsable du traitement pour l'exécution de tâches qui se rapportent à l'octroi de crédit, notamment à la collecte des données, ou à la sélection des risques doivent présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité des données qu'ils traitent pour son compte.</p> <p>La convention signée par le responsable avec chaque intervenant externe qu'il a choisi décrit :</p> <ul style="list-style-type: none"> <li>- les opérations que celui-ci a pour mission d'exécuter à partir des données à caractère personnel qui lui auront été communiquées à cette fin ;</li> <li>- les engagements qu'il prend pour garantir le respect du secret bancaire, la sécurité et la confidentialité des données communiquées, en particulier l'interdiction d'utiliser les données à d'autres fins que celles indiquées par la convention et de les mettre en relation avec d'autres sources de données à caractère personnel et l'engagement de procéder à la destruction des fichiers manuels ou informatisés stockant les données personnelles dès l'achèvement du contrat.</li> </ul> <p>Le responsable de traitement doit s'assurer du caractère suffisant des mesures prises en vue d'assurer la sécurité et la confidentialité des données.</p>
Autres conditions à remplir.	<p>Les techniques statistiques utilisées pour l'élaboration et l'actualisation des modèles de score doivent régulièrement faire l'objet de tests de fiabilité et de pertinence.</p> <p>Les données prises en compte pour le calcul du score sont choisies et pondérées en fonction du lien de corrélation qu'elles présentent avec le risque attaché à l'opération.</p> <p>Aucune variable ne doit recevoir une pondération telle qu'elle puisse à elle seule avoir un effet d'exclusion absolue ou disqualifiant. Il en va de même pour tout ensemble de variables étroitement corrélées les unes aux autres.</p> <p>L'utilisation et la présentation du résultat de l'application du score aux demandes de crédit sont encadrées par des procédures écrites détaillées, destinées au personnel du réseau commercial, ainsi que par des clauses contractuelles avec les apporteurs d'affaires, sous la responsabilité exclusive du mandant vis-à-vis du consommateur concerné.</p>