

La **Loi n° 1.165 du 23 décembre 1993** relative à la protection des informations nominatives n'est plus. La **Loi n° 1.565 du 3 décembre 2024** la remplace.



Pour les dossiers déposés sous l'empire de la Loi n°1.165 du 23 décembre 1993, modifiée, et toujours en cours d'instruction, la CCIN/l'APDP informera les responsables du traitement concernés de la nature de leurs nouvelles obligations.

Cette nouvelle législation prend en compte :

- la **Convention 108+** du Conseil de l'Europe et
- le « **paquet européen de protection des données** » de l'Union européenne, à savoir le **Règlement Général sur la Protection des Données** (RGPD) et la Directive dite « **Police-Justice** ».

Cette nouvelle Loi a une **portée à la fois territoriale et extraterritoriale** puisqu'elle s'applique aux traitements de données à caractère personnel, automatisés en tout ou partie, ainsi qu'aux traitements non automatisés de données contenues ou appelés à figurer dans des fichiers :

- **mis en œuvre par un responsable du traitement ou un sous-traitant établi à Monaco**, que le traitement ait lieu à Monaco ou non ;
- **relatifs à des personnes concernées se trouvant sur le territoire de la Principauté et mis en œuvre par un responsable du traitement ou un sous-traitant établi hors du territoire de la Principauté** lorsque les activités de traitement sont liées à l'offre de biens ou de services ou au suivi du comportement de ces personnes.

La Loi ne s'applique en revanche pas aux traitements mis en œuvre par une **personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques**.

Exemple : le stockage de photos de famille ou de photos privées sur un ordinateur

La nouvelle législation relative à la protection des données personnelles en 9 points clés :

Point 1 : Une nouvelle Autorité avec des pouvoirs renforcés

Les informations nominatives deviennent des **données personnelles** et la **Commission de Contrôle des Informations Nominatives (CCIN)** est remplacée par l'**Autorité de Protection des Données Personnelles (APDP)**.

Conformément à la Convention 108+, les pouvoirs de la nouvelle Autorité de protection des données sont renforcés, en particulier dans le **domaine des sanctions**.

Les missions de l'APDP sont au nombre de 20 et sont détaillées à l'article 38 de la nouvelle législation.

Elles peuvent se résumer comme suit :

- Protéger et défendre les droits des personnes concernées
- Accompagner et aider à la conformité
- Veiller au respect des obligations légales
- Sanctionner en cas de manquement à la Loi

Point 2 : Les principes essentiels en matière de protection des données personnelles

La Loi reprend dans son article 4 les **6 grands principes** prévus par les textes européens, à savoir :

- 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** ;
- le principe de **sécurité**.

Point 3 : Le renforcement des droits des personnes concernées

La personne concernée bénéficie désormais de 8 droits lui permettant de garder la maîtrise des données la concernant, à savoir :

- le droit à l'**information** (articles 10 et 11) ;
- le droit d'**accès** à ses données (article 12) ;
- le droit de **rectification** de ses données (article 13) ;
- le droit à l'**effacement** de ses données (article 14) ;
- le droit à la **limitation** du traitement (article 15) ;
- le droit d'**opposition** au traitement de ses données (article 17) ;
- le droit à la **portabilité** (article 18) ;
- le droit de **ne pas faire l'objet d'une décision produisant des effets juridiques à son égard ou l'affectant de manière significative**, prise sur le seul fondement d'un traitement automatisé, y compris le profilage (article 19).

Point 4 : Les obligations du responsable du traitement

La nouvelle loi **supprime un très grand nombre des formalités préalables** en vertu du nouveau **principe de responsabilisation**.

A cet égard, elle intègre **les outils de mise en conformité des traitements** applicables aux responsables du traitement, à savoir :

- la désignation dans certains cas d'un **représentant** en Principauté ou, à défaut, au sein d'un Etat membre de l'Union (article 25) ;
- la désignation dans certains cas d'un **Délégué à la Protection des Données** (articles 28, 29 et 30) ;
- la tenue d'un **registre des activités de traitement** (article 27) ;
- le respect de la protection des données **dès la conception et par défaut** (article 23) ;
- l'obligation de notifier les **violations de données** susceptibles d'engendrer un risque pour les droits et libertés des personnes concernées (article 32) ;
- l'obligation de réaliser une **analyse d'impact**, pour les traitements entraînant un **risque élevé** pour les droits et libertés des personnes concernées (articles 35 et 36) ;
- la possibilité d'adhérer à un **code de conduite** (article 33) ;
- la possibilité d'obtenir une **certification** (article 34).

Point 5 : Suppression de la plupart des formalités préalables

Dans une logique de **responsabilisation des responsables du traitement**, un très grand nombre de traitements ne font désormais plus l'objet de formalités préalables auprès de l'APDP (exemples : gestion des fichiers clients, gestion des obligations en matière de LAB).

Des exceptions demeurent toutefois (article 58 de la Loi).

Sont ainsi soumis à l'**avis préalable** de l'APDP, trois catégories de traitements présentant une **sensibilité particulière** :

- 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 ;
- les traitements portant sur des **données génétiques ou biométriques** nécessaires à l'**authentification** ou au **contrôle de l'identité** des personnes ;

Pour ces deux premières catégories de traitements, ne sont concernées par cette obligation de formalités préalables que **les Autorités administratives et judiciaires compétentes** dans le cadre exclusif des missions qui leur sont légalement conférées.

- les traitements ayant pour fin la **recherche dans le domaine de la santé**.

Est par ailleurs soumis à l'**autorisation préalable** de l'APDP, le transfert de données à destination d'un pays, d'un territoire ou d'une organisation internationale **n'assurant pas un niveau de protection adéquat** lorsque :

- des **garanties appropriées n'ont pas été mises en place**, et
- **aucune des dérogations prévues** à l'article 99 de la Loi ne s'applique, et
- les **4 conditions prévues** par le chiffre 3 de l'article 99 **ne sont pas réunies**.

Cas particulier des systèmes de vidéosurveillance :

L'article 85 de la Loi prévoit en outre que les systèmes de vidéosurveillance installés dans les **lieux non ouverts au public** sont **portés, sans délai, à la connaissance de l'APDP**.

Au sens de l'exposé des motifs, un lieu non ouvert au public est « *par exemple un lieu privé, (domicile, garage,...) ou des locaux à usage professionnel tels que les bureaux ou les entrepôts* ».

S'agissant plus particulièrement des **domiciles**, ou tout autre lieu affecté à un usage personnel ou domestique, la déclaration auprès de l'APDP doit être effectuée **uniquement si des personnes extérieures au cercle familial ou amical interviennent au domicile** ex : gens de maison, aides à domicile.

Les systèmes de vidéosurveillance installés dans des **lieux ouverts au public ou filmant les abords de voie publique, d'espaces ouverts au public ou à la circulation du public**, restent quant à eux soumis à **l'autorisation préalable du Ministre d'Etat**.

Au sens de l'exposé des motifs, les lieux ouverts au public sont par exemple « *un restaurant, une galerie commerciale, ou un guichet d'administration* ».

Enfin, il est important de souligner que dans certains cas, le responsable du traitement devra également « *procéder à une analyse d'impact comme notamment lorsque la surveillance s'exerce à grande échelle, par exemple, dans un centre commercial ou dans une galerie marchande* ».

Point 6 : Un encadrement du recours à la sous-traitance

Dès lors qu'un responsable du traitement a recours à un sous-traitant, ce dernier doit présenter les **garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées** de manière à assurer la **protection des données personnelles** et le **respect des droits des personnes concernées**.

Tout recours à un sous-traitant doit être régi par un contrat dont les clauses minimales sont prévues à l'article 26.

Le sous-traitant est par ailleurs soumis aux obligations suivantes :

- la désignation dans certains cas d'un **représentant** en Principauté ;
- la désignation dans certains cas d'un **Délégué à la Protection des Données** ;
- la tenue d'un **registre des activités de traitement**.

Point 7 : Une obligation de sécurité renforcée des données et de leur traitement

Tout responsable du traitement ou sous-traitant doit mettre en place des **mesures techniques et organisationnelles appropriées** afin de garantir un **niveau de sécurité adapté aux risques** pour les droits et libertés des personnes concernées.

L'adoption de ces mesures nécessite une analyse permettant d'identifier les risques puis de déterminer leur niveau de probabilité et de gravité.

Point 8 : Des sanctions renforcées

La formation restreinte de l'APDP peut prononcer une des sanctions suivantes en vertu de l'article 51 :

- un **avertissement** ;
- une **obligation de mise en conformité** du traitement ou de **satisfaire aux besoins de la personne concernée**, qui peut être assortie d'une astreinte pouvant aller jusqu'à **10.000 € / jour de retard calendaire** ;
- une **limitation temporaire ou définitive du traitement** ;
- un **retrait de l'agrément** ou l'injonction de refuser une certification ou de retirer la certification accordée ;
- un **retrait de la certification** délivrée ;
- une suspension totale ou partielle de la **décision d'approbation des règles d'entreprises contraignantes** ;
- une **suspension des flux de données** adressées à un destinataire situé à l'étranger ;
- une **amende administrative** (articles 53 et 54 de la Loi) pouvant aller jusqu'à 5.000.000 € (ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent) ou 10.000.000 € (ou, dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent).

Point 9 : Un encadrement des transferts de données

Si l'article 97 pose le principe selon lequel **tout transfert de données personnelles hors de la Principauté** peut s'effectuer **sans aucune formalité préalable** dès lors que la législation ou la réglementation des données personnelles du pays, du territoire ou de l'organisation internationale destinataire **dispose d'un niveau de protection adéquat**, les articles 98 et 99 encadrent strictement tous les autres transferts.

Ainsi tout transfert vers un pays ne disposant pas d'un niveau de protection adéquat, ne peut s'effectuer que si des **garanties appropriées** ont été mises en place par le responsable du traitement ou, lorsque cela n'est pas le cas, si une des dérogations expressément prévues par la Loi s'applique.

Si aucune de ces exigences n'est remplie, une **autorisation préalable de transfert** doit être demandée à l'APDP conformément à l'article 100.

Des documents seront produits par l'APDP pour informer et accompagner les responsables du traitement dans leur mise en conformité. De même, des outils de conformité seront mis à leur disposition sur le futur site de l'APDP.