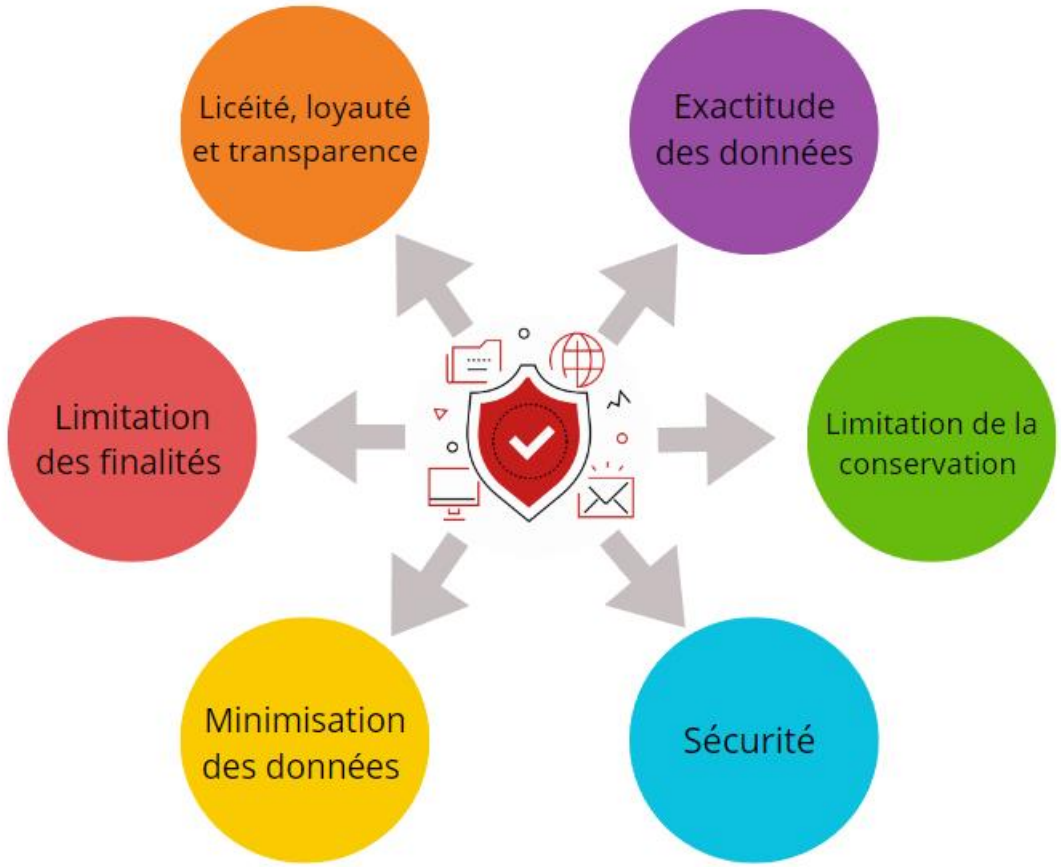
Les grands principes en matière de protection des données personnelles

L'article 4 de la Loi n° 1.565 du 3 décembre 2024 dresse la liste des 6 principes essentiels applicables en matière de protection des données personnelles que tout responsable du traitement se doit de respecter.

Ceux-ci sont les suivants :

- le principe de licéité, de loyauté et de transparence ;
- le principe de limitation des finalités ;
- le principe de minimisation des données ;
- le principe d'exactitude des données ;
- le principe de limitation de la conservation des données ; et
- le principe de sécurité des données.



Le principe de licéité, de loyauté et de transparence du traitement

La licéité

Conformément à l'article 5 de la Loi n° 1.565 du 3 décembre 2024, un traitement doit, pour être licite, répondre à au moins une des 6 exigences suivantes :

- l'obtention d'un **consentement**, pour **une ou plusieurs finalités** spécifiques, de la personne concernée ;

Qu'entend-on par consentement de la personne concernée ?
Le consentement est défini à l'article 2 de la Loi comme « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* ». La personne concernée doit donc manifester son accord au traitement de ses données personnelles de façon **libre, spécifique, éclairée et univoque, au moyen d'un acte positif clair.** [Pour plus d'information, voir la fiche pratique **Le consentement**]

Exemple : un site Internet prévoit deux cases à cocher lorsqu'il collecte l'adresse email des internautes, la 1ère pour autoriser l'envoi de la lettre d'information, la seconde pour consentir à l'envoi d'offres commerciales

- le besoin de respecter **une obligation légale** à laquelle est soumis le responsable du traitement ;

Exemple : le traitement relatif aux obligations en matière de lutte contre le blanchiment mis en œuvre par les banques

- sa nécessité pour **l'exécution d'un contrat** auquel la personne concernée est partie ou **l'exécution des mesures précontractuelles** prises à la demande de celle-ci ;

Exemple : la collecte du nom et de l'adresse postale du destinataire est nécessaire pour la livraison d'une commande effectuée en ligne

- sa nécessité pour la **sauvegarde des intérêts vitaux** de la personne concernée ou d'une autre personne physique ;

Exemple : le fichier automatisé tenu par un médecin pour le suivi médical de ses patients

- l'existence d'un **motif d'intérêt public** lorsque les traitements sont mis en œuvre par une personne morale de droit public ou par une personne morale de droit privé investie d'une mission d'intérêt général ou concessionnaire d'un service public ;

Exemple : le traitement par un service administratif des données relatives au suivi des personnes placées en foyer

- sa nécessité pour la réalisation d'un **intérêt légitime** poursuivi par le responsable du traitement ou par un tiers**, à moins que ne prévalent les intérêts ou les libertés des droits fondamentaux de la personne concerné** qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est **un mineur.**

Quelles questions se poser pour évaluer l'intérêt légitime ?
1ère étape : identifier un intérêt légitime : pourquoi voulez-vous traiter les données ? Quels sont vos objectifs ? Qui bénéficie du traitement ? Quel serait l'impact si vous ne pouviez pas continuer ? L'utilisation des données serait-elle contraire à l'éthique ou illégale d'une manière ou d'une autre ?... **2ème étape : démontrer que le traitement est nécessaire pour atteindre cet objectif :** le traitement contribue-t-il réellement à promouvoir cet intérêt ? S'agit-il d'une manière raisonnable de procéder ? Existe-t-il un autre moyen moins intrusif d'obtenir le même résultat ?... **3ème étape : trouver l'équilibre entre cet intérêt et les intérêts, droits et libertés des individus** : certaines données sont-elles considérées comme sensibles ? L'utilisateur s'attendrait-il raisonnablement à ce que les données soient utilisées de cette manière ? Certains utilisateurs pourraient-ils s'y opposer et dire que c'est trop intrusif ? Quel va être l'impact du traitement des données sur les personnes concernées ? Quelles garanties peuvent être mises en place pour minimiser l'impact ?...

Exemple *:* une bijouterie souhaite mettre en place un dispositif de vidéosurveillance à des fins sécuritaires. Son intérêt légitime est ainsi la protection de ses locaux et des biens de grande valeur qu'ils contiennent. Ce dispositif aura un effet de dissuasion puisqu'un affichage à l'entrée indiquera que l'établissement est sous vidéosurveillance et les images collectées par les caméras permettront la constitution de preuves en cas d'infractions. Enfin, les droits des personnes concernées seront protégés puisque celles-ci seront informées par l'affichage et que les caméras seront placées uniquement au niveau des endroits les plus sensibles, à savoir l'entrée et les espaces de vente.

Les traitements effectués par une personne morale de droit public ou par une personne morale de droit privé investie d'une mission d'intérêt général ou concessionnaire d'un service public dans l'exécution de leurs missions ne peuvent être fondés sur l'intérêt légitime. Dans ce cas, ces organismes peuvent utiliser le fondement du motif **d'intérêt public** pour justifier leur traitement.

Ces organismes peuvent toutefois fonder leurs traitements sur l'intérêt légitime, dès lors que ceux-ci ne rentrent pas dans leurs missions de service public. Il s'agit par exemple des traitements des données de leurs propres agents ou salariés, des activités purement internes, ou de prestations **qui ne sont pas proposées dans le cadre de leurs missions de service public.**

Lorsque le traitement poursuit une **autre finalité que celle pour laquelle les données ont été collectées**, le responsable du traitement doit **s'assurer que le traitement ultérieur est compatible avec la finalité pour laquelle les données ont été initialement collectées**. Pour ce faire, il peut notamment tenir compte :

- de **l'existence éventuelle d'un lien** entre les finalités initiales et les finalités du traitement ultérieur envisagé ;
- du **contexte** dans lequel les données personnelles ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;
- de la **nature des données personnelles**, en particulier si le traitement porte sur des données sensibles ou sur des données relatives aux infractions et condamnations pénales ;
- des **conséquences possibles du traitement ultérieur envisagé** pour les personnes concernées ;
- de **l'existence de garanties appropriées** pouvant comprendre le chiffrement ou la pseudonomysation.

Qu'est-ce que le chiffrement ?

Le terme « *chiffrement* » désigne un processus **réversible** permettant de rendre les informations d'un document **illisibles** afin d'en préserver la **confidentialité**.

Après chiffrement il est donc toujours possible de retrouver les données initialement chiffrées à l'aide d'une clé c'est-à-dire d'un algorithme de déchiffrement.

Qu'est-ce que la pseudonomysation ?

La pseudonomysation est un procédé qui consiste à **remplacer les données directement identifiantes** (nom, prénom, **…) par des données indirectement identifiantes** (numéro matricule, numéro de sécurité sociale, plaque d'immatriculation, numéro de téléphone, …).

Attention toutefois à ne pas confondre la pseudonomysation avec **l'anonymisation** qui est un processus neutralisant **irréversiblement** les données. Une donnée anonymisée ne permet pas ou plus d'identifier directement ou indirectement une personne physique.

Les données pseudonomysées **demeurent juridiquement des données à caractère personnel** contrairement aux données anonymisées.

La loyauté

Les données à caractère personnel doivent être également **traitées de manière loyale**. Cela implique que la personne concernée doit être informée du risque d'impact sur sa vie privée afin de s'assurer que le traitement n'a pas d'effets négatifs imprévisibles.

La transparence

Enfin, les données à caractère personnel doivent être **traitées de manière transparente**. Le principe de transparence implique que le responsable du traitement doit fournir à la personne concernée un certain nombre d'informations relatives au traitement de ses données (finalité(s), à l'identité du responsable de traitement ainsi que ses coordonnées, à la durée de conservation, aux destinataires, …) et leur respect au moment du traitement.

[Pour plus d'informations, voir la fiche pratique **Information des personnes concernées]**

Le principe de limitation des finalités

Les données personnelles peuvent être collectées pour **plusieurs finalités**, à condition que ces finalités soient :

- **déterminées** ;
- **explicites** ;
- **légitimes**.

De plus, les données ne doivent pas être **traitées ultérieurement** de manière **incompatible** avec ces finalités.

Exemple de finalité conforme : le service marketing d'une entreprise peut collecter l'adresse email de ses clients dans l'objectif de procéder à des envois d'offres promotionnelles

Exemple de finalité non conforme : l'opérateur téléphonique recueille l'adresse email de la personne concernée pour envoyer mensuellement les factures **et** pour tout autre traitement au choix de l'opérateur.

Cependant, le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, est considéré comme compatible avec les finalités initiales de la collecte **dès lors que des garanties appropriées** ont été mises en place**.**

Ne sont pas concernés par cette exception, les traitements :

- mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;
- qui intéressent la sécurité nationale.

Le principe de minimisation des données

Le responsable du traitement doit s'assurer que les données collectées sont « *limitées* » à la réalisation de ses objectifs.

Afin de respecter ce principe, les données personnelles collectées doivent être :

- **adéquates**,
- **pertinentes** et
- **limitées** à ce qui est nécessaire au regard des finalités du traitement.

Exemple : une boutique en ligne qui souhaite envoyer une offre promotionnelle pour l'anniversaire de ses clients n'a pas besoin de connaitre leur année de naissance. Seuls le jour et le mois suffisent.

Le principe d'exactitude des données

Les données personnelles traitées doivent être **exactes** et, si nécessaires, **mises à jour**.

Le responsable du traitement prend les **mesures raisonnables**, c'est-à-dire celles ne nécessitant pas des efforts **disproportionnés**, pour que les données inexactes ou incomplètes, soient effacées ou rectifiées **dans les meilleurs délais**.

Le principe d'exactitude des données doit être respecté pour **chaque** traitement mis en place par le responsable du traitement et s'apprécie **au regard du contexte** de la finalité du traitement des données.

Dans certaines hypothèses, il peut arriver que les données ne puissent être mises à jour. Il s'agit des cas où la finalité est essentiellement la documentation des évènements tels un **« *instantané* » historique**. Un compte-rendu médical ne pourra ainsi pas être mis à jour, même s'il apparaît par la suite que les conclusions y figurant étaient inexactes. Seuls des ajouts pourront être effectués, à condition d'être clairement identifiés comme étant des contributions intervenues à une date ultérieure.

Inversement, dans certaines situations, la mise à jour des données et leur exactitude est d'une **nécessité absolue** en raison du dommage potentiel pouvant être causé à la personne concernée si les données sont inexactes.

Exemple : les bases de données spéciales qui contiennent des données sur les antécédents de crédits de particuliers. Ces bases sont très utiles pour les établissements bancaires car elles permettent de vérifier la solvabilité du client potentiel en vue de l'obtention d'un crédit.

Le principe de la limitation de la conservation des données

Les données personnelles collectées ne peuvent être conservées indéfiniment sous une forme permettant l'identification des personnes concernées. Dès lors, la pratique a permis d'identifier 3 phases de la conservation d'une donnée : la conservation en base active et la conservation en base intermédiaire, qui forment ensemble la **durée d'utilité administrative,** et l'archivage définitif.

Conservation en base active

Les données personnelles sont conservées en base active pendant **la durée nécessaire à la réalisation des finalités** pour lesquelles elles ont été collectées.

Elles sont conservées de telle façon à être **facilement accessibles** pour les personnes qui sont **en charge du traitement de la demande**.

Exemples :

- les données personnelles fournies dans le cadre d'un formulaire de contact pendant le temps de traitement de la demande
- un dossier de candidature pour un poste.

Conservation en base intermédiaire

Une fois la finalité accomplie, certaines données doivent être conservées en base intermédiaire. Ce sont les données :

- présentant un **intérêt administratif pour l'organisme**

Exemple : la conservation des données/documents en cas de gestion d'un éventuel contentieux

ou

- faisant l'objet **d'une obligation légale**.

Exemple : la conservation des données de facturation

Archivage définitif

Certaines données peuvent être conservées pour une durée plus longue si elles sont traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques et ce sous réserve **de l'existence de garanties appropriées**.

Le principe de sécurité des données

Les traitements mis en place doivent garantir une **sécurité appropriée des données personnelles** afin de prévenir tout effet négatif pour la personne concernée, y compris la protection contre le traitement non autorisé ou illicite ou contre la perte, la destruction ou les dégâts d'origine accidentelle.

A cet effet, le responsable du traitement doit prendre des **mesures techniques et/ou organisationnelles** nécessaires afin de garantir l'intégrité et la confidentialité des données.

Le caractère approprié des mesures doit être **déterminé au cas par cas et réexaminé régulièrement**.