RÉFÉRENTIEL

RELATIF AUX TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL MIS EN ŒUVRE AUX FINS DE GESTION DES ACTIVITÉS COMMERCIALES

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. À qui s'adresse ce référentiel ?

Ce référentiel propose des pistes de mise en conformité pour les fichiers « clients » et « prospects » des organismes de droit privé ou public.

Compte tenu de la nature particulière de leurs activités, ce référentiel n'a pas vocation à proposer un cadre pour les traitements mis en œuvre par :

- les établissements de santé ou d'éducation ;
- les établissements bancaires ou assimilés ;
- les entreprises d'assurances ;
- les opérateurs soumis à l'agrément de l'Autorité nationale des jeux.

2. Portée du référentiel

Les traitements réalisés dans le cadre de la gestion des activités commerciales, 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). 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 (RGPD), de la loi du 6 janvier 1978 modifiée, ainsi qu'aux dispositions spécifiques relatives à la protection de la vie privée dans le secteur des communications électroniques (« ePrivacy »).

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 de traitements, conformément aux dispositions de l'article 30 du RGPD (voir les modèles de registre sur le site cnil.fr).

L'application de ce référentiel, qui n'a pas de caractère contraignant, permet d'assurer la conformité des traitements de gestion des activités commerciales aux règles de protection des données à caractère personnel. 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 leur conformité au RGPD.

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 les traitements (finalités)

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

a) **gestion des contrats** (par exemple : gestion des commandes, de la livraison, de l'exécution du service ou de la fourniture du bien, des factures et paiements) ;
b) **gestion de programmes de fidélité au sein d'une entité ou de plusieurs entités juridiques.** Dans ce dernier cas, la personne doit être, par exemple au moment de la souscription au programme de fidélité, explicitement informée, notamment, de l'identité de la ou des entités considérées comme responsable unique ou conjointement responsables du traitement et de l'étendue du programme et, s'il implique la combinaison de données à caractère personnel détenues par plusieurs entités **;**
c) tenue de la comptabilité générale et des comptabilités auxiliaires qui peuvent lui être rattachées ;
d) établissement de statistiques financières concernant les clients ;
e) suivi de la relation client pour la réalisation d'enquêtes de satisfaction, la gestion des réclamations et du service après-vente ;
f) sélection de clients pour réaliser des études sur la qualité des produits ou des enquêtes de consommation (par exemple : des tests de produits, des statistiques de vente réalisées par l'organisme concerné) ;
g) **réalisation d'actions de prospection commerciale** (par exemple : envoi de messages publicitaires, jeux concours, parrainage, promotion) ;
h) **gestion des avis des personnes sur des produits, services ou contenus ;**

Ces traitements peuvent impliquer :

- **un profilage réalisé exclusivement à partir des données collectées par le responsable de traitement directement auprès de la personne concernée ; ou**
- **la mise à jour des données de contact** (coordonnées téléphoniques, adresses électroniques, adresses physiques).

Les informations recueillies pour l'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 au titre 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.

Par ailleurs, le référentiel fournit également des indications relatives aux opérations de transmission de données à des tiers afin de leur permettre de réaliser des opérations de prospection commerciale en précisant les bases légales susceptibles d'être mobilisées pour fonder ces opérations (voir point 6, ci-dessous).

Les traitements répondant aux finalités suivantes ne sont pas concernés par ce référentiel :

- la détection et la prévention de la fraude ;
- l'exclusion temporaire ou permanente des personnes du bénéfice d'une prestation de services ou de la fourniture d'un bien (par exemple, en raison d'impayés, d'incivilités des clients ou de comportements abusifs) ;
- le profilage réalisé à partir de données collectées depuis des sources tierces au responsable de traitement, ainsi que ceux réalisés à partir de données collectées par le biais de *cookies* et autres traceurs. Sur ce point, voir les lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « *cookies* et autres traceurs ») ainsi que les recommandations

proposant des modalités pratiques de mise en conformité en cas de recours aux « *cookies* et autres traceurs ».

4. Base(s) légale(s) des traitements

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

a) le consentement libre, spécifique, éclairé et univoque de la personne concernée ;

Le consentement, requiert, pour être valable, une action positive et spécifique de la personne concernée (p. ex. : une case à cocher dédiée et qui ne soit pas pré-cochée). Comme indiqué par le CEPD, l'acceptation de conditions générales d'utilisation ne peut suffire. L'accord doit être libre.

b) **l'exécution,** soit **d'un contrat auquel la personne concernée est partie**, soit **de mesures pré-contractuelles** prises à sa demande. 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 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 ;
c) le respect d'une obligation légale incombant à l'organisme ;
d) la réalisation de l'intérêt légitime poursuivi par l'organisme ou par le tiers, sous réserve de ne pas méconnaitre l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Le tableau ci-après, qui n'a pas vocation à être exhaustif, recense des exemples de bases légales pouvant être retenues en fonction de chaque finalité poursuivie par le ou les traitement(s) visés par le présent référentiel.

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

Illustration pratique des bases légales et des durées de conservation

FINALITÉ		BASE LÉGALE	DURÉE DE CONSERVATION RECOMMANDÉE
Gestion des contrats / programmes de fidélité	Gestion des commandes, de la livraison, de l'exécution du service ou fourniture du bien, etc.	Exécution du contrat	Durée de la relation contractuelle
Tenue de la comptabilité	Obligations comptables, fiscales, etc.	Respect d'une obligation légale de conservation des données (par exemple, l'obligation de s'assurer de l'identité de la personne en demandant la fourniture	Sous la forme d'archive intermédiaire : durée légale de conservation (par exemple, obligation comptable de 10 ans). La pièce d'identité est conservée le temps nécessaire pour procéder à la vérification

		d'un justificatif d'identité)	de l'identité de la personne concernée. Une copie d'un titre d'identité peut être conservée pendant la durée de 6 ans si celle-ci est nécessaire à des fins de preuve ou pour répondre à une obligation légale
Suivi de la relation client	Enquêtes de satisfaction	Intérêt légitime de l'organisme ou Consentement*	Durée nécessaire pour la réalisation de l'objectif de l'enquête ou jusqu'à l'exercice du droit d'opposition ou le retrait du consentement
	Gestion des réclamations	Exécution du contrat	Durée de la relation contractuelle
	Service après-vente	Exécution du contrat	Durée de la relation contractuelle
Sélection de clients / Etudes / Enquêtes	Études sur la qualité des produits	Intérêt légitime de l'organisme ou Consentement*	Durée nécessaire pour la réalisation de l'objectif de l'étude ou jusqu'à l'exercice du droit d'opposition ou le retrait du consentement
	Tests de produits		
	Statistiques de vente	Intérêt légitime de l'organisme	Durée nécessaire pour la réalisation de l'objectif visé par les statistiques ou jusqu'à l'exercice du droit d'opposition
Actions de prospection commerciale, (messages publicitaires, jeux concours, parrainage, promotion, etc.).	Par voie électronique (en vue de l'envoi de courriel, SMS, système automatisé de communication électronique sans intervention humaine, etc.), pour des biens ou services qui n'ont pas déjà été achetés par les personnes visées	Consentement (voir art. L. 34-5 du CPCE)	Jusqu'au retrait du consentement ou 3 ans à compter du dernier contact des personnes avec l'organisme
	Par voie postale ou système automatisé d'appels donnant lieu à intervention humaine et	Intérêt légitime de l'organisme ou consentement*	

	appels téléphoniques		
	À destination de professionnels (par voie électronique, postale ou téléphone)		
	Par voie électronique, pour des biens et services analogues déjà achetés / souscrits auprès du responsable de traitement		

* Conformément au RGPD, il revient au responsable de traitement de déterminer, en fonction des caractéristiques du traitement mis en œuvre, la base légale la plus appropriée.

5. Données à caractère personnel concernées

L'organisme ne doit collecter et n'utiliser que les données pertinentes et nécessaires au regard de ses besoins de gestion des activités commerciales. Il peut s'agir des données relatives :

a) à l'identification de la personne concernée ;

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 avant d'entrer en relation commerciale avec elle, 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 pré-constituer 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 maximale 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) à la vie professionnelle ;
c) **aux moyens de paiement utilisés,** c'est-à-dire les données strictement nécessaires pour l'exécution d'un paiement, plus précisément les données relatives à la carte bancaire (numéro, fin de validité, cryptogramme visuel, RIB) ou au chèque ;
d) **aux biens ou services souscrits** (données liées au règlement des factures, au suivi de la relation commerciale, aux avis laissés, à la gestion des réclamations, etc.).

Lorsque le bien acheté ou le service souscrit implique par exemple le traitement de données de santé ou de données directement relatives à l'orientation sexuelle, le consentement des personnes est requis. Par exemple, un site de rencontres qui requiert de renseigner son orientation sexuelle ou une

application mobile collectant des données de santé devraient, au préalable, recueillir le consentement des personnes désirant s'y inscrire.

La nature du bien ou du service consommé par une personne ne devrait pas être utilisée pour en déduire des informations la concernant susceptibles de relever de la catégorie des données dites « sensibles » (prétendue origine raciale ou origine ethnique, opinions politiques, convictions religieuses ou philosophiques ou appartenance syndicale, données concernant la vie sexuelle ou l'orientation sexuelle). En tout état de cause, toute catégorisation ou création de segments sur la base de telles données, aux fins de réaliser un tel profil et/ou d'adresser de la publicité personnalisée, doit répondre à une finalité légitime (article 5 du RGPD) et être soumise au recueil du consentement préalable du client concerné.

e) **à la situation familiale, économique et financière de la ou des personnes concernées** par la transaction lorsque de telles données présentent un lien avec la relation commerciale.

Un tableau ci-après énumère les principales données pouvant être collectées et traitées par l'organisme. En application du principe de minimisation des données, ne peuvent être collectées que celles qui sont nécessaires à la mise en œuvre de la finalité envisagée par le traitement de gestion commerciale (voir le point 3). La minimisation des données favorise, notamment, la conservation de données exactes et à jour.

Après s'être assuré de la nécessité et de la pertinence des données à caractère personnel qu'il utilise, l'organisme doit 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 de vie du traitement.

Type de donnée	Exemples
Identité	Civilité, nom, prénoms, adresse (y compris lieu de facturation), n° de téléphone, n° de fax, adresses de courrier électronique, date de naissance, code interne de traitement permettant l'identification du client, code d'identification comptable.
	Le code interne permettant l'identification ne peut pas être le numéro de carte bancaire, de sécurité sociale, ni de titre d'identité. En cas de collecte de la copie d'un titre d'identité, des mesures de sécurité renforcées, telles que, par exemple, la limitation de la qualité de l'image numérisée, l'intégration d'un filigrane comportant la date de collecte et l'identité du responsable de traitement, peuvent être mises en œuvre afin de se prémunir contre les risques de mésusage de ces informations et, par exemple, d'utilisation des photographies que ces pièces comprennent à des fins de reconnaissance faciale.
Situation personnelle	Vie maritale, nombre de personnes composant le foyer, nombre et âge du (ou des) enfant(s) au foyer, profession, domaine d'activité, catégorie socioprofessionnelle, présence d'animaux domestiques.
	La collecte de données sensibles (c'est-à-dire susceptibles de révéler une prétendue origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, l'orientation sexuelle ou des informations sur la santé de la personne concernée), sous réserve d'avoir recueilli le consentement de la personne concernée.
Vie professionnelle	Profession, catégorie économique, activité.

Type de donnée	Exemples
Règlement / Paiement	Données relatives à la carte bancaire (numéro, date de fin de validité, cryptogramme visuel), au virement (RIB) ou au chèque.
	Cryptogramme visuel de la carte bancaire, qui doit systématiquement être supprimé convient une fois la transaction effectuée.
	Remises consenties, reçus, soldes, crédits souscrits (montant et durée, nom de l'organisme prêteur) en cas de financement de la commande par crédit.
Transaction	Numéro de la transaction, détail de l'achat, de l'abonnement, du bien ou du service souscrit.
Suivi de la relation commerciale	Demandes de documentation, demandes d'essai, articles, produit acheté, service ou abonnement souscrit, services faisant l'objet de la commande et de la facture, quantité, montant, périodicité, date et montant de la commande et de la facture, échéance de la facture, conditions et adresse de livraison, historique des achats et des prestations de services, retour des produits, origine de la vente (vendeur, représentant, partenaire, affilié).
	Commandes, factures, correspondances avec le client et service après-vente, échanges et commentaires des clients et prospects, personne(s) en charge de la relation client.
Avis	Données relatives aux contributions des personnes qui déposent des avis sur des produits, services ou contenus, notamment leur pseudonyme.

6. Accédants et 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.

La réalisation de certaines des finalités couvertes par ce référentiel peut justifier de transmettre des données à des tiers (services de poste, bureaux d'étude ou de communication, organismes comptables etc.). Selon les cas, ces destinataires auront la qualité de sous-traitant de données ou seront pleinement responsables du traitement des données reçues.

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. Les habilitations d'accès devraient être documentées et les accès aux différents traitements faire l'objet de mesures de traçabilité (voir le point 10 relatif à la sécurité).

La transmission, à titre onéreux ou non, de données à caractère personnel à des partenaires commerciaux (tiers souhaitant les réutiliser à des fins commerciales) doit par ailleurs respecter les principes suivants :

- Si la transmission a pour finalité de permettre aux partenaires commerciaux de réaliser de la prospection sur la base de leur intérêt légitime (prospection non électronique) :

- elle peut elle-même être réalisée sur le fondement de l'intérêt légitime ;
- l'organisme transmettant les données doit informer les personnes concernées, sur le support de collecte des données (formulaire en ligne ou formulaire papier) de la finalité de cette transmission et des catégories de partenaires rendus destinataires des données. Dans un objectif de transparence, une liste exhaustive des destinataires, comportant leur identité, pourrait être régulièrement actualisée et mise à la disposition des personnes concernées depuis ce même support (par exemple, en y faisant figurer un lien hypertexte). Ce second niveau d'information peut aussi utilement indiquer la manière de prendre connaissance de la politique de protection des données de chaque partenaire commercial ;
- l'organisme transmettant les données doit offrir aux personnes concernées, de manière expresse et dénuée d'ambiguïté, la possibilité de s'opposer, sans frais et de manière simple, à la transmission de leurs données à caractère personnel **au moment où celles-ci sont recueillies** et à tout moment.

- Si la transmission a pour finalité de permettre aux partenaires commerciaux de réaliser de la prospection nécessitant le recueil du consentement préalable des personnes concernées (prospection électronique) :
  - eu égard au fait que la prospection commerciale par voie électronique présente des risques spécifiques (notamment par le volume de sollicitations susceptibles d'être reçues du fait de son automatisation), l'organisme transmettant les données doit informer les personnes concernées, sur le support de collecte des données (formulaire en ligne ou formulaire papier), et recueillir leur consentement à cette transmission ;
  - l'organisme transmettant les données doit, au préalable, avoir permis aux personnes concernées d'apprécier les conséquences de leur choix quant à la transmission en les informant de l'étendue de celle-ci. La mise en évidence, auprès des personnes concernées, du nombre et du secteur d'activité des partenaires qui seraient rendus destinataires des données, est un exemple de mesure contribuant à respecter les attentes raisonnables des personnes concernées en la matière ;
  - avant de réaliser de la prospection par voie électronique, les partenaires rendus destinataires des données doivent prouver qu'ils disposent, eux aussi, du consentement des personnes qui seront démarchées. En l'absence d'un tel consentement, le traitement de prospection commerciale par voie électronique est illicite.
    - À cet égard, la Commission recommande aux organismes transmettant les données de recueillir ce consentement, pour le compte des destinataires, au moment de la collecte initiale des données. Pour ce faire, les personnes doivent être informées de l'identité des partenaires responsables de traitement qui utiliseraient leurs données à des fins de prospection, par le biais d'une liste exhaustive mise à disposition directement sur ou depuis le support de collecte (par exemple, en y faisant figurer un lien hypertexte), ainsi que de la finalité spécifique de la transmission.
    - Dans un tel cas, les organismes transmettant les données peuvent utiliser une seule et même case à cocher pour recueillir le consentement à la transmission des données et celui lié à l'utilisation future des données, sous réserve de fournir une information préalable complète telle que décrite plus haut.
  - Lorsque l'organisme collectant et transmettant les données n'a pas recueilli le consentement pour le destinataire, ce dernier doit garantir la licéité de ses opérations de prospection par voie électronique, en recueillant lui-même, préalablement, le consentement des personnes concernées.
    - À cet égard la Commission estime que l'opération de sollicitation par laquelle l'acquéreur de la base de données propose aux personnes de recevoir des offres commerciales par voie électronique est elle-même un traitement de ces données, qui peut être fondé sur son intérêt légitime.
    - À ce titre, afin de vérifier si une telle opération s'inscrit dans le cadre des attentes raisonnables des personnes concernées, il incombe notamment au

partenaire de s'assurer que les personnes concernées ont reçu une information suffisante lors de la transmission de leurs données (par exemple sur le type de sollicitation, le nombre approximatif de partenaires, les secteurs concernés*, et la durée pendant laquelle le responsable de traitement sera autorisé à transmettre les données*).

- En tout état de cause, le nombre de sollicitations adressées à une même personne concernée devrait être limité dès lors que les personnes ne s'attendent pas à recevoir des sollicitations multiples qui peuvent constituer une nuisance importante.
- Le partenaire doit par ailleurs veiller à ce que la demande de consentement envoyée ne soit pas elle-même assimilable à une forme de prospection commerciale, soumise, de par son contenu et son mode de transmission, au régime du consentement préalable prévu par l'article L. 34-5 du CPCE. Dès lors, s'il est envoyé par voie électronique, le message de demande de consentement ne doit pas promouvoir l'image du destinataire ou les biens et services qu'il commercialise ;

Dans tous les cas, le consentement des personnes doit être conservé à titre probatoire et le recours à des cases pré-cochées n'est pas admis pour collecter le consentement des personnes concernées.

Enfin, de manière générale :

- les partenaires rendus destinataires des données doivent, lors de la première communication avec les personnes concernées, informer ces dernières de toutes les mentions prévues à l'article 14 du RGPD, telles que la manière d'exercer leurs droits, et notamment le droit d'opposition, ainsi que de la source d'où proviennent les données utilisées ;
- l'organisme transmettant les données est tenu de notifier aux partenaires auxquels les données à caractère personnel ont été communiquées, toute demande d'effacement ou de limitation du traitement exprimée par les personnes concernées.

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 doit être fixée en fonction de chaque finalité. De manière générale, les durées de conservation ne devraient, en principe, pas dépasser les durées de prescriptions légales.

Le référentiel propose des durées de conservation. Un organisme peut faire le choix de s'écarter du référentiel et choisir de conserver les données pour une durée plus longue ; il devra alors s'assurer que cette durée n'excède pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (article 6 du RGPD).

Le cryptogramme visuel de la carte bancaire doit être supprimé dès que le règlement de la prestation ou de l'achat est finalisé, d'une part parce qu'il n'est plus nécessaire une fois l'achat finalisé et, d'autre part, parce que sa conservation créée des risques en termes de sécurité. En revanche, le numéro d'une carte de paiement peut être conservé pour permettre des achats ultérieurs dans les conditions posées par la recommandation relative au traitement de la carte de paiement en matière de vente de biens ou de fourniture de services à distance (délibération n° 2018-303 du 6 septembre 2018).

Les données nécessaires à l'exécution des contrats sont conservées pendant la durée de la relation contractuelle.

Au terme du contrat, elles doivent être conservées en archivage intermédiaire et pour un délai raisonnable, 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. Il conviendra de prévoir à cet effet une base de données d'archives dédiée ou une séparation logique dans la base de données active, après avoir opéré un tri des données pertinentes à archiver. Dans ces hypothèses, les données sont traitées pour une autre finalité que l'exécution du contrat et doivent, conformément au RGPD, reposer sur une autre base légale, telle que l'intérêt légitime prévu à l'article 6.1.f ou l'obligation légale prévue à l'article 6.1.c.

Les données des clients utilisées à des fins de prospection commerciale peuvent être conservées pendant la relation commerciale, puis pour une durée de trois ans à compter de la fin de la relation commerciale (par exemple, à compter d'un achat, de la date d'expiration d'une garantie, du terme d'un contrat de prestations de services ou du dernier contact émanant du client).

Les données à caractère personnel relatives à un prospect non client peuvent être conservées pendant un délai de trois ans à compter de leur collecte par le responsable de traitement ou du dernier contact émanant du prospect (par exemple, une demande de documentation ou un clic sur un lien hypertexte contenu dans un courriel renvoyant vers le produit promu ; en revanche, la simple ouverture d'un courriel ne devrait pas être considérée comme un contact émanant du prospect).

Au terme de ce délai de trois ans, le responsable de traitement pourra reprendre contact avec la personne concernée afin de savoir si elle souhaite continuer à recevoir des sollicitations commerciales. En l'absence de réponse positive et explicite de la personne, il conviendra de supprimer les données ou de les archiver pour une durée conforme aux dispositions en vigueur.

Pour les activités commerciales qui impliquent la création d'un compte en ligne par les clients (par exemple, les sites de rencontres ou les réseaux sociaux), les données peuvent être conservées jusqu'à la suppression du compte par l'utilisateur. Toutefois, il est fréquent que les utilisateurs n'utilisent plus ces comptes sans pour autant les supprimer, ce qui conduit à faire perdurer ces comptes indéfiniment. Dans ce cas, l'organisme devrait déterminer un délai raisonnable à l'issue duquel le compte sera considéré comme inactif et devra en conséquence être supprimé. À cet égard, un délai de deux ans apparait proportionné. Enfin, les utilisateurs concernés pourront être avertis avant l'échéance de ce délai afin de leur laisser la possibilité d'exprimer leur souhait de maintenir leur compte actif.

Lorsqu'une personne exerce ses droits, les données collectées dans ce cadre, telles que les informations relatives à la demande de la personne concernée, peuvent être conservées jusqu'à ce que le responsable de traitement donne suite à la demande et dans le respect du principe de minimisation prévu à l'article 5.1.c. du RGPD. La réponse apportée pourra être conservée à des fins de preuve, dans la limite du délai

de prescription applicable, à compter du moment où le responsable de traitement répond à la demande.

Enfin, la collecte de pièces justificatives d'identité dans le cadre de l'exercice des droits n'est possible que lorsqu'il existe un doute raisonnable quant à l'identité de la personne, conformément à l'article 12.6 du RGPD. En principe, celles-ci doivent être supprimées dès qu'il a été fait droit à la demande de la personne concernée. En effet, la fourniture de tels documents a pour seul but de vérifier l'identité de la personne dont émane la demande et il n'est pas nécessaire de conserver ceux-ci une fois l'identité confirmée. Toutefois, il est possible de conserver ces documents à des fins d'établissement de preuves dans certains cas exceptionnels où le responsable de traitement identifie un risque contentieux fort, selon une analyse au cas par cas et dument documentée. Dans cette hypothèse, la durée de conservation des justificatifs est déterminée conformément aux délais de prescription de l'action publique prévus aux articles 8 et 9 du code de procédure pénale.

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, 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 web de la CNIL.

Selon la finalité poursuivie et les données collectées, le consentement des personnes (par exemple : en cas de prospection par voie électronique) ou un moyen de s'opposer à certaines opérations de traitement (par exemple : la prospection pour des produits ou services analogues, la prospection entre professionnels ou encore par voie postale) doivent également être prévus sur le formulaire de collecte des données.

Conformément au RGPD, les personnes concernées doivent également 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 de retirer leur consentement ou de s'opposer au traitement de leurs données ;
- 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, elle 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 porter à la connaissance des personnes les traitements visés par ce 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.

La prise en compte de la demande d'opposition dans un tel cas doit toutefois être systématique si elle porte sur des données faisant l'objet d'un traitement de prospection commerciale.

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. La mise en place d'un canal dédié à la réception des demandes d'exercice de droits n'exonère pas l'organisme de son obligation de traiter les demandes qui lui sont adressées par d'autres canaux.

Tout organisme voulant mettre en œuvre de la prospection commerciale par voie téléphonique devra retirer de sa liste les personnes inscrites sur la liste d'opposition prévue par les dispositions des articles L. 223-1 et suivants du code de la consommation (liste dite « BLOCTEL »), sans préjudice des exceptions légales.

10. Sécurité

L'organisme doit prendre, conformément au RGPD, 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.

Catégories	Mesures
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.
	Recueillir le 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 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.

Catégories	Mesures
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 dont le traitement remplit les conditions fixées par le présent référentiel doit 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 doit 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, à savoir :

- la liste des traitements pour lesquels une analyse d'impact n'est pas requise ; puis
- la liste des traitements pour lesquels une analyse d'impact est requise.

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

Type d'opérations de traitement	Exemples non exhaustifs
Traitements de données de localisation à large échelle	• Application mobile permettant de collecter les données de géolocalisation de ses utilisateurs ; • fourniture d'un service de géolocalisation de mobilité urbaine utilisé par un grand nombre de personnes ; • base de données « clients » des opérateurs de communication électronique.

Si le traitement mis en œuvre n'est pas présent sur l'une de ces listes, le responsable de traitement doit s'interroger sur la nécessité d'effectuer une AIPD. À cette fin, il convient de consulter les critères établis par le Comité européen de la protection des données (CEPD) dans ses lignes directrices. 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.

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.