RÉFÉRENTIEL

RELATIF AUX TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL MIS EN ŒUVRE AUX FINS DE GESTION DES IMPAYÉS

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. À QUI S'ADRESSE CE RÉFÉRENTIEL ?

Ce référentiel encadre la mise en œuvre par les organismes de droit privé ou public d'un traitement de gestion d'impayés avérés, c'est-à-dire les cas dans lesquels la personne concernée est incontestablement débitrice d'une somme d'argent.

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 et les organismes d'enquête civile.

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 (clients, prospects, fournisseurs et toute personne susceptible d'être en relation contractuelle avec l'organisme dans le cadre de la gestion de son activité commerciale). À ce titre, ils sont soumis aux dispositions du RGPD et de la loi du 6 janvier 1978 modifiée.

Les organismes concernés, en tant que responsables de traitement, doivent mettre en œuvre toutes les mesures techniques et organisationnelles appropriées afin de garantir un haut niveau de protection des données personnelles 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. Les traitements mis en œuvre doivent être inscrits dans le registre prévu à l'article 30 du RGPD (voir les modèles de registre sur le site cnil.fr).

L'application de ce référentiel permet d'assurer la conformité des traitements de gestion des impayés au regard des principes relatifs à la protection des données. Il constitue également une aide à la réalisation d'une analyse d'impact relative à la protection des données (AIPD) dans les cas où celle-ci est nécessaire. Les organismes pourront ainsi définir les mesures permettant d'assurer la proportionnalité et la nécessité de leur traitements (points 3 à 7), de garantir les droits des personnes (points 8 et 9) et la maîtrise de leurs risques (point 10). À cette fin, l'organisme pourra se référer aux lignes directrices de la CNIL sur les analyses d'impact relatives à la protection des données (AIPD).

3. OBJECTIF(S) POURSUIVI(S) PAR LE TRAITEMENT (FINALITÉS)

Un traitement de gestion des impayés peut être mis en œuvre pour les finalités 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 première. Tout nouvel usage des données doit en effet 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.

Parce que plus sensibles, ce référentiel n'a pas vocation à encadrer les traitements suivants :

- 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 de l'identité des personnes en situation d'impayé avec des tiers et/ou avec d'autres débiteurs.

4. BASE(S) LÉGALE(S) DU TRAITEMENT

Chaque finalité du traitement doit correspondre à l'une des bases légales fixées par la réglementation.
La finalité d'exclusion de la personne pour toute transaction à venir peut être fondée sur **l'exécution d'un contrat auquel la personne concernée est partie.**
Dans le cas où la décision d'exclusion serait prise de manière entièrement automatisée, il est impératif, en application de l'article 22 alinéa 2(a) du RGPD, que le traitement soit fondé sur son caractère nécessaire à la conclusion d'un contrat entre la personne concernée et l'organisme.

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 PERSONNELLES CONCERNÉES

Dans un souci de minimisation des données personnelles 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** ;
b) **aux moyens de paiement utilisés** (voir également le point 7) ;
c) **à l'incident de paiement** (numéro de dossier, date de survenance de l'impayé, montant de l'impayé, motif de l'impayé, etc.).

Après s'être assuré de la nécessité et de la pertinence des données personnelles qu'il utilise, l'organisme doit par ailleurs s'assurer, tout au long de la durée de vie du traitement, de la qualité des données qu'il traite. Cela signifie en pratique que, conformément à la règlementation, les données soient exactes et mises à jour.

6. DESTINATAIRES DES INFORMATIONS

Les données personnelles doivent uniquement être rendues accessibles aux personnes habilitées à en connaitre au regard de leurs attributions.

Les habilitations d'accès doivent être documentées par les organismes, et les accès aux différents traitements doivent faire l'objet de mesures de traçabilité (**voir point 9 relatif à la sécurité**).

En cas de recours à un sous-traitant, le contrat qui le lie à l'organisme doit faire mention des obligations qui lui incombent en matière de protection des données (article 28 du RGPD). Le Guide du sous-traitant édité par la CNIL précise ces obligations et les clauses à intégrer dans les contrats.

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

- 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 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. **En aucun cas, les données ne doivent être conservées pour une durée indéfinie**.

En cas de régularisation de l'impayé, les informations relatives à la personne concernée doivent être effacées du fichier recensant les personnes en situation d'impayé au plus tard dans les 48 heures à partir du moment où l'impayé a été effectivement soldé. Si les circonstances le justifient, l'organisme peut, de manière exceptionnelle, conserver les données relatives à l'impayé même si ce dernier a été régularisé, à condition qu'il puisse démontrer que cette conservation est nécessaire et proportionnée, afin d'en prévenir leur renouvellement.

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 3 ans à compter de la survenance de l'impayé.

En tout état de cause, elles peuvent être archivées, si le responsable du traitement en a l'obligation légale (par exemple, pour répondre à des obligations comptables ou fiscales) ou s'il 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 auront ont été dûment anonymisées (Voir les lignes directrices du G29 sur l'anonymisation).

8. INFORMATION DES PERSONNES

Un traitement de données personnelles doit être mis en œuvre en toute transparence vis-à-vis des personnes concernées.

Dès le stade de la collecte des données personnelles, les personnes concernées doivent être informées des modalités de traitement de leurs données dans les conditions prévues par les articles 13 et 14 du RGPD. Voir les modèles de mention d'information.

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. 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 second lieu, en cas de survenance d'un impayé, la personne concernée doit être informée des moyens dont elle dispose pour régulariser son paiement, et de la possibilité qu'elle a de présenter ses observations et, le cas échéant, 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 et les excluant de ce fait du bénéfice d'une prestation.

En quatrième lieu, les personnes dont les données seraient conservées alors que la régularisation a eu lieu doivent en être spécifiquement informées, conformément aux principes de loyauté et de transparence. Cette information doit présenter les circonstances particulières justifiant une telle conservation, et expliquer en des termes clairs son caractère nécessaire et proportionné. En outre, la personne doit être clairement informée de la durée pour laquelle les données vont être conservées, cette durée ne pouvant excéder 1 an à compter de la régularisation.

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'ils 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 (par exemple, lorsque la personne conteste l'exactitude de ses données, celle-ci peut demander à l'organisme le gel temporaire du traitement de ses 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 sur la base de son consentement ou d'un contrat. Il est donc recommandé de préciser aux personnes les traitements concernés par ce droit à la portabilité.

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 du présent référentiel, **soit l'organisme adopte les mesures suivantes, soit il justifie de leur équivalence ou du fait de ne pas avoir besoin ou 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*) unique 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
	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
	Limiter les flux réseau au strict nécessaire

Catégories	Mesures
Protéger le réseau informatique interne	Sécuriser les accès distants des appareils informatiques nomades par VPN
	Mettre en œuvre le protocole 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 incrporé aux URL
	Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu
	Mettre un bandeau de consentement pour les *cookies* non nécessaires au service
Sauvegarder et prévoir la continuité d'activité	Effectuer des sauvegardes régulières
	Stocker les supports de sauvegarde dans un endroit sûr
	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 reconnues
	Conserver les secrets et les clés cryptographiques de manière sécurisée

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