

Fiche métier du Délégué à la Protection des Données

Qualifié par le Groupe de travail « Article 29 » (GT art. 29)¹ comme étant « *l'une des pierres angulaires du régime de responsabilité* », le Délégué à la Protection des Données (DPD) est désormais en Principauté un acteur clé dans le nouveau système de gouvernance des données.

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 Délégué à la Protection des Données 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 ;

¹ Groupe de travail européen indépendant qui traitait les questions relatives à la protection de la vie privée et aux données à caractère personnel jusqu'au 25 mai 2018 avant d'être remplacé par le Comité européen de la protection des données

Quid de la notion de suivi régulier et systématique

Selon les « *Lignes directrices concernant les délégués à la protection des données* » adoptées par le Groupe de travail « *Article 29* » le 13 décembre 2016, le terme « **régulier** » doit s'entendre comme :

- continu ou se produisant à intervalles réguliers au cours d'une période donnée ; ou
- récurrent ou se répétant à des moments fixes ; ou
- ayant lieu de manière constante ou périodique.

Le terme « **systématique** » s'entend quant à lui comme :

- se produisant conformément à un système ; ou
- préétabli, organisé ou méthodique ; ou
- ayant lieu dans le cadre d'un programme général de collecte de données ; ou
- effectué dans le cadre d'une stratégie.

Exemples : activité de marketing dont la personnalisation est fondée sur les données personnelles, profilage et notation à des fins d'évaluation des risques ou encore géolocalisation par des applications mobiles.

- 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**.

Quid de la notion de traitement à grande échelle

En vertu de l'article 2 de la Loi n° 1.565 du 3 décembre 2024 le traitement à grande échelle est entendu 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 du traitement et de son étendue géographique ».

Exemples : traitement des données de patients par un hôpital dans le cadre du déroulement normal de ses activités, traitement des données de voyage des passagers utilisant un moyen de transport public urbain ou encore traitement des données de clients par une compagnie d'assurance ou une banque dans le cadre du déroulement normal de ses activités.



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**.

Qui peut être nommé Délégué à la protection des données ?

Les qualifications

Le Délégué à la protection des données doit être désigné sur la base de ses qualités professionnelles et, en particulier, de ses **connaissances spécialisées du droit et des pratiques en matière de protection des données**, et de sa capacité à accomplir ses missions.

Ce niveau d'expertise doit être **proportionné** à la sensibilité, à la complexité et au volume des données traitées par l'organisme.



Il est important par ailleurs que le Délégué à la protection des données ait une **bonne compréhension** des opérations de traitement effectuées par l'organisme, des systèmes d'informations utilisés par ledit organisme et des besoins de celui-ci en matière de protection des données.

L'organisme doit également permettre au Délégué à la protection des données **d'entretenir et de compléter ses compétences et connaissances** (formation continue, participation à des ateliers, ...) pendant toute la durée de sa mission.

Les risques de conflits d'intérêts

La fonction de Délégué à la protection des données n'est pas forcément un emploi à temps plein. Il arrive en effet que celui-ci soit nommé à temps partiel et exerce d'autres fonctions au sein de l'organisme. Aussi, afin d'éviter que le Délégué à la protection des données ne soit « *juge et partie* », l'organisme doit s'assurer qu'il ne **dispose d'aucun pouvoir décisionnel sur la détermination des finalités et moyens de traitements**.

Pour cela, les responsables du traitements ou sous-traitants doivent adopter des **règles internes** pour définir et prévenir les conflits d'intérêts.

Ce risque de conflits d'intérêts s'apprécie en effet *au cas par cas* en fonction des activités, de la taille et de la structure de l'organisme et il est recommandé de procéder à un recensement des fonctions incompatibles avant de procéder à la nomination d'un Délégué à la protection des données.

A titre d'exemples, les fonctions suivantes sont plus susceptibles que d'autres d'entraîner un conflit d'intérêts : directeur général, directeur financier, directeur des opérations, directeur des ressources humaines ou encore responsable de la sécurité des systèmes d'information (RSSI). *Les cas particuliers*

Un seul Délégué à la protection des données peut être désigné **pour plusieurs personnes morales de droit public ou pour plusieurs personnes morales de droit privé investies d'une mission d'intérêt général ou concessionnaires d'un service public** compte tenu de leur structure organisationnelle et de leur taille.

Une convention devra alors déterminer les conditions dans lesquelles s'exerce cette **mutualisation**. **Chacune des parties à la convention de mutualisation demeure responsable des traitements qu'elle met en œuvre ainsi que de ses sous-traitants.**

Un **groupe d'entreprises** peut également désigner un seul Délégué à la protection des données à condition que celui-ci soit **facilement joignable à partir de chaque lieu d'établissement**.

Enfin, la fonction de Délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service (consultant, cabinet d'avocats, cabinet de conseil, ...).

Quelles sont les missions du Délégué à la protection des données ?

Les missions du Délégué à la protection des données consistent à accompagner, informer et conseiller l'organisme afin que celui-ci soit en conformité avec la législation monégasque en matière de protection des données.

Il a par ailleurs pour mission de coopérer avec l'Autorité de protection.



Les missions du Délégué à la protection des données sont ainsi au nombre de 5 :

- **Informier 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 traitements mis en œuvre 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.

De plus le Délégué à la protection des données peut être contacté par les personnes concernées pour toute question relative au traitement de leurs données, et pour l'exercice de leurs droits.



Pour l'accomplissement de ses missions, le Délégué à la protection des données doit impérativement **tenir compte du risque associé aux opérations de traitement** compte tenu de la nature, de la portée, du contexte et des finalités.

Comment le Délégué à la protection des données exerce-t-il ses missions ?

Les garanties

Afin de permettre aux Délégués à la protection des données de mener à bien les missions pour lesquelles ils ont été nommés, plusieurs garanties ont été mises en place.

C'est ainsi que le Délégué à la protection des données doit tout d'abord pouvoir **agir en toute indépendance**.

Pour cela, il ne doit recevoir d'instructions d'aucune autorité en ce qui concerne l'exercice de ses missions de DPD. Un dirigeant ne peut donc pas, par exemple, indiquer au Délégué à la protection des données quel résultat doit être obtenu ou quelle interprétation d'une disposition législative en matière de protection des données doit être retenue.

Cette indépendance ne signifie toutefois pas que le Délégué à la protection des données dispose de pouvoirs de décision allant au-delà des missions qui lui sont confiées.

Le Délégué à la protection des données doit par ailleurs disposer de **ressources suffisantes**.

Outre l'octroi de moyens financiers nécessaires et d'infrastructures (locaux, équipements, ...) adéquats, cette garantie comprend également le soutien actif du Délégué à la protection des données par l'encadrement supérieur, un temps nécessaire, notamment lorsque le Délégué à la protection des données est à temps partiel, pour accomplir ses missions, ou encore un accès facilité aux autres services (service des ressources humaines, service juridique, service informatique ...) pour l'obtention des informations dont il a besoin.



Le Délégué à la protection des données doit aussi être **associé**, d'une manière appropriée et en temps utiles, **à toutes questions relatives à la protection des données**. L'organisme devra donc veiller à inviter le Délégué à la protection des données à toutes réunions utiles et à prendre son avis avant toute décision ayant un impact sur la protection des données personnelles. Il devra également le consulter immédiatement en cas de violation de données ou de tout autre incident.



Il fait **directement rapport** au niveau **le plus élevé de la direction** du responsable du traitement ou du sous-traitant.

L'organisme doit en outre donner au Délégué à la protection des données l'accès aux données et aux opérations de traitement, à l'exception des traitements qui intéressent la sécurité nationale.

Les personnes concernées peuvent prendre contact avec le Délégué à la protection des données au sujet de **toutes les questions relatives au traitement de leurs données** à caractère personnel et à l'exercice des droits que leur confère la Loi.

Le Délégué à la protection des données **ne peut être relevé de ses fonctions ou pénalisé** par l'organisme pour l'exercice de ses missions. Concrètement, cela signifie qu'il ne pourra pas par exemple être relevé de ses fonctions pour avoir conseillé à l'organisme de faire une analyse d'impact pour un traitement de données qu'il considère susceptible d'engendrer un risque élevé pour la protection des données personnelles.

Enfin, le Délégué à la protection des données **ne peut être tenu responsable du non-respect par l'organisme de la législation sur la protection des données**. C'est en effet l'organisme qui reste tenu de s'assurer et d'être en mesure de démontrer que le traitement est conforme à la législation sur la protection des données. En conséquence, si l'organisme prend des décisions contraires à l'avis du Délégué à la protection des données, celui-ci doit pouvoir faire part clairement de son opinion divergente auprès de l'encadrement supérieur.

Les obligations

En contrepartie de toutes ces garanties, le Délégué à la protection des données est également tenu à certaines obligations.

La toute première d'entre elles est une **obligation de confidentialité** en ce qui concerne l'exercice de ses missions. Il est également soumis au **secret professionnel**.

Le Délégué à la protection des données doit en outre **faire preuve d'intégrité et d'un haut niveau de déontologie** afin de promouvoir et de faire respecter la protection des données personnelles au sein de l'organisme dans lequel il exerce ses fonctions.

Enfin, le Délégué à la protection des données **doit être joignable**, soit en étant physiquement dans le même lieu que les employés, soit au travers d'un service d'assistance téléphonique ou de tout autre moyen de communication sécurisé, afin que les personnes concernées puissent prendre contact avec lui.



A cet égard, 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.

Quelle est la sanction encourue en cas de manquement à l'obligation de nommer un Délégué à la protection des données ?

L'article 53 de la Loi n° 1.565 du 3 décembre 2024 prévoit que le manquement à l'obligation de nommer un Délégué à la protection des données est puni d'une amende administrative ne pouvant excéder **5.000.000 euros ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.**