

Les formalités à effectuer auprès de l'APDP

Si dans une logique de responsabilisation des responsables du traitement, un très grand nombre de traitements ne font plus l'objet de formalités auprès de l'APDP, des exceptions demeurent avec un régime de demandes préalables d'avis pour les traitements les plus sensibles, d'autorisations pour certains transferts et de déclarations, notamment pour les dispositifs de vidéosurveillance installés dans des lieux non ouverts au public.

Par ailleurs, de nouvelles obligations incombent également aux responsables du traitement, et parfois aux sous-traitants, en vertu de la Loi n° 1.565 du 3 décembre 2024, telles que la désignation d'un délégué à la protection des données et les notifications de violations de données.



Les demandes préalables

Les demandes d'avis

Sont 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**.

L'APDP rend son avis dans un délai de **deux mois** à compter du dépôt du dossier complet de demande d'avis.

Ce délai peut être renouvelé une fois sur **décision motivée** du Président de l'APDP.

Lorsque l'avis n'est pas rendu à l'expiration du délai, ledit avis est **réputé favorable**.

Que doivent contenir les demandes d'avis ?

Les demandes d'avis soumises à l'APDP doivent impérativement comporter les mentions suivantes :

- le **nom** et les **coordonnées professionnelles** du responsable du traitement ou de son représentant à Monaco ;
- le **fondement juridique** du traitement et, le cas échéant, le projet d'arrêté ministériel ou le projet d'arrêté du Secrétaire d'Etat à la Justice, Directeur des Services Judiciaires ;
- la ou les **finalité(s)** des traitements ;
- la **dénomination**, s'il y a lieu, du traitement ;
- les **catégories de données personnelles** traitées, leur origine et les catégories de personnes concernées par le traitement ;
- la **durée de conservation** des données personnelles traitées ou, en cas d'impossibilité, les critères utilisés pour déterminer cette durée ;
- le ou les **service(s) chargé(s) de la mise en œuvre** du traitement ;
- **l'analyse des risques relative à la sécurité** des traitements, y compris les mesures de sécurité ;
- l'autorité ou la fonction de la personne ou le service auprès de laquelle/duquel s'exerce le **droit d'accès** ainsi que les mesures prises pour faciliter l'exercice de ce droit ;
- les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont **accès aux données personnelles** ;
- les destinataires ou catégories de destinataires habilités à recevoir **communication des données personnelles** ;
- le cas échéant, **les interconnexions, les rapprochements**, ou toute autre forme de mise en relation avec d'autres traitements ;
- le cas échéant, l'identité et l'adresse du **sous-traitant** ;
- le cas échéant, les **transferts de données hors de la Principauté** et les **garanties appropriées** encadrant lesdits transferts.

Toute modification de traitement portant sur :

- le **fondement juridique** du traitement (et, le cas échéant, le projet d'arrêté ministériel ou projet d'arrêté);
- la ou les **finalité(s)** des traitements ;
- les **catégories de données personnelles** traitées, leur origine et les catégories de personnes concernées par le traitement ;
- la **durée de conservation** des données personnelles traitées ou, en cas d'impossibilité, les critères utilisés pour déterminer cette durée ;

doit faire l'objet sans délai d'une nouvelle demande d'avis.

Toute autre modification de traitement doit être communiquée sans délai par écrit à l'Autorité.

Les demandes d'autorisation

Sont soumis à l'**autorisation préalable** de l'APDP, les transferts de données à destination d'un Etat, 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 n° 1.565 du 3 décembre 2024 ne s'applique, et
- les **4 conditions prévues** par le chiffre 3 de l'article 99 de cette même loi **ne sont pas réunies**.



L'APDP délivre son autorisation dans un délai de **deux mois** à compter du dépôt du dossier complet de demande d'autorisation.

Ce délai peut être renouvelé une fois sur **décision motivée** du Président de l'APDP.

Lorsque l'autorisation n'est pas rendue à l'expiration du délai, ladite autorisation est **réputée refusée**.

[Pour plus d'informations, voir la fiche pratique **Les transferts de données hors Principauté : les scénarios à envisager**]

Lorsqu'une demande d'avis ou d'autorisation ne comporte pas l'ensemble des éléments obligatoires pour son instruction, l'APDP informe le responsable du traitement, dans un délai de 15 jours à compter de sa réception, des documents ou renseignements à fournir. Si ceux-ci ne lui sont pas communiqués sous un délai d'un mois à compter de la notification, la demande est déclarée irrecevable.



Les déclarations obligatoires

Les systèmes de vidéosurveillance dans des lieux non ouverts au public

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

Qu'entend-on par lieu non ouvert au public ?

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 (exemples : gens de maison, aides à domicile).



Quid des caméras installés dans des lieux ouverts au public

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* ».

Les transferts répondant aux critères du chiffre 3 de l'article 99 de la Loi n° 1.565 du 3 décembre 2024

Le chiffre 3 de l'article 99 de la Loi n°1.565 du 3 décembre 2024 prévoit qu'**en l'absence de niveau de protection adéquat et de garanties appropriées et si aucune des dérogations prévues aux chiffres 1 et 2 de cet article 99 n'est applicable**, un transfert de données vers un pays, un territoire ou une organisation internationale ne disposant pas d'un niveau de protection adéquat est possible, **si les 4 conditions suivantes sont réunies** :

- le transfert ne revêt **pas de caractère répétitif** ;
- le transfert ne touche qu'un **nombre limité de personnes** ;

- le transfert est nécessaire aux fins d'**intérêts légitimes impérieux** poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés des personnes concernées ;
- des **garanties appropriées** ont été prises.

Le responsable du traitement doit informer l'APDP de ce transfert.

Il **doit également informer les personnes concernées** par le transfert **des intérêts légitimes impérieux** qu'il poursuit **et des garanties appropriées** qui ont été prises.

Les Délégués à la protection des données (DPD ou DPO en anglais)

Obligatoire dans certains organismes et souvent recommandé dans d'autres, le DPD facilite le respect de la législation en matière de protection des données et agit à la fois comme l'interlocuteur privilégié pour toutes les questions relatives aux données personnelles, qu'elles soient internes ou bien qu'elles émanent d'une personne concernée par un traitement effectué, et comme le correspondant de l'Autorité de protection.

Dans quel cas un DPD doit-il impérativement être nommé ?

L'article 29 de la Loi n° 1.565 du 3 décembre 2024 prévoit qu'à l'exception des juridictions dans l'exercice de leurs fonctions juridictionnelles, la désignation d'un Délégué à la Protection des Données est obligatoire dans les cas suivants :

- le traitement de données est effectué par une **personne morale de droit public ou une personne morale de droit privé investie d'une mission d'intérêt général ou concessionnaire de service public** ;
- les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée ou de leurs finalités, exigent un **suivi régulier et systématique à grande échelle** des personnes concernées ;
- les activités de base de responsable du traitement ou du sous-traitant consistent en un traitement **à grande échelle de données sensibles ou de données à caractère personnel relatives à des condamnations pénales ou à des infractions**.



Dans tous les autres cas, même si cela n'est pas obligatoire, il est **recommandé de désigner un Délégué à la protection des données** dès lors qu'un organisme est **confronté à des problématiques liées à la protection des données personnelles**.

[Pour plus d'informations, voir la fiche pratique **Fiche métier du Délégué à la protection des données**]



Il appartient à l'organisme de publier les coordonnées professionnelles du Délégué à la protection des données et de les communiquer à l'Autorité de protection.

Les représentants

Mentionné à l'article 25 de la Loi n° 1.565 du 3 décembre 2024, le représentant est la personne physique ou morale **établie sur le territoire de la Principauté** ou, à défaut, au sein d'un Etat membre de l'Union européenne qui a été **mandatée** par un responsable du traitement ou un sous-traitant **non établi à Monaco** pour être **le contact** à la fois des personnes concernées par le traitement et de l'APDP. Celles-ci pourront alors s'adresser au représentant **pour toutes questions**.

Sa désignation est **obligatoire** dès lors qu'un responsable du traitement ou un sous-traitant, **non établi à Monaco, propose des produits ou des services** à des personnes **situées sur le territoire de la Principauté** ou met en œuvre des traitements relatifs au **suivi de leur comportement**.

Exemples :

- une entreprise de e-commerce établie en Italie et proposant des produits ou des services à des personnes situées en Principauté
- une entreprise de presse américaine qui propose un service d'abonnement en ligne à un journal sans disposer de bureau à Monaco

La désignation d'un représentant se fait par **tous moyens écrits**.

Cette obligation n'est pas générale et comporte **3 exceptions** :

- le traitement est **occasionnel** et n'implique pas un **traitement à grande échelle de données sensibles** ;
- le traitement est relatif à des **condamnations pénales** ou à des **infractions** ;
- le responsable du traitement est une **personne morale de droit public** ou un **organisme public**.

Les notifications de violations de données

La Loi n° 1.565 du 3 décembre 2024 introduit une nouvelle obligation à la charge du responsable du traitement : la notification de **toute violation des données à caractère personnel dont il a connaissance** dès lors que celle-ci est **susceptible** d'engendrer un **risque pour les droits et libertés des personnes concernées**.

Qu'est-ce qu'une violation de données ?

Une violation de données est un incident de sécurité qui concerne les données personnelles que détient un responsable du traitement.

Conformément aux trois principes de sécurité classiques, ces violations peuvent être classées en trois catégories :

- Les « **violations de la confidentialité** » : survient en cas de divulgation ou d'accès non autorisé ou accidentel à des données personnelles ;
- Les « **violations de l'intégrité** » se produit en cas d'altération non autorisée ou accidentelle de données personnelles ;
- Les « **violations de la disponibilité** » : correspond à la perte ou destruction accidentelle/ malveillante de données personnelles, ou à leur chiffrement par un tiers non autorisé.



Cette notification se fait **obligatoirement** auprès de **l'APDP** dès lors qu'une violation présente un risque **faible, moyen ou élevé** pour les droits et libertés des personnes concernées.

Elle doit se faire **dans les meilleurs délais**, et si possible dans un délai maximum de **72 heures après en avoir pris connaissance**.

Si le responsable du traitement ne dispose pas de toutes les informations concernant une violation dans les 72 heures après en avoir pris connaissance, notamment en cas de violation complexe, il peut procéder à une **notification échelonnée** avec une notification préalable de l'APDP dans les 72 heures contenant un résumé succinct de l'incident puis par la suite la fourniture d'éléments complémentaires et plus détaillés.

Lorsque la notification n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

[Pour plus d'informations, voir la fiche pratique **Les notifications de violations de données**]

Les consultations/validations obligatoires

Les analyses d'impact

Qu'est-ce qu'une analyse d'impact?
Nouvel instrument introduit par la Loi n° 1.565 du 3 décembre 2024, l'analyse d'impact relative à la protection des données (AIPD ou DPIA anglais) est une étude dont l'objectif est de déterminer et d'analyser les risques qu'un traitement de données peut poser à la vie privée des individus. Toute opération qui pourrait engendrer des risques pour les droits et libertés des personnes physiques ne requiert toutefois pas automatiquement une analyse d'impact. La loi n'exige en effet une analyse d'impact que lorsqu'un traitement est susceptible d'entraîner un risque élevé pour les droits et libertés, notamment en cas de recours à une nouvelle technologie de traitement.

Si lors de la réalisation de l'analyse d'impact, le responsable du traitement se rend compte que **les risques identifiés ne peuvent pas être suffisamment réduits** et qu'il existe des **risques résiduels élevés non maîtrisés**, l'article 36 de la Loi n° 1.565 du 3 décembre 2024 prévoit qu'il **doit** consulter au préalable l'APDP.

Le responsable du traitement communique ainsi à l'APDP les informations suivantes :

- les **responsabilités respectives** du responsable du traitement, des responsables conjoints et des sous-traitants participant au traitement et les coordonnées du délégué à la protection des données lorsque que celui-ci a été désigné ;
- **les finalités et les moyens** du traitement envisagé ;
- **les mesures et les garanties** prévues afin de protéger les droits et libertés des personnes concernées ;
- **l'analyse d'impact** qu'il a réalisée ;
- toute autre information demandée par l'Autorité.

L'APDP aura alors un délai de **8 semaines** pour rendre un **avis écrit** au responsable du traitement ; délai qui pourra être prolongé de 6 semaines en cas de traitements complexes.

Si l'Autorité considère que le traitement constitue en l'état une violation, elle imposera au responsable du traitement **les mesures appropriées** et pourra procéder aux **vérifications et investigations** prévues à l'article 46 de la Loi n° 1.565 du 3 décembre 2024.

[Pour plus d'informations, voir la fiche pratique **L'Analyse d'Impact relative à la protection des données personnelles**]

Les codes de conduite

Qu'est-ce qu'un code de conduite ?

Les codes de conduite font partie des nouveaux outils de conformité mis en place par la nouvelle législation (article 33).

Ils sont élaborés par les associations et organismes professionnels représentant des **catégories de responsables du traitement ou de sous-traitants**.

Ils permettent ainsi de répondre, **dans un secteur particulier**, aux **besoins opérationnels** des professionnels dans leurs démarches de conformité en matière de protection des données, en fournissant une **description détaillée** de l'ensemble des **comportements** les plus appropriés et les plus éthiques.

Une fois élaborés, les codes de conduite applicables à Monaco sont transmis à l'APDP pour **validation et publication**.

Toute modification ultérieure d'un code ou, le cas échéant, **sa prorogation** doit être transmise à l'APDP qui vérifie alors que ledit code **offre toujours des garanties de protection appropriées**.

L'APDP valide les projets de code, leur modification et leur prorogation dans un délai de **4 mois** à compter de la réception de la demande. Ce délai peut être prolongé de **2 mois supplémentaires** sur décision de son Président.

Lorsque l'APDP ne s'est pas prononcée dans ces délais, la demande est **réputée rejetée**.

Les codes de conduite, leurs modifications et, le cas échéant, leurs prorogations sont répertoriés par l'APDP **dans un registre accessible au public**.



Lorsqu' un code de conduite a déjà été **approuvé par une autorité de protection étrangère**, le responsable du traitement ou le sous-traitant doit le transmettre à l'APDP afin que celle-ci vérifie que les dispositions dudit code contiennent les **garanties appropriées au regard de la Loi**.

Pour résumer :

Demandes préalables	Déclarations	Consultations/validations
Demandes d'avis : (recherches dans le domaine de la santé et certains traitements mis en œuvre par les Autorités administratives et judiciaires compétentes dans le cadre exclusif des missions qui leur sont légalement conférées) Demandes d'autorisation (transferts ne répondant à aucune des conditions prévues aux articles 97 à 99 de la Loi)	Vidéosurveillance dans les lieux non ouverts au public Transfert répondant aux critères du chiffre 3 de l'article 99 Délégués à la protection des données Représentants Notifications de violations de données	Analyses d'impact qui présentent des risques résiduels élevés non maîtrisés Codes de conduite

Les formulaires pour effectuer ces formalités préalables sont disponibles sans frais sur le site Internet de l'APDP dans l'onglet **Formulaires et Outils** de la page **Professionnels**.