



<https://www.porttic.be>

Le Délégué à la protection des données
(DPO)
Note de synthèse

Avec le soutien de la Wallonie
Avec le soutien de
la



Wallonie

Avec le soutien de
la



Wallonie

CAIPS a.s.b.l. Concertation des Ateliers d'Insertion Professionnelle et Sociale

Rue du Pont 24 – 4540 AMAY

Tél 04 337 89 64

Fax : 04/330 18 80

E-Mail : info@caips.be

Site Internet: www.caips.be - Delta Lloyd 634-2064301-19 - Ent. 0438406049 - RPM Liège - BIC: BNAGBEBB - Iban: BE39.6342 0643 0119

TABLE DES MATIERES

INTRODUCTION.....	2
CADRE LÉGAL.....	3
Base légale.....	3
Définitions utiles	3
LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES.....	4
1. Désignation.....	4
1.1. Principes généraux.....	4
1.2. Qualifications requises.....	5
2. Fonction du délégué à la protection des données	6
3. Missions.....	7
4. Responsabilités et protection du DPO.....	8
RESSOURCES	9

Introduction

Le Règlement général sur la protection des données (RGPD) est entré en vigueur le 25 mai 2018, imposant de nouvelles règles pour la collecte et le traitement des données, dont notamment la désignation d'un délégué à la protection des données à caractère personnel (DPO ou data protection officer en anglais – DPO).

Conformément à l'article 37.1. a) du RGPD, un(e) délégué(e) à la protection des données doit être désigné(e) dans trois cas :

1. Le traitement est effectué par une autorité publique ou un organisme public ;
2. Les activités de base du responsable de traitement consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées (profilage) ;
3. Les activités de base du responsable de traitement consistent en un traitement à grande échelle de données sensibles.

Jusqu'ici, seuls les CPAS se savaient directement concernés par cette obligation... mais au final, peu d'opérateurs y échapperont ! Suite à l'entrée en vigueur du RGPD, la notion d'autorité publique a été précisée par la loi du 30 juillet 2018 « vie privée » en son article 5. L'Unisoc (Union des entreprises à profit social), d'avis que cet article a une portée limitée à l'application de cette loi et que celle-ci ne fournit pas une définition de la notion d'autorité publique telle que reprise au RGPD, a saisi l'Autorité de protection des données pour en avoir confirmation.

Hélas, l'APD a rejeté les arguments de l'Unisoc. Par conséquent, **les asbl dont soit, l'activité est financée majoritairement par les autorités ou organismes publiques, soit, la gestion est soumise à un contrôle des autorités publiques, soit, la majorité des membres du conseil d'administration sont désignés par les autorités publiques, sont dans l'obligation de désigner un(e) délégué(e) à la protection des données.**

À titre subsidiaire, l'Unisoc a demandé à l'APD de prévoir un moratoire sur les contrôles afin de se donner la possibilité de prendre les initiatives politiques nécessaires pour faire trancher ce point. Cette demande a été rejetée également.

Par conséquent, nous ne pouvons que vous conseiller en tant qu'asbl qui rentre dans les critères de l'article 5 de la nouvelle loi « vie privée » de désigner un DPO pour éviter une sanction en cas de contrôle ou de plainte. Pour sa part, l'Unisoc ne manquera pas d'interpeller le prochain gouvernement fédéral sur cette interprétation qu'elle considère excessive et inadéquate de la portée de cette nouvelle loi.

Cadre légal

Base légale

- Règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ;
- Loi belge du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;
- Loi du 3 décembre 2017 portant création de l'Autorité de protection des données ;
- Lignes directrices concernant les délégués à la protection des données, adoptée le 13 décembre 2016 par le Groupe de Travail « article 29 » sur la protection des données ;
- Recommandation n° 04/2017 du 24 mai 2017 relative à la désignation d'un délégué à la protection des données conformément au Règlement général sur la protection des données, en particulier l'admissibilité du cumul de cette fonction avec d'autres fonctions dont celle de conseiller en sécurité.

Définitions utiles

- **Données à caractère personnel**

« Toute information se rapportant à une personne physique identifiée ou identifiable. Est réputée être une personne « 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 ».

- **Traitement des données à caractère personnel**

« Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensemble de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».

- **Responsable du traitement**

« La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement »

- **Sous-traitant**

« La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».

- **Autorité de protection des données (APD)**

« L'autorité de contrôle des traitements de données à caractère personnel »

Le Délégué à la protection des données

Le RGPD reconnaît le/la DPO en tant qu'acteur clé dans le nouveau système de gouvernance des données et établit les conditions relatives à sa désignation, à sa fonction et à ses missions.

Celui-ci doit informer, conseiller ou adresser des recommandations au responsable de traitement.

Il/elle est par ailleurs chargé(e) de contrôler les traitements des données au sein de l'association ainsi que sa mise en conformité au regard du RGPD.

Outre qu'il favorise le respect des règles grâce à la mise en oeuvre d'outils de responsabilité (comme la facilitation d'analyses d'impact relatives à la protection des données et la facilitation ou la réalisation d'audits relatifs à la protection des données), le délégué à la protection des données agit comme intermédiaire entre les acteurs concernés (par exemple, l'Autorité de contrôle, les personnes concernées et les entités au sein d'un organisme).

1. Désignation

1.1. Principes généraux

- **Délégué désigné en interne ou sur base d'un contrat de service :**

Le délégué peut être désigné en interne parmi les membres du personnel. Il est également possible de désigner une personne externe à l'Institution qui exercera ses missions sur la base d'un contrat de service.

Dans tous les cas, la disponibilité du délégué (qu'il se trouve physiquement dans le même lieu que les employés ou qu'il soit joignable à travers un service d'assistance téléphonique ou d'autres moyens de communication sécurisés) est essentielle pour que les personnes concernées puissent prendre contact avec lui.

- **La mission du délégué peut être assurée par une seule personne ou par une équipe :**

Les compétences et les atouts individuels de chacun peuvent être combinés de sorte que plusieurs personnes, travaillant en équipe, puissent mieux remplir les missions attribuées au délégué. Dans un souci de clarté et de bonne organisation, il est recommandé de prévoir une répartition claire des tâches au sein de l'équipe chargée de la fonction de délégué et de désigner, pour chaque bénéficiaire, une seule personne comme personne de contact principale. La structure interne de l'équipe ainsi que les tâches et responsabilités de chacun de ses membres doivent donc être clairement établies.

- **Possibilité de désigner un délégué unique pour plusieurs organismes :**

Il est possible de désigner un seul délégué pour plusieurs organismes. En effet, le RGPD autorise un groupe de structures à désigner un seul délégué à condition qu'il soit « *facilement joignable à partir de chaque lieu d'établissement* ». Cette nécessité d'être joignable se justifie par le fait que le délégué est le point de contact pour les personnes concernées et pour l'autorité de contrôle mais également en interne au sein de l'organisme.

Pour veiller à ce qu'il soit joignable, il est important de s'assurer que ses coordonnées sont mises à dispositions conformément aux exigences du RGPD.

Etant donné que le délégué est chargé d'une série de missions, le responsable du traitement doit s'assurer qu'un seul délégué peut, avec l'aide d'une équipe si nécessaire, s'acquitter efficacement de ces missions en dépit du fait qu'il soit désigné par plusieurs organismes.

- **Absence de conflit d'intérêt :**

Le RGPD autorise le délégué à exécuter d'autres missions et tâches. Toutefois, l'organisme doit veiller à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts. Cela signifie en particulier que le délégué ne peut exercer au sein de l'organisme une fonction qui l'amène à déterminer les finalités et les moyens du traitement de données à caractère personnel. Il convient donc d'éviter toute situation où une personne prend des décisions relatives à des traitements de données ou aux mesures de sécurité qui encadrent ces traitements et que, par la suite, cette même personne rende un avis sur les règles et les processus internes à appliquer.

Parmi les fonctions susceptibles de donner lieu à un conflit d'intérêts au sein de l'organisme peuvent figurer les fonctions d'encadrement supérieur (ex : directeur général, directeur financier, responsable du service informatique, etc.) mais aussi d'autres rôles à un niveau inférieur de la structure si ces fonctions supposent la détermination des finalités et moyens du traitement.

Le DPO ne peut donc pas être le directeur du personnel, un responsable du service informatique, etc.

- **Publication et communication des coordonnées du délégué :**

Le responsable du traitement doit publier les coordonnées du délégué et communiquer ces coordonnées à l'Autorité de protection des données.

Ces exigences visent à garantir que les personnes concernées et les autorités de contrôle puissent facilement prendre contact avec le délégué.

Ainsi, les coordonnées du délégué doivent être communiquées à l'Autorité de protection des données ainsi qu'aux employés de l'organisme et être publiées pour être rendues accessibles aux personnes concernées.

1.2. Qualifications requises

S'agissant des **qualifications** du délégué, le RGPD exige que le délégué à la protection des données soit désigné sur la base de ses qualités professionnelles (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.

- **Niveau d'expertise :**

Aucun diplôme ni certification particulière ne sont requis ; le niveau de connaissances spécialisées du DPO sera déterminé en fonction des opérations de traitement de données effectuées et de la protection exigée pour les données traitées. Elles seront donc adaptées à la sensibilité des données, la complexité et le volume de données traitées, de si les traitements impliquent des transferts réguliers ou occasionnels hors des frontières de l'Union, etc.

- **Qualités professionnelles :**

Il est nécessaire que le délégué dispose d'une expertise dans le domaine des législations et pratiques nationales et européennes en matière de protection des données, ainsi qu'une connaissance approfondie du RGPD. La formation adéquate et régulière des délégués est donc encouragée.

Outre un niveau d'expertise en protection des données, la connaissance du secteur d'activité et de l'organisation du responsable du traitement est essentielle. Le délégué devrait également disposer d'une bonne compréhension des opérations de traitement effectuées, ainsi que des systèmes d'information et des besoins du responsable du traitement en matière de protection et de sécurité des données.

- **Aptitude à exercer ses missions :**

La capacité du délégué à accomplir ses missions doit être évaluée tant au regard de ses qualités personnelles et ses connaissances que de sa position au sein de l'organisme. Ethique et intégrité sont liées au rôle clé que le DPO doit jouer dans la promotion d'une culture de la protection des données au sein de l'organisme, ce qui nécessitera souvent des capacités humaines de communication et de gestion des conflits.

« Il n'y a donc pas de **profil type** du/de la délégué(e) qui peut être une personne issue du domaine technique, juridique ou autre, mais la personne qui a vocation à devenir délégué à la protection doit pouvoir réunir les qualités et compétences suivantes :

- l'aptitude à **communiquer efficacement** et à exercer ses fonctions et missions en **toute indépendance**. Le délégué ne doit pas avoir de **conflit d'intérêts** avec ses autres missions. Cela signifie qu'il ne peut occuper des fonctions, au sein de l'organisme, qui le conduisent à déterminer les finalités et les moyens d'un traitement (éviter d'être « juge et partie »).
- une **expertise** en matière de **législations** et pratiques en matière de protection des données, acquise notamment grâce à une **formation continue**. Le niveau d'expertise doit être **adapté à l'activité** de l'organisme et à la **sensibilité** des traitements mis en œuvre.
- une **bonne connaissance** du secteur d'activité et de l'organisation de l'organisme et en particulier des **opérations de traitement**, des **systèmes d'information** et des **besoins** de l'organisme en matière de **protection** et de **sécurité** des données.
- un **positionnement efficace en interne** pour être en capacité de **faire directement rapport au niveau le plus élevé** de l'organisme et également **d'animer un réseau** de relais au sein des filiales d'un groupe par exemple et/ou une **équipe** d'experts en interne (expert informatique, juriste, expert en communication, traducteur, etc.) »

(source : CNIL.fr, Autorité française de protection des données, consulté le 12/04/2019)

2. Fonction du délégué à la protection des données

Le responsable du traitement doit veiller à ce que le délégué « soit associé, d'une manière appropriée et en temps utiles, à toutes les questions relatives à la protection des données à caractère personnel ».

Dans le cadre de sa fonction globalement d'accompagnement et de suivi du respect du RGPD au sein de l'organisation, plus que de contrôle au sens strict du terme, un(e) délégué(e) pourra notamment :

- Collecter des informations pour identifier les activités de traitement ;
- Analyser et vérifier la conformité des activités de traitement au RGPD, et ;
- Informer, conseiller ou adresser des recommandations au responsable du traitement ou au sous-traitant ;
- Former et sensibiliser toute personne impliquée ;
- Coopérer avec l'autorité de protection des données et être le contact privilégié pour la personne concernée.

Pour ce faire, le RGPD exige de l'organisation qu'elle aide son délégué en lui fournissant l'accès aux données à caractère personnel et aux opérations de traitement ainsi qu'en mettant à sa disposition les **ressources** nécessaires pour exercer ses missions, et en lui permettant d'entretenir ses connaissances spécialisées. Au plus les traitements sont complexes et/ou sensibles, au plus il convient d'offrir des ressources au délégué.

À cet égard, il convient notamment de prévoir ce qui suit :

- Soutien actif de la fonction du délégué par le management supérieur (par ex. au niveau de la direction) ;
- L'associer en temps utile, et dès le départ d'un nouveau projet, à toutes les questions relatives à la protection des données à caractère personnel ;
- Temps suffisant pour que le délégué puisse remplir ses missions. Cet aspect est particulièrement important lorsqu'un délégué est désigné à temps partiel ou lorsqu'il est chargé de la protection des données en plus d'autres tâches. Autrement, des conflits de priorités pourraient conduire à ce que les tâches du délégué soient négligées. Il est important que le délégué puisse consacrer suffisamment de temps à ses missions.
- Soutien suffisant en termes de ressources financières, d'infrastructures (locaux, installations, équipements) et, si nécessaire, de personnel ;
- Communication officielle de la désignation du délégué à l'ensemble du personnel ainsi qu'à l'Autorité de contrôle afin de veiller à ce que l'existence et la fonction de celui-ci soient connues ;
- L'accès requis aux autres services au sein de l'organisation (ressources humaines, service juridique, informatique, etc.) de sorte que le délégué reçoive le soutien, la contribution et les informations essentiels de ces autres services ;
- Formation continue : le délégué doit avoir la possibilité de maintenir ses connaissances à jour en ce qui concerne les évolutions dans le domaine de la protection des données.
- L'assurance que l'avis du délégué soit toujours dûment pris en considération. A titre de bonne pratique, le G29 recommande de consigner les raisons pour lesquelles l'avis du délégué n'a pas été suivi.
- Indépendance et autonomie : le responsable du traitement doit veiller à ce que le délégué ne reçoive aucune instruction en ce qui concerne l'exercice de ses missions. Le délégué doit être en mesure d'exercer ses fonctions et missions en toute indépendance. Il ne doit donc recevoir aucune instruction sur la façon de traiter une affaire.
Toutefois, il ne dispose pas de pouvoirs de décision allant au-delà des missions qui lui incombent. En effet, le responsable du traitement reste responsable du respect de la législation sur la protection des données et doit être en mesure de démontrer ce respect.

3. Missions

Le RGPD définit par ailleurs les **missions** (minimales) du délégué qu'il/elle accomplira en tenant compte du risque associé aux opérations de traitement lié à la nature, la portée, le contexte et les finalités du traitement :

- Informer et conseiller le responsable du traitement ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu de la réglementation en matière de protection des données;
- Contrôler le respect de la réglementation en la matière et des règles internes du responsable du traitement en matière de protection des données à caractère personnel, 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 et vérifier l'exécution de celle-ci ;
- Coopérer avec l'autorité de contrôle ;

- Faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable, et mener des consultations, le cas échéant, sur tout autre sujet.

Par ailleurs, le délégué tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement. Ainsi, le délégué doit établir des priorités dans ses activités et concentrer ses efforts sur les questions qui représentent un risque élevé en matière de protection des données.

Ces missions du délégué couvrent la protection des données dans tous ses aspects juridiques, techniques et organisationnels :

- principes de licéité, finalité, proportionnalité et sécurité ;
- droits des personnes concernées ;
- protection des données dès la conception et par défaut ;
- registre des activités de traitement ;
- encadrement des flux transfrontières ;
- sécurité des traitements et de l'information ;
- notification des violations de données.

4. Responsabilités et protection du DPO

Le délégué ne doit pas être relevé de ses fonctions ou pénalisé par le responsable du traitement pour l'exercice de ses missions. Cette exigence renforce l'autonomie du délégué et contribue à garantir que celui-ci agisse en toute indépendance et bénéficie d'une protection suffisante dans l'exercice de ses missions relatives à la protection des données.

Afin de l'aider à pouvoir faire son travail en toute **indépendance**, le RGPD reprend différentes garanties :

- Le délégué ne reçoit aucune instruction sur la manière d'exécuter ses missions en tant que délégué ;
- Le délégué fait rapport directement au niveau le plus élevé de la direction ;
- Le délégué ne peut pas être relevé de ses fonctions ou pénalisé pour l'exercice de ses missions ;
- Le délégué peut se voir conférer d'autres missions et responsabilités uniquement si celles-ci n'engendrent pas de conflit d'intérêt.

Par ailleurs, le délégué n'est pas personnellement responsable en cas de non-respect du RGPD. C'est le responsable de traitement qui est tenu de s'assurer et d'être en mesure de démontrer que le traitement est effectué conformément aux dispositions du RGPD. Le respect de la protection des données relève de la responsabilité du responsable du traitement ou du sous-traitant.

Ressources

Pour vous accompagner dans le **choix d'un délégué** en conformité avec le RGPD, l'Autorité de protection des données a publié une [recommandation](#) (n° 04/2017 du 24 mai 2017) en la matière.

Participant au Groupe de Travail institué par l'article 29 de la directive 95/46/CE, l'APD a également publié des lignes directrices d'interprétation des articles pertinents du RGPD ainsi que formulé un certain nombre de recommandations : « [Lignes directrices concernant les délégués à la protection des données \(DPO\)](#) » (WP 243 du 13 décembre 2016, révisé après consultation publique et adopté dans sa version définitive le 5 avril 2017).

Retrouver ces infos en vidéo (<https://www.youtube.com/watch?v=i8PSL2T4pSo>), et plus, au dossier thématique « Délégué à la protection des données » sur le site de l'APD : <https://www.autoriteprotectiondonnees.be/dossier-thematique-delegue-a-la-protection-des-donnees>.