Glossaire

Analyse d'impact relative à la protection des données (AIPD) : nouvel instrument introduit par la Loi n° 1.565 du 3 décembre 2024, l'analyse d'impact relative à la protection des données est une étude dont l'objectif est de **déterminer et d'analyser, avant le lancement d'un nouveau traitement de données personnelles,** la façon dont les droits et libertés des personnes concernées par ledit traitement seront affectés.

Toute opération qui pourrait engendrer des risques pour les droits et libertés des personnes physiques ne requiert pas automatiquement une analyse d'impact.

La Loi n'exige en effet une telle analyse 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**.

La liste des critères permettant de déterminer si un traitement est susceptible d'engendrer un risque élevé est établie par l'Arrêté Ministériel n° 2025-361 du 14 juillet 2025 portant application de l'article 35 de la loi n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles .

Anonymisation : l'anonymisation est une technique consistant « *à supprimer tout caractère identifiant à un ensemble de données* ».

Il s'agit du « *processus par lequel des informations personnellement identifiables (IPI) sont irréversiblement altérées de telle façon que le sujet des IPI ne puisse plus être identifié directement ou indirectement, que ce soit par le responsable du traitement des IPI seul ou en collaboration avec une quelconque autre partie* » (Norme ISO 29100 : 2011).

L'anonymisation est donc marquée par le caractère **irréversible** de la **perte du caractère identifiable** d'individus.

[Pour plus d'informations, voir la fiche pratique **Anonymisation ou pseudonymisation**]

Certification : prévue à l'article 34 de la Loi n° 1.565 du 3 décembre 2024, la certification permet de démontrer que les **opérations de traitement** effectuées par les responsables du traitement ou les sous-traitants respectent la Loi.

C'est un outil de conformité **juridiquement contraignant**, pour ceux qui choisissent de s'engager dans cette démarche.

Ainsi, le candidat à la certification s'engage à respecter les critères approuvés par l'APDP et à maintenir cette conformité aux critères pendant toute la **durée de validité de son certificat.**

Il s'agit toutefois d'une **démarche volontaire.**

La procédure de certification peut être mise en œuvre par l'APDP ou par des organismes indépendants agréés par l'APDP.

Chiffrement : défini à l'article 2 de la Loi n° 1.565 du 3 décembre 2024 comme un « *procédé de transformation cryptographique des données permettant de les rendre incompréhensibles à toute personne qui ne dispose pas de la clé de déchiffrement* ».

Il s'agit d'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.

Codes de conduite : élaborés par les associations et organismes professionnels représentant des **catégories de responsables du traitement ou de sous-traitants**, les codes de conduite font partie des nouveaux outils de conformité mis en place par l'article 33 de la Loi n° 1.565 du 3 décembre 2024.

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 approprié et les plus éthiques.

Il s'agit d'une **démarche volontaire** qui encourage les professionnels d'un secteur donné à adopter des **bonnes pratiques et usages** (par exemple : des mesures de sécurité spécifiques) et à **démontrer**, auprès des personnes concernées et autres acteurs, le **respect des dispositions applicables aux traitements de données personnelles.**

Consentement : défini à l'article 2 de la Loi n° 1.565 du 3 décembre 2024 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 ».*

L'accord manifesté par la personne concernée doit donc **remplir 4 conditions**, à savoir être :

- **libre**: la personne concernée doit être en mesure **d'opérer un réel choix** concernant le traitement de ses données. Dès lors, elle **ne doit être ni contrainte ni influencée** dans son choix. Elle ne doit pas non plus subir des conséquences négatives si elle ne donne pas son consentement.
- **spécifique** : le consentement doit **être spécifique à la finalité** du traitement. En conséquence, lorsque le traitement comporte **plusieurs finalités**, le consentement doit être **indépendamment recueilli pour chaque finalité**. On parle alors de consentement **distinct** pour chaque finalité.
- **éclairé**: avant que la personne concernée ne fasse un choix, le responsable du traitement doit lui **communiquer certaines informations** qui sont listées à l'article 11 de la Loi n° 565 du 3 décembre 2024.

- **univoque**: le consentement doit être donné par une déclaration **orale** ou **écrite** de la personne concernée ou bien résulter d'un **acte positif clair**. Il ne doit en effet pas exister de doute raisonnable quant au souhait de la personne concernée de donner son accord au traitement de ses données.

Le silence ou l'inaction de la personne concernée ne constitue ainsi **pas un consentement valable** au sens de la législation relative à la protection des données personnelles car le consentement n'est pas univoque.

[Pour plus d'informations, voir la fiche pratique **Le consentement**]

Délégué à la protection des données ou DPD : prévu aux article 28, 29 et 30 de la Loi n° 1.565 du 3 décembre 2024, le DPD est la personne qui au sein d'une entité 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'APDP**.

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 DPD 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 de l'organisme 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 ;

Exemple : profilage et notation à des fins d'évaluation des risques

- les activités de base de l'organisme 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**.

Exemple : traitement des données de clients par une compagnie d'assurance ou une banque dans le cadre du déroulement normal de ses activités

Les missions du DPD sont au nombre de 5 :

- **informer et conseiller** l'organisme ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu de la législation en vigueur en Principauté ;
- **contrôler** le respect de la législation en matière de protection des données personnelles ainsi que les règles internes de l'organisme en matière de protection des données personnelles, y compris en ce qui concerne la **répartition des responsabilités**, la **sensibilisation et la formation du personnel** participant aux opérations de traitement, et les **audits** s'y rapportant ;
- **dispenser des conseils**, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données personnelles ;

- **coopérer** avec l'Autorité de protection et être son correspondant sur les questions relatives au traitement ;
- **présenter à l'Autorité de protection les demandes d'avis** lorsqu'elles portent sur les traitements suivants :
- les traitement mis en œuvre par les autorités administratives et judiciaires compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en 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 mis en œuvre par les autorités administratives et judiciaires, agissant dans le cadre de leurs prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.

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

Destinataire : défini à l'article 2 de la Loi n° 1.565 du 3 décembre 2024 comme « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers* ».

Ce même article précise toutefois que « *les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière ne sont pas considérées comme des destinataires* ».

Sont donc considérés comme des destinataires, les personnes, services, directions...autres que les autorités publiques dans le cadre d'enquête particulière, qui reçoivent communication des données.

Exemple : les partenaires commerciaux

[Pour plus d'informations, voir la fiche pratique **Les acteurs clés de la protection des données en Principauté**]

Données à caractère personnel ou données personnelles : définies à l'article 2 de la Loi n° 1.565 du 3 décembre 2024 comme « *toute information se rapportant à une personne physique identifiée ou identifiable […]. Est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

Ces données qui étaient qualifiées d'« *informations nominatives* » par la Loi n° 1.165 du 23 décembre 1993, modifiée, ont été détaillées par rapport à cette ancienne définition afin de préciser que :

- **les données génétiques** et
- **les données de localisation**

sont des données personnelles.

Dès lors, constitue une donnée personnelle toute information qui **se rapporte à une personne physique.**

Il convient de distinguer deux types de données personnelles :

- les données **directement identifiantes**

Ces données permettent **d'identifier clairement** l'identité de la personne.

Exemple : les nom et prénom d'une personne

- les données **indirectement identifiantes**.

Ces données permettent l'identification d'une personne de 2 façons :

- **par référence** à un numéro d'identification, comme par exemple :
- un numéro de téléphone
- une adresse postale ou un courriel
- un numéro de sécurité sociale
- un numéro de dossier
- une plaque d'immatriculation
- une adresse IP
- **par des éléments propres à son identité physique**, telles que :
- une photo ou vidéo
- un extrait sonore de la voix
- une empreinte digitale

En revanche, les coordonnées d'entreprises ainsi que les courriels de contact générique **ne sont pas**, en principe, des données personnelles.

Lorsqu'il est possible d'identifier une personne **par recoupement de plusieurs informations** telles que le sexe, l'âge, le métier et le lieu d'habitation, les données sont **toujours** considérées comme personnelles.

Données biométriques : définies à l'article 2 de la Loi n° 1.565 du 3 décembre 2024 comme « *les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques* ».

La biométrie se réfère aux **caractéristiques physiques** mais également aux **caractéristiques comportementales** d'un individu.

Exemples :

- la gestuelle
- la démarche

En vertu de la Loi, ces caractéristiques sont considérées comme des données sensibles lorsqu'elles sont traitées pour une finalité d'identification ou d'authentification unique d'une

personne physique.

Exemples :

- l'enregistrement de la voix **à des fins d'identification unique** d'une personne est une donnée sensible
- l'enregistrement de la voix à des fins d'amélioration du service qualité d'une entreprise sans identification de la personne n'est pas une donnée sensible

Données génétiques : définies à l'article 2 de la Loi n° 1.565 du 3 décembre 2024 comme « *les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question* ».

Ce sont des données relatives à des **caractéristiques héréditaires** qui sont notamment utilisées dans le **domaine de la santé**.

Exemples :

- la salive
- le sang
- le bulbe des cheveux

Elles peuvent également être utilisées pour une **finalité d'identification d'une personne** par le biais de ses empreintes génétiques.

Données sensibles : définies à l'article 2 de la Loi n° 1.565 du 3 décembre 2024 comme « *les données à caractère personnel qui révèlent, directement ou indirectement, des opinions ou des appartenances politiques, les* ***origines*** *raciales ou* ***les origines*** *ethniques,* ***les convictions*** *religieuses, philosophiques ou* ***l'appartenance syndicale,*** *ou encore des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique ou des données concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique* ».

Les données sensibles sont des données personnelles particulières en raison de leur **caractère hautement privé**.

L'article 7 de la Loi n° 1.565 du 3 décembre 2024 pose le **principe d'interdiction du traitement des données sensibles**.

Néanmoins, la Loi prévoit **13 dérogations** à ce principe, notamment :

- pour les traitements basés sur le **consentement explicite de la personne concernée**
- pour les traitements **nécessaires à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique,** dans le cas où celle-ci ne peut valablement donner son consentement par suite d'une altération de ses facultés personnelles, d'une incapacité physique ou juridique ou d'une impossibilité matérielle ;
- pour les traitements portant sur **des données manifestement rendues publiques**

Notification de violations de données : en vertu de l'article 32 de la Loi n° 1.565 du 3 décembre 2024, le responsable du traitement doit notifier **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.**

Exemple : un tiers non autorisé accède à un fichier RH d'une entreprise et en modifie le contenu

Cette notification doit se faire **dans les meilleurs délais**, et si possible dans un délai maximum de **soixante-douze heures après en avoir pris connaissance**.

Elle se fait **obligatoirement** auprès de **l'APDP** afin d'assurer la préservation des droits et libertés des personnes concernées par la violation par toute intervention nécessaire.

La notification peut également être accompagnée, dans certains cas, d'une **communication** auprès des **personnes concernées** par cette violation, lorsque ladite violation est **susceptible d'engendrer un risque élevé pour les droits et libertés** d'une personne physique**.**

L'appréciation du risque élevé se fait à la lumière d'un incident particulier et repose sur les conséquences qui pourraient en découler.

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

Personne concernée : la personne physique à laquelle **se rapportent les données** qui font l'objet du traitement.

Exemple : lorsqu'un magasin met en place un dispositif de vidéosurveillance, les personnes concernées sont toutes les personnes pouvant entrer dans le champ de vision des caméras, à savoir les salariés, les visiteurs et tout prestataire intervenant sur place.

Si la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives octroyait des droits aux **personnes morales**, à savoir un droit d'opposition et un droit d'accès, la nouvelle Loi n° 1.565 du 3 décembre 2024 a fait le **choix de ne pas maintenir lesdits droits** ; la pratique ayant démontré que **l'exercice** de ces droits était extrêmement **limité, voire inexistant et source de difficulté.**

Pseudonymisation : la pseudonymisation est définie au chiffre 16 de l'article 2 de la Loi n° 1.565 du 3 décembre 2024 comme étant « *le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable* ».

Aussi appelée « *anonymisation réversible* », elle consiste à **remplacer un attribut par un autre** dans un enregistrement.

La personne physique est donc toujours susceptible d'être identifiée indirectement.

Exemple: pour les recherches médicales, les participants sont identifiés uniquement par un numéro de patient attribué par le médecin investigateur. Ce dernier conserve toutefois un document non automatisé sur lequel ce numéro de patient est associé avec les nom et prénom du patient auquel il a été attribué afin de pouvoir si besoin l'identifier

[Pour plus d'informations, voir la fiche pratique **Anonymisation ou pseudonymisation**]

Profilage : l'article 2 de la Loi n° 1.565 du 3 décembre 2024 définit le profilage comme :« *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser celles-ci pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* ».

Exemple : l'accord d'un crédit est conditionné au résultat d'un algorithme qui se fonde sur des critères entièrement automatisés

Représentant : en vertu de l'article 2 de la Loi n° 1.565 du 3 décembre 2024, il s'agit de 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 établi hors du territoire de la Principauté pour être **le contact** à la fois des personnes concernées par le traitement et de l'APDP. Ces dernières 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

[Pour plus d'informations, voir la fiche pratique **Les acteurs clés de la protection des données en Principauté**]

Responsable du traitement : défini à l'article 2 de la Loi n° 1.565 du 3 décembre 2024 comme « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui détermine, seul ou conjointement avec d'autres, les finalités et les moyens du traitement* ».

Le responsable du traitement est ainsi la personne ou l'organe qui **dispose du pouvoir de décision** à l'égard des finalités et des moyens du traitement de données.

En général, il s'agit généralement de **la personne morale** (entreprise par exemple) incarnée par **son représentant légal** (son président par exemple).

Exemple : une holding qui décide pour ses entités des finalités d'un traitement en est le responsable.

Si deux responsables du traitement ou plus **déterminent ensemble** les finalités et les moyens du traitement, ils sont considérés en vertu de l'article 24 de la Loi n° 1.565 du 3 décembre 2024 comme étant les **responsables conjoints** du traitement.

Exemple : création et utilisation d'une plateforme commune par deux responsables du traitement qui proposent des services différents.

A ce titre, ils doivent définir **de manière transparente au sein d'un accord leurs obligations respectives**, notamment en ce qui concerne l'exercice des droits de la personne concernée.

Indépendamment des termes de l'accord, la personne concernée pourra exercer les droits que lui confère la Loi à l'égard de l'un ou l'autre, et contre chacun des responsables du traitement.

[Pour plus d'informations, voir la fiche pratique **Les acteurs clés de la protection des données en Principauté**]

Service de la société de l'information : défini à l'article 2 de la Loi n° 1.565 du 3 décembre 2024 comme étant « *tout service, à titre onéreux ou non, rendu à distance et sans que les parties soient simultanément présentes par voie électronique et à la demande individuelle d'un destinataire de services* ».

Exemples :

- commande de vêtements sur un site marchand
- abonnement en ligne à une revue électronique

Sous-traitant : défini à l'article 2 de la Loi n° 1.565 du 3 décembre 2024 comme « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* ».

L'article 26 de la Loi n° 1.565 du 3 décembre 2024 prévoit à cet égard que lorsque le responsable du traitement a recours à un sous-traitant, celui-ci 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**.

Par ailleurs, un sous-traitant ne peut agir que **sur instruction documentée** du responsable du traitement.

[Pour plus d'informations, voir la fiche pratique **Les acteurs clés de la protection des données en Principauté**]

Transferts de données : un transfert de données est **tout flux de données** vers un **pays, un territoire** ou **une organisation internationale hors Principauté**.

Il peut s'agir d'un **transfert physique** ou d'un **accès à distance**, que ce soit à l'intérieur d'un groupe ou à destination d'un tiers.

Exemple : la délocalisation des traitements (outsourcing)

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 règlementation des données personnelles du pays, du territoire ou de l'organisation internationale **destinataire** dispose d'un **niveau de protection adéquat constaté par la Principauté.**

Lorsque l'Etat ou l'organisation internationale destinataire des données ne figure pas sur la liste de pays assurant un niveau de protection adéquat, les différents scénarios prévus aux articles 98, 99 et 100 sont alors à envisager successivement :

- des garanties appropriées ont été mises en place par le responsable du traitement ou le sous-traitant ;
- le transfert remplit les conditions d'application d'une des dérogations prévues par la Loi ;
- les 4 conditions prévues par le chiffre 3 de l'article 96 sont réunies ;
- le transfert a été préalablement autorisé par l'APDP sur la base de mesures de protection particulières ou de clauses contractuelles spécifiques.

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

Traitement à grande échelle : défini à l'article 2 de la Loi n° 1.565 comme « *toute opération qui vise à traiter un volume considérable de données à caractère personnel, pouvant affecter un nombre important de personnes concernées apprécié en valeur absolue ou en valeur relative par rapport à la population concernée, et susceptible d'engendrer un risque élevé, compte tenu notamment de la durée ou la permanence de l'activité de traitement et de son étendue géographique* ».

Exemple: traitement des données de l'ensemble de ses clients par une compagnie d'assurance ou une banque dans le cadre du déroulement normal de ses activités

Traitement de données personnelles : défini à l'article 2 de la Loi n° 1.565 du 3 décembre 2024 comme « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, notamment la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'extraction, la consultation, l'utilisation, l'adaptation ou la modification, la communication, l'archivage, l'effacement ou la destruction de données, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'application d'opérations logiques ou arithmétiques à ces données* ».

Toute opération portant sur des données personnelles constitue ainsi un traitement au sens de la législation applicable en la matière.

Exemples:

- la collecte du nom et de l'adresse email d'une personne par le biais de la rubrique contact d'un site Internet
- l'enregistrement des conversations téléphoniques
- la mise en place d'un dispositif de géolocalisation sur des véhicules de fonction

Le traitement peut être **automatisé ou non**.

Exemple: un fichier papier

Sont toutefois exclus du champ d'application de la Loi n° 1.565 du 3 décembre 2024 les traitements relatifs aux **activités personnelles et domestiques**

Exemple : la constitution d'un fichier de coordonnées d'amis