RÉFÉRENTIEL

RELATIF AUX TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL MIS EN ŒUVRE AUX FINS DE GESTION DES IMPAYÉS DANS UNE TRANSACTION COMMERCIALE

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. À qui s'adresse ce référentiel ?

Ce référentiel propose des solutions de mise en conformité pour la mise en œuvre par les organismes de droit privé ou public d'un traitement de données de gestion d'impayés avérés, c'est-à-dire les cas dans lesquels la personne dont les données sont traitées est incontestablement débitrice d'une somme d'argent. Il porte plus précisément sur des impayés faisant suite à une transaction commerciale portant sur des biens ou des services.

Il ne s'applique pas aux traitements mis en œuvre pour détecter un risque d'impayé ou recenser des manquements autres que pécuniaires (comme, par exemple, des incivilités des clients).

Compte tenu de la nature particulière de leurs activités, ce référentiel ne s'applique pas aux traitements mis en œuvre par :

- les organismes de gestion et de recouvrement de créances ;
- les organismes d'enquête civile ;
- les établissements bancaires ou assimilés ;
- les entreprises d'assurance.

2. Portée du référentiel

Les traitements mis en œuvre aux fins de gestion des impayés, qu'ils soient mis en œuvre à partir d'outils internes ou externalisés auprès d'un prestataire de service, conduisent à collecter des données relatives à des personnes physiques clientes de l'organisme. À ce titre, ils sont soumis aux dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après « RGPD ») et de la loi du 6 janvier 1978 modifiée.

Les organismes concernés, en tant que responsables de traitement, doivent mettre en place toutes les mesures techniques et organisationnelles appropriées afin de garantir un haut niveau de protection des données à caractère personnel dès la conception des traitements et tout au long de la vie de ceux-ci. Ils doivent, en outre, être en mesure de démontrer cette conformité à tout instant. Ces traitements doivent faire l'objet d'une inscription au registre des traitements, conformément aux dispositions de l'article 30 du RGPD (voir les modèles de registre sur le site cnil.fr).

Le référentiel n'aborde pas les règles de droit autres que celles relatives à la protection des données à caractère personnel. Il appartient aux acteurs concernés de s'assurer qu'ils respectent les autres réglementations qui peuvent par ailleurs trouver à s'appliquer.

L'application de ce référentiel, qui n'a pas de caractère contraignant, permet d'assurer la conformité des traitements de gestion des impayés au regard des principes relatifs à la protection des données. Les organismes peuvent choisir de s'écarter du référentiel au regard des conditions particulières tenant à leur situation, en s'assurant de prendre toutes les mesures appropriées à même de garantir la conformité des traitements à la réglementation en matière de protection des données à caractère personnel.

Les organismes doivent, conformément au RGPD, évaluer si leur traitement est susceptible d'entraîner un risque élevé tel qu'interprété par le Comité européen de la protection des données dans ses « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est susceptible d'engendrer un risque élevé », afin de déterminer s'ils doivent effectuer une analyse d'impact ou non.

Ce référentiel sera régulièrement mis à jour par la CNIL afin de garantir sa compatibilité avec les dernières évolutions législatives et technologiques.

3. Objectif(s) poursuivi(s) par le traitement (finalités)

Le référentiel fournit un cadre pour les traitements dont les finalités sont les suivantes :

a) **le recensement des impayés avérés ;**
b) **l'identification des personnes en situation d'impayé aux fins d'exclusion pour toute transaction à venir.**

Les informations recueillies pour une de ces finalités ne peuvent pas être réutilisées pour poursuivre un autre objectif qui serait incompatible avec la finalité définie lors de leur collecte. Par ailleurs, les traitements mis en œuvre dans le cadre de ce référentiel ne doivent pas donner lieu à des interconnexions ou échanges autres que ceux nécessaires à l'accomplissement des finalités énoncées ci-dessus.

Ce référentiel n'a pas vocation à encadrer les traitements répondant aux finalités suivantes :

- la prévention d'un impayé incluant une évaluation (« *scoring* ») visant à déterminer si une personne est susceptible d'être en situation d'impayé ;
- l'enrichissement du traitement à partir d'informations collectées par ou auprès de tiers ;
- le partage ponctuel et/ou la mutualisation des données relatives à l'identité des personnes en situation d'impayé avec des tiers et/ou avec d'autres créanciers, hors sous-traitants.

4. Base(s) légale(s) du traitement

Chaque finalité du traitement visée par le référentiel doit reposer sur l'une des bases légales fixées par le RGPD.

Les différents fondements susceptibles d'être mobilisés pour traiter des données à caractère personnel à des fins de gestion des impayés dans le cadre du présent référentiel sont listés ci-dessous :

a) **l'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures pré-contractuelles prises à sa demande.** Conformément au RGPD, les données collectées doivent être nécessaires à l'exécution des mesures contractuelles et/ou pré-contractuelles. À cet égard, le CEPD indique que le fait que le contrat conclu entre la personne concernée et le responsable du traitement mentionne la collecte de données spécifiques ne suffit pas en principe à démontrer que ces données sont nécessaires à l'exécution du contrat. Ainsi, pour reposer sur cette base légale, la collecte des données doit être indispensable pour fournir le service ou le bien attendu par la personne concernée ;
b) **la réalisation de l'intérêt légitime poursuivi par l'organisme ou par le tiers, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.**

Si l'intérêt légitime du responsable du traitement ne peut être exclu pour justifier du traitement de gestion des impayés, le recours à la base légale de l'exécution du contrat semble toutefois plus approprié.

Par ailleurs, dans le cas où l'exclusion serait décidée de manière entièrement automatisée, le traitement doit, en application de l'article 22 alinéa 2.a du RGPD, se fonder sur l'exécution du contrat pour être conforme au référentiel.

Comme prévu par le RGPD, les bases légales doivent être portées à la connaissance des personnes dont les données sont traitées puisqu'elles permettent, notamment, de déterminer leurs droits.

5. Données à caractère personnel concernées

Dans un souci de minimisation des données à caractère personnel traitées, l'organisme doit veiller à ne collecter et utiliser que les données pertinentes et nécessaires au regard de ses propres besoins de gestion des impayés. Il peut s'agir des données relatives :

a) **à l'identification de la personne concernée (qui peut être le débiteur ainsi que la ou les personnes physiques ayant la qualité de caution car s'étant engagées à remplir l'obligation du débiteur en cas de défaillance de ce dernier) ;**

Le code interne utilisé pour identifier la personne concernée dans la base de données ne peut pas être son numéro de carte bancaire, ni son numéro de sécurité sociale, ni encore celui de son titre d'identité.
Si l'organisme doit s'assurer de l'identité d'une personne, la simple consultation d'un justificatif (pièce d'identité) peut suffire. Lorsque la loi le prévoit ou si l'organisme justifie en avoir besoin pour se préconstituer une preuve en cas de contentieux, et ce en fonction des risques de mise en cause contentieuse, une copie de ce justificatif peut être conservée pour une durée de 6 ans. Dans ce cas, des mesures de sécurité renforcées telles que, par exemple, la limitation de la qualité de l'image numérisée ou l'intégration d'un filigrane comportant la date de collecte et l'identité de l'organisme, doivent être mises en œuvre afin de lutter contre les risques de mésusage de ces informations, en particulier l'utilisation des photographies à des fins de reconnaissance faciale. De même, ces informations ne doivent pas être conservées en base active mais doivent être stockées en base d'archivage intermédiaire.

b) **aux moyens de paiement utilisés** (voir le point 7) ;
c) **à l'incident de paiement :** numéro de dossier, date de survenance de l'impayé, montant de l'impayé, objet de l'impayé (descriptif du produit ou du service n'ayant pas fait l'objet de paiement par la personne concernée).

Après s'être assuré de la nécessité et de la pertinence des données à caractère personnel qu'il utilise, l'organisme doit par ailleurs, tout au long de la durée de vie du traitement, prendre toutes les mesures raisonnables pour garantir la qualité des données qu'il traite, afin de s'assurer de leur exactitude, tout au long de la durée du traitement.

Au titre de cette obligation d'exactitude des données qu'il traite, l'organisme doit prendre des mesures spécifiques afin de garantir que les personnes exclues de futures transactions sont bien celles qui sont en situation d'impayé avéré. Ces mesures peuvent comprendre des vérifications supplémentaires en cas de doute sur l'identité de la personne concernée ou des mesures pour empêcher la fraude à l'identité.

6. Destinataires des informations

Afin de respecter l'obligation de sécurité des données, les données à caractère personnel doivent être rendues accessibles uniquement aux personnes habilitées à en connaitre au regard de leurs attributions au sein des services internes de l'entreprise, des services chargés des contrôles ou auprès des sous-traitants.

En cas de recours à un sous-traitant, le contrat qui le lie à l'organisme doit faire mention des obligations qui incombent respectivement à chacune des parties en matière de protection des données (article 28 du RGPD). Le responsable de traitement doit documenter les instructions qu'il adresse au sous-traitant et qui concernent les modalités de traitement des données (article 22 alinéa 3.a du RGPD). Le guide du sous-traitant édité par la CNIL précise la nature de ces obligations et les clauses qu'il est recommandé d'intégrer dans les contrats. Par ailleurs, les habilitations d'accès doivent être documentées et les accès aux différents traitements doivent faire l'objet de mesures de traçabilité. Voir le point 10 relatif à la sécurité.

Pour assurer la continuité de la protection des données à caractère personnel, les transferts de ces données en dehors de l'Union européenne sont soumis à des règles particulières. Ainsi, toute transmission de données hors de l'UE doit, conformément au RGPD :

- être fondée sur une décision d'adéquation ; ou
- être encadrée par des règles internes d'entreprise, des clauses types de protection des données, un code de conduite ou un mécanisme de certification approuvé par la CNIL ; ou
- être encadrée par des clauses contractuelles ad hoc préalablement autorisées par la CNIL ; ou
- répondre à l'une des dérogations prévues à l'article 49 du RGPD.

7. Durées de conservation

Une durée de conservation précise doit être fixée en fonction de chaque finalité. Les données ne doivent en aucun cas être conservées pour une durée indéfinie. De manière générale, les durées de conservation ne devraient, en principe, pas dépasser les durées de prescriptions légales.

Des durées de conservations énumérées ci-après sont proposées. Si l'organisme choisit de conserver les données pour une durée plus longue que celle proposée par le référentiel, il devra s'assurer que cette durée n'excède pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

- En cas de régularisation de l'impayé, les informations relatives à la personne concernée devraient être effacées du fichier recensant les personnes en situation d'impayé dans les **48 heures** suivant le constat de la régularisation par l'organisme ou à partir du moment où l'impayé a été effectivement soldé.
- En cas de non-régularisation, les informations peuvent être conservées dans le fichier recensant les personnes en situation d'impayés et les excluant de ce fait du bénéfice d'une prestation, dans la limite de **5 ans à compter de la survenance de l'impayé.**

En tout état de cause, elles peuvent être archivées si l'organisme en a l'obligation légale (par exemple, pour répondre à des obligations comptables ou fiscales) ou si l'organisme souhaite se constituer une preuve en cas de contentieux et dans la limite du délai de prescription applicable.

Pour en savoir plus, vous pouvez vous référer aux guides de la CNIL :

- « Sécurité : Archiver de manière sécurisée » ;
- « Limiter la conservation des données ».

Les données utilisées à des fins statistiques ne sont plus qualifiées de données à caractère personnel dès lors qu'elles ont été dûment anonymisées (voir les lignes directrices du G29 sur l'anonymisation).

8. Information des personnes

Les traitements de données à caractère personnel doivent être mis en œuvre en toute transparence vis-à-vis des personnes concernées.

Dès le stade de la collecte des données à caractère personnel, les personnes doivent être informées des modalités de traitement de leurs données dans les conditions prévues par les dispositions des articles 13 et 14 du RGPD. Voir les modèles de mention d'information sur le site www.cnil.fr.

Conformément au RGPD, les organismes doivent mettre en œuvre les modalités d'information suivantes :

- En premier lieu, une information générale sur l'existence d'un traitement de données à caractère personnel relatif aux personnes en situation d'impayés doit être donnée au moment de la conclusion du contrat ou de la collecte de données ou avant d'effectuer le traitement,

conformément à l'article 13 (3) du RGPD. La personne concernée doit être clairement informée de la possibilité qu'elle y soit inscrite si elle ne remplit pas ses obligations de paiement.

- En deuxième lieu, en cas de survenance d'un impayé, la personne concernée doit être informée des moyens dont elle dispose pour régulariser son paiement, de la possibilité qu'elle a de présenter ses observations et, le cas échéant, de demander un réexamen de sa situation.
- En troisième lieu, si la personne n'a pas procédé à la régularisation du paiement, elle doit être informée de son inscription dans le fichier recensant les personnes en situation d'impayés, les excluant de ce fait du bénéfice d'une prestation.

Les personnes concernées doivent par ailleurs être informées de la manière d'exercer leurs droits.

9. Droits des personnes

Les personnes concernées disposent des droits suivants, qu'elles exercent dans les conditions prévues par le RGPD :

- droit d'**accès, de rectification et d'effacement** des données qui les concernent ;
- droit à la **limitation** du traitement : lorsque la personne conteste l'exactitude des données qui la concernent, elle peut demander à l'organisme le gel temporaire du traitement de ces données, le temps que celui-ci procède aux vérifications nécessaires ;
- droit à la **portabilité** : l'organisme doit permettre à toute personne de recevoir, dans un format structuré et couramment utilisé, l'ensemble des données traitées par des moyens automatisés. La personne concernée peut demander à ce que ses données soient directement transmises par l'organisme initial à un autre organisme. Ne sont concernées que les données fournies par la personne, comme par exemple la donnée relative à la régularisation de l'impayé, sur la base de son consentement ou d'un contrat. Il est donc recommandé de préciser aux personnes les traitements concernés par le droit à la portabilité.

Conformément à l'article 21 du RGPD, si la base légale du traitement est l'intérêt légitime, les personnes concernées disposent d'un droit d'opposition, à moins que l'organisme démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.

Conformément à l'article 22 du RGPD, et dès lors que le traitement est fondé sur l'exécution d'un contrat auquel la personne est partie, la personne concernée peut faire l'objet d'une décision fondée exclusivement sur un traitement automatisé produisant des effets juridiques la concernant, tels que le refus de toute transaction ultérieure en cas d'impayé non régularisé, sous réserve de lui garantir le droit d'obtenir une intervention humaine pour analyser sa situation, d'exprimer son point de vue et de contester la décision.

Pour faciliter l'exercice des droits, la CNIL recommande que l'organisme mette, a minima, à la disposition des personnes concernées une adresse de courriel dédiée et/ou les coordonnées du délégué à la protection des données (DPD/DPO) de l'organisation.

10. Sécurité

L'organisme doit prendre toutes les précautions utiles au regard des risques présentés par son traitement pour préserver la sécurité des données à caractère personnel, et notamment au moment de leur collecte, durant leur transmission et leur conservation, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

En particulier, dans le contexte spécifique de ce référentiel, l'organisme est invité à adopter les mesures suivantes, à justifier de leur équivalence ou du fait de ne pas avoir besoin ou de ne pas pouvoir y recourir :

Catégories	Mesures
Sensibiliser les utilisateurs	Informer et sensibiliser les personnes accédant aux données.
	Rédiger une charte informatique et lui donner une force contraignante.
Authentifier les utilisateurs	Définir un identifiant (*login*) propre à chaque utilisateur.
	Adopter une politique de mot de passe utilisateur conforme aux recommandations de la CNIL.
	Obliger l'utilisateur à changer son mot de passe après réinitialisation.
	Ne pas stocker les mots de passe en clair.
	Limiter le nombre de tentatives d'accès à un compte.
Gérer les habilitations	Définir des profils d'habilitation.
	Supprimer les permissions d'accès obsolètes.
	Réaliser une revue annuelle des habilitations.
Tracer les accès et gérer les incidents	Prévoir un système de journalisation.
	Informer les utilisateurs de la mise en place du système de journalisation.
	Protéger les équipements de journalisation et les informations journalisées.
	Prévoir les procédures pour les notifications de violation de données à caractère personnel.
Sécuriser les postes de travail	Prévoir une procédure de verrouillage automatique de session.
	Utiliser des antivirus régulièrement mis à jour.
	Installer un « pare-feu » (*firewall*) logiciel.
	Recueillir l'accord de l'utilisateur avant toute intervention sur son poste.
Sécuriser l'informatique mobile	Prévoir des moyens de chiffrement des équipements mobiles.
	Faire des sauvegardes ou des synchronisations régulières des données.
	Exiger un secret pour le déverrouillage des ordiphones.
Protéger le réseau informatique interne	Limiter les flux réseau au strict nécessaire.
	Sécuriser les accès distants des appareils informatiques nomades par VPN.
	Mettre en œuvre les protocoles WPA2 ou WPA2-PSK pour les réseaux Wi-Fi.
Sécuriser les serveurs	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées.
	Installer sans délai les mises à jour critiques.
	Assurer une disponibilité des données.
Sécuriser les sites web	Utiliser le protocole TLS et vérifier sa mise en œuvre.
	Vérifier qu'aucun mot de passe ou identifiant n'est incorporé aux URL.
	Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu.

Catégories	Mesures
	Recueillir le consentement pour les *cookies* et autres traceurs non nécessaires au service.
Sauvegarder et prévoir la continuité d'activité	Effectuer des sauvegardes régulières.
	Stocker les supports de sauvegarde dans un endroit sûr et éloigné du site principal.
	Prévoir des moyens de sécurité pour le convoyage des sauvegardes.
	Prévoir et tester régulièrement la continuité d'activité.
Archiver de manière sécurisée	Mettre en œuvre des modalités d'accès spécifiques aux données archivées.
	Détruire les archives obsolètes de manière sécurisée.
Encadrer la maintenance et la destruction des données	Enregistrer les interventions de maintenance dans une main courante.
	Encadrer par un responsable de l'organisme les interventions par des tiers.
	Effacer les données de tout matériel avant sa mise au rebut.
Gérer la sous-traitance	Prévoir des clauses spécifiques dans les contrats des sous-traitants.
	Prévoir les conditions de restitution et de destruction des données.
	S'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, *etc.*).
Sécuriser les échanges avec d'autres organismes	Chiffrer les données avant leur envoi.
	S'assurer qu'il s'agit du bon destinataire.
	Transmettre le secret par un envoi distinct et via un canal différent.
Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées.
	Installer des alarmes anti-intrusion et les vérifier périodiquement.
Encadrer les développements informatiques	Proposer par défaut des paramètres respectueux de la vie privée aux utilisateurs finaux.
	Éviter les zones de commentaires libres ou les encadrer strictement.
	Tester sur des données fictives ou anonymisées.
Utiliser des fonctions cryptographiques	Utiliser des algorithmes, des logiciels et des bibliothèques reconnus.
	Conserver les secrets et les clés cryptographiques de manière sécurisée.

L'organisme qui n'est pas tenu, en vertu de sa propre analyse, d'effectuer une analyse d'impact sur la protection des données, doit néanmoins s'assurer que le traitement respecte le niveau de sécurité approprié requis par l'article 32 du RGPD, en tenant compte de l'état de la technique, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques posés par le traitement, dont le degré de probabilité et de gravité varient pour les droits et libertés des personnes physiques.

Pour ce faire, l'organisme pourra utilement se référer au Guide de la sécurité des données personnelles.

11. Analyse d'impact relative à la protection des données

En vertu de l'article 35 du RGPD, le responsable de traitement pourrait avoir à réaliser une analyse d'impact relative à la protection des données (AIPD) dès lors que le traitement qu'il met en œuvre est susceptible de présenter un risque élevé pour les droits et les libertés des personnes concernées.

Tout d'abord, il conviendra de se référer aux listes publiées par la CNIL relatives aux traitements susceptibles de faire systématiquement l'objet ou non d'une AIPD :

- la liste des traitements pour lesquels une AIPD n'est pas requise ; puis,
- la liste des traitements pour lesquels une AIPD est requise.

Concernant cette dernière, s'y trouve notamment le type d'opérations de traitement suivant :

Type d'opération de traitement	Exemple
Traitements impliquant le profilage des personnes pouvant aboutir à leur exclusion du bénéfice d'un contrat ou à la suspension voire à la rupture de celui-ci	Traitement de lutte contre la fraude aux moyens de paiement.

Si le traitement mis en œuvre n'est pas présent sur l'une de ces listes, il faut alors s'interroger sur la nécessité d'effectuer une AIPD. A cette fin, il convient de consulter les critères établis par le Comité européen de la protection des données (CEPD) dans les lignes directrices concernant les AIPD. Celles-ci prévoient que la réalisation d'une AIPD est obligatoire dès lors qu'au moins deux des neuf critères ci-dessous sont remplis :

- évaluation ou notation d'une personne ;
- prise de décision automatisée ;
- surveillance systématique ;
- traitement de données sensibles ou à caractère hautement personnel ;
- traitement à grande échelle ;
- croisement ou combinaison d'ensembles de données ;
- données concernant des personnes vulnérables ;
- utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles ;
- traitements qui empêchent les personnes d'exercer un droit ou de bénéficier d'un service ou d'un contrat.

Afin de réaliser une AIPD, le responsable de traitement pourra recourir :

- aux principes contenus dans ce référentiel ;
- aux outils méthodologiques proposés par la CNIL sur son site web.

Dans le cas où l'organisme a désigné un délégué à la protection des données (DPD/DPO), ce dernier devra être consulté.

Pour rappel, conformément à l'article 36 du RGPD, le responsable de traitement devra consulter la CNIL avant toute mise en œuvre de son traitement si l'analyse d'impact indique qu'il ne parvient pas à identifier des mesures suffisantes pour réduire les risques à un niveau acceptable.