https://ressources.anap.fr/numerique/publication/2741-mutualisation-externalisation-dpd

Avis d'experts

Mutualiser ou externaliser la fonction de Délégué à la Protection des Données (DPD-DPO)

Cet avis d'expert aborde les éléments à prendre en compte dans la décision de mutualiser ou d'externaliser la fonction de Délégué à la Protection des Données exigée par le RGPD.

Cet avis d'expert a été rédigé par Christian VIALLON, membre du collège d'experts de l'ANAP.

Rappels

- **La désignation d'un Délégué à la Protection des Données** (DPD)[1] est **obligatoire** dans les secteurs sanitaire et médico-social[2] lorsqu'au moins une des trois conditions suivantes est remplie :
  - les traitements sont effectués par une autorité publique ou un organisme public[3] ;
  - les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement exigeant un suivi régulier et systématique à grande échelle des personnes concernées (ex. : le suivi d'un patient à l'hôpital est considéré comme générant un traitement de données à grande échelle) ;
  - les activités de base du responsable du traitement consistent en un traitement à grande échelle de données sensibles (ex. : données de santé) ou de données personnelles relatives à des condamnations pénales et à des infractions ;
- La désignation du DPD s'effectue au niveau du Responsable de Traitement (ie : la structure dotée de la personnalité juridique) et non de chaque établissement ou service (lorsque celui-ci n'est pas doté de la personnalité juridique).

Par exemple l'association A gère 3 IME, 1 ESAT et 4 EHPAD. La responsabilité est recherchée au niveau de la personne morale (l'association A) - elle est incarnée par le dirigeant élu de cette association (Président(e)) et, possiblement par délégation par le dirigeant salarié (Directeur(trice) général(e). Un DPD unique est désigné au niveau de l'association A.

- **Les missions du DPD**
  - Informer et conseiller ;
  - Contrôler la conformité ;
  - Former et sensibiliser ;
  - Être le point de contact avec la CNIL et coopérer avec elle ;
  - Aider à la réalisation des analyses d'impact relatives à la protection des données prévues par l'article 35 du RGPD ;
  - Analyser les risques liés aux opérations de traitement ;
  - Tenir le registre des activités de traitement (même si cette mission incombe au Responsable de Traitement, elle est souvent, dans les faits, assumée par le DPD).
- **Les qualités et compétences attendues d'un DPD**

Le DPD doit posséder :

- de bonnes connaissances juridiques en matière du droit des données ;
- de bonnes connaissances des Systèmes d'information et des technologies qui y sont liées ;
- de bonnes connaissances des métiers et des besoins de la structure ;
- de bonnes qualités relationnelles.

De surcroît des connaissances en matière de gestion des risques ou de management de la qualité constituent des atouts supplémentaires.

Trois formules pour le DPD

Le DPD peut être :

- **interne** : désigné parmi les membres du personnel de la structure ;
- **externe** : désigné sur la base d'un contrat de service ;
- **mutualisé** : désigné par un groupe d'acteurs responsables de traitement, la seule condition étant qu'il puisse facilement être joignable depuis chaque établissement. Exemple : soit 3 associations A, B et C, l'association B dispose d'une compétence DPD en interne, elle met ce DPD à disposition des 2 autres.

Pourquoi envisager d'externaliser ou de mutualiser la fonction DPD ?

Plusieurs raisons peuvent conduire à envisager l'externalisation ou la mutualisation :

- Aucun professionnel de la structure n'est disponible ou ne présente les compétences attendues ;
- Il existe un risque de conflit d'intérêts (la personne pressentie détermine les finalités et les moyens des traitements, la personne pressentie est membre de l'encadrement supérieur de la structure) ;
- La quotité de temps requise par la mission est trop faible pour être compatible avec l'organisation des services.

Avantages et inconvénients de désigner un DPD hors de l'organisation

- **Avantages :**
  - Répondre rapidement à l'obligation de désigner un DPD ;
  - Disposer rapidement des compétences d'une ressource non disponible dans la structure ;
  - Éviter d'avoir à modifier l'organigramme de la structure pour y intégrer le DPD généralement pour un temps très partiel (0,25 à 0,50 ETP) ;
  - Éliminer le risque de conflit d'intérêts (à nuancer tout de même dans le cas de la mutualisation) ;
  - Disposer d'un point de vue extérieur.
- **Inconvénients :**
  - Le coût de la prestation peut être élevé ;
  - Il peut être difficile de trouver un prestataire réunissant les qualités attendues ;
  - Il peut être difficile pour le prestataire de s'approprier les spécificités de l'activité de la structure.

Précautions à prendre

- **Cas de la mutualisation**

- Les précautions à prendre sont les mêmes que pour tout projet de coopération-mutualisation :
  - bien définir la finalité,
  - garantir les mêmes droits pour chaque structure,
  - opérer des choix concertés,
  - clarifier les rôles et les responsabilités de chacun,
  - construire une représentation commune (ici en matière de protection des données personnelles),
  - prévenir et maîtriser les risques (notamment en cas d'interruption de la mutualisation),
  - s'accorder sur la répartition des coûts ;
- Éliminer le risque de conflit d'intérêts : le DPD mutualisé ne peut pas être concepteur ou décisionnaire de traitement de données pour une quelconque des structures (ce ne peut pas, par exemple, être un cadre dirigeant). Il ne peut pas non plus être en situation de sous-traitant. Un prestataire informatique assurant, par exemple, l'hébergement des données d'une des structures et à ce titre considéré comme sous-traitant (RGPD art. 4 8) ne peut pas être désigné DPD dans le cadre d'un contrat de service.

- **Cas de l'externalisation**
  - Définir un **cahier des charges** fixant notamment le périmètre de la mission et passer un appel d'offres ;
  - Éliminer le risque de **conflit d'intérêts** : par exemple l'avocat d'affaires de la structure peut difficilement être son DPD, même remarque pour un prestataire informatique chargé de l'hébergement par exemple ;
  - Appréhender le **coût de la mission** : celui-ci peut être élevé notamment si le prestataire se voit confier des tâches qui ne relèvent pas strictement des missions statutaires du DPD, mais qui, dans les faits, lui sont souvent confiées : la tenue du registre des activités de traitement, la réalisation et la validation des analyses d'impact, la tenue de la documentation permettant au Responsable de Traitement de démontrer la conformité, la réception des plaintes et des réclamations des personnes concernées ;
  - Fixer le **périmètre** de la mission :
    - informer et conseiller,
    - informer sur les manquements constatés et conseiller sur les mesures à prendre,
    - documenter la conformité dans le cadre de l'obligation de rendre compte (principe d'« accountability »),
    - veiller à l'application du principe de protection des données dès la conception d'un traitement,
    - auditer et contrôler régulièrement le respect de la réglementation,
    - piloter la production et la mise en œuvre de politiques, de lignes directrices, de procédures et de règles de contrôle,
    - gérer les demandes d'exercice de droits, de réclamations et de requêtes formulées par des personnes concernées par les traitements de la structure,
    - être l'interlocuteur privilégié de la CNIL et coopérer avec elle,
    - dispenser des conseils en ce qui concerne les analyses d'impact,
    - mettre la structure en position de notifier d'éventuelles violations de données auprès de la CNIL et conseiller le Responsable de Traitement,
    - s'assurer que l'inventaire des traitements est tenu et documenter les traitements de données à caractère personnel,
    - gérer la fin de la mission et réaliser le relais avec le successeur.
  - Le périmètre de la mission est large et, pour des raisons d'efficacité et de coût, les tâches et responsabilités doivent être réparties entre le prestataire et un (ou plusieurs) **correspondant en interne**. L'externalisation ne se conçoit pas comme une prestation « tout compris » et/ou « clés en main » ;
  - Acter l'obligation de **secret professionnel** pour le prestataire et ses intervenants ;
  - Vérifier les **compétences** du prestataire et de ses intervenants. La CNIL a mis en place des référentiels de certification du DPO[4]. La certification ne peut être délivrée que par un organisme agréé par la CNIL (voir le site de la CNIL[5]) ;
  - Signer une **charte de déontologie**[6] **;**
  - Identifier les **éléments clés** du contrat de service :
    - le périmètre de la mission,
    - la coordination entre le prestataire et les ressources internes affectées à la protection des données à caractère personnel,
    - les livrables attendus,
    - le coût de la mission,
    - les compétences du prestataire et de ses intervenants,
    - la disponibilité du prestataire et de ses intervenants[7],
    - l'organisation de la fin de mission.

Arbre de décision

Le processus conduisant à la désignation d'un DPD peut être formalisé en arbre de décision (cf. Figure 1). Selon ce schéma, le Responsable de Traitement :

1. Recherche la possibilité de désigner un DPD en interne ;
2. Envisage la mutualisation dans le cas où l'hypothèse 1) n'est pas envisageable ;
3. Envisage l'externalisation dans le cas où l'hypothèse 2) n'est pas réalisable ;
4. Si aucune des 3 hypothèses ne se révèle opérante il faut revenir au point de départ sachant que la désignation d'un DPD est obligatoire et, le cas échéant, réexaminer les éléments pour parvenir à une solution, fût-ce en mode dégradé.

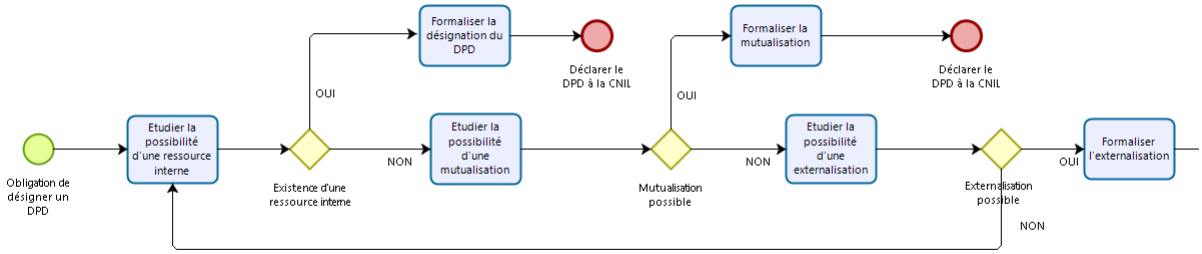

Figure 1- arbre de décision

Conclusion

L'externalisation peut constituer, avec la mutualisation, un moyen intéressant pour satisfaire aux obligations posées par le RGPD. Cette perspective nécessite d'être étudiée et mise en œuvre avec soin, notamment du point de vue de la sélection du prestataire.

1. Un avis de la Commission d'enrichissement de la langue française publié au JORF n° 0202 du 31 août 2019 prescrit d'utiliser la forme déléguée à la protection des données (DPD) comme équivalent de data protection officer (DPO). https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000039002295&dateTexte=&categorieLien=id?
2. Avis d'expert : En tant que structure médico-sociale, suis-je concerné par le RGPD ??
3. Le RGPD renvoie au droit national la définition des notions d' « autorité publique » ou d' « organisme public ». Toutefois les lignes directrices du CEPD (WP 243rev01 2.1.1) et la directive européenne 2003/98/CE (art. 2 2) c)) englobent dans ces catégories les organismes « dont soit l'activité est financée majoritairement par l'État, les collectivités territoriales ou d'autres organismes de droit public, soit la gestion est soumise à un contrôle par ces derniers » ce qui, par extension, concernerait la plus grande partie des organismes gestionnaires du secteur médico-social.?
4. https://www.cnil.fr/fr/certification-des-competences-du-dpo-la-cnil-adopte-deux-referentiels]?
5. https://www.cnil.fr/fr/organisme-agrees?
6. Par exemple, celle de l'AFCPD (Association française des correspondants aux données personnelles) https://afcdp.net/charte-de-deontologie-du-dpo/?
7. Par exemple, en cas de violation de données constatée le délai de prévenance de la CNIL est de 72 heures calendaires.?

Ressources associées

PERSONNE RESSOURCE
Etienne MAUGET

PERSONNE RESSOURCE
Gilles HERENGT

PERSONNE RESSOURCE
Elise MORICHON

Glossaire

ANAP
CNIL
DPD
ETP
EHPAD
externalisation
IME
mutualisation
personne
processus
ressource
RGPD
risque