STATUT, POSITIONNEMENT, ET MOYENS
D'UN.E DÉLÉGUÉ.E A LA PROTECTION DES DONNÉES (DPO) DANS L'ESR

Synthèse :

Du fait du nombre important de nouveaux traitements mis en œuvre et de données traitées, relevant des activités d'enseignement et de recherche des établissements de l'ESR, il est recommandé de **privilégier un DPO interne à l'organisme**, afin de suivre au plus près la mise en œuvre des traitements.

Une politique de site sur la protection des données mutualisée entre plusieurs établissements peut utilement être mise en place ; dans cette hypothèse, elle pourrait s'appuyer sur une **collaboration entre les DPO des différents établissements, ou un DPO mutualisé** à plusieurs établissements disposant *a minima* de relais au sein de chaque organisme.

Pour lui permettre d'exercer ses missions de manière optimale, il est nécessaire que le DPO soit **appuyé par une politique d'établissement, et dispose d'un accès direct au plus haut niveau** de l'organisme.

Le choix du délégué est certainement l'une des plus importantes décisions que l'établissement aura à prendre pour assurer la conformité de son établissement au Règlement général sur la protection des données (RGPD)[1], dès lors que le DPO a notamment pour mission de conseiller le responsable des traitements, informer les employés, contrôler les directions métiers et être le point de contact tant de l'autorité de contrôle que des personnes dont les données sont traitées.

Il doit également être associé à toutes les questions portant sur la protection des données, et est ainsi effectivement « *au cœur du nouveau cadre juridique* »[2]. Son rôle est nécessairement transversal, dans un environnement numérique généralisé. Le profil retenu, les moyens qui lui sont accordés et son positionnement sont donc des éléments importants de la stratégie de l'établissement ; ils doivent être adaptés aux spécificités de celui-ci, tel que son champ disciplinaire dominant, sa culture interne, sa taille, ou son niveau de maturité en termes de protection des données.

On rappelle à toutes fins utiles que le rôle du DPO est **d'accompagner** la démarche de conformité au RGPD **menée par l'établissement** « responsable des traitements » de données personnelles, réalisés dans le cadre de ses missions de service public.

[1] RGPD : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679
[2] *Guidelines* 16/FR – WP 243 rev.01 https://www.cnil.fr/sites/default/files/atoms/files/wp243rev01_fr.pdf

- **Statut :**

Le DPO peut être interne à l'organisme, mutualisé avec d'autres (au sein d'un groupe d'entreprises ou, pour une autorité ou un organisme public, auprès de plusieurs autorités ou organismes de ce type, « *compte tenu de leur structure organisationnelle et de leur taille* »)[3], ou encore externe.

Dans tous les cas, les caractéristiques de l'organisme (nombre d'étudiants, d'enseignants-chercheurs, de laboratoires,…), ses particularités (composantes de santé, sciences humaines et sociales, ZRR,…) sont nécessairement à prendre en compte dans cette première décision :

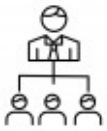
- **un DPO interne** pourra être soit administratif, soit enseignant-chercheur : le choix d'un personnel administratif -AENES ou ITRF- est le plus fréquent[4], et permet un dialogue naturel avec les directions fonctionnelles et opérationnelles.

  Toutefois, dans le cas où la mise en conformité au RGPD nécessiterait un chantier particulièrement important, par exemple pour un organisme à fort effectifs, ou qui ne dispose pas d'un premier niveau institutionnel de « maturité CNIL » -i.e. s'il n'avait pas désigné de CIL-, le portage par un enseignant-chercheur, plus apte à pouvoir dialoguer avec le pouvoir exécutif et la communauté scientifique et académique, pourrait être retenu.

  Le type de contrat par lequel est recruté un DPO doit aussi faire l'objet d'une attention particulière : ainsi, le CEPD[5] considère qu'un contrat court ou un CDD est à éviter. Un contrat lié à la durée de mandat du responsable des traitements est également à éviter.

- **un DPO mutualisé** (également administratif ou enseignant-chercheur) est une solution qui pourra permettre de coordonner une politique de site pour plusieurs établissements, ou de mettre en place une organisation régionale.

  Cette solution ne doit en revanche pas viser à réaliser des économies d'échelles, dès lors que la charge correspondante pourra nécessiter la constitution d'un réseau de relais auprès de chacun des organismes pour lesquels le DPO est mutualisé.



  Un DPO peut également être mutualisé avec des unités de recherche, considérant que celles-ci peuvent être « responsable de traitement »[6].

- **un DPO externe**, recruté par contrat de service, peut également être désigné, pour une ou plusieurs structures. Il pourra s'agir soit d'une personne physique, soit d'une personne morale -dans cette hypothèse, une personne devrait être plus particulièrement identifiée au sein de "l'organisme DPO", comme contact de l'établissement-.

  Le recours à un DPO externe n'exonère pas le responsable de traitement de ses responsabilités, ni ne le prémunit des risques de sanctions administratives.

  L'opportunité de recourir à un DPO externe pourrait notamment être estimée au regard :

[3] RGPD, art. 37-3
[4] 76% de CIL de l'ESR étaient BIATSS en 2017, cf. https://reseau.supdpo.fr/publications/
[5] https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_fr
[6] doctrine de la CNIL établie par courriers des 26 juin 2012 et 2 février 2016 ; courrier de la CPU aux unités du 4 septembre 2017

- de sa connaissance du secteur d'activité, qui fait intervenir différents statuts, diverses formes d'organisations et de structures, et des règles de fonctionnement particulières ;

- de sa capacité à dialoguer avec les différents acteurs (DGS, DSI, RSSI, DAJ, FSD,…) et de mettre en place une organisation efficace au sein de la structure;

- du nombre de sollicitations qui sont susceptibles d'intervenir, donc de la fréquence de mise en œuvre de nouveaux traitements : dans le cas, par exemple, d'un nombre important de collectes de données (mémoires, thèses, recherches,…), il paraît préférable de privilégier le recrutement d'un DPO interne, dont le coût chargé sera inférieur à celui d'une prestation externe -laquelle devra par ailleurs faire l'objet d'une mise en concurrence- et qui pourra suivre, au quotidien, la mise en œuvre de ses recommandations.

• Positionnement :

Les lignes directrices du G29, groupe des autorités de contrôle européennes, considèrent que *"les délégués à la protection des données (DPD) seront au cœur de ce nouveau cadre juridique pour de nombreux organismes, pour faciliter la conformité avec les dispositions du RGPD* »[7]

Ce rôle central doit être assuré par un DPO mis en capacité de dialoguer avec les personnes concernées par les traitements, avec la CNIL, ainsi que, en interne, de donner des recommandations aux différentes directions support et aux personnes chargées de la mise en œuvre des traitements.

Le DPO doit donc disposer d'un rattachement lui assurant une visibilité suffisante pour connaître des traitements envisagés et mis en œuvre, une légitimité lui permettant d'intervenir auprès de l'ensemble de la communauté, et un accès aisé au responsable des traitements[8].

Il est recommandé d'être rattaché fonctionnellement à un membre de l'équipe de gouvernance, soit politique (idéalement le Président, ou un vice-Président), soit administrative (le Directeur général des services, par exemple).

Son positionnement central et transversal dans les opérations de conformité, ainsi que sa responsabilité et sa forte exposition -on rappellera que le niveau de sanctions administratives a été réhaussé par le RGPD à 20 M€[9], et que les notifications de violations de données doivent mentionner nom et coordonnées du DPO[10]- devraient également impacter son niveau de rémunération[11][12], le cas échéant par le régime indemnitaire. Cet élément contribuera également à assurer la légitimité du DPO dans l'organisme.

Considérant qu'il peut par ailleurs exercer d'autres fonctions, il peut également, par facilité d'organisation, être hiérarchiquement rattaché à une direction ou à un service. Dans ce cas, il convient de veiller à ce que son indépendance soit respectée[13], -cf. exemple du CEPD

[7] *Guidelines* 16/FR – WP 243 rev.01
[8] RGPD, art. 38.3 : "*le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable*"
[9] RGPD, art. 83.5
[10] RGPD, art. 34.2
[11] https://www.usine-digitale.fr/article/en-2018-le-poste-le-plusen-vue-sera-le-data-protection-officer.N641043
[12] https://www.cadremploi.fr/editorial/actualites/actu-emploi/detail/article/le-rgpd-va-t-ilvraiment-creer-des-postes-cadres-a-75-000-euros.html
[13] RGPD, art. 38.3 : "*Le responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données ne reçoive aucune instruction en ce qui concerne l'exercice des missions*"

: qu'il n'ait pas de compte à rendre à son supérieur hiérarchique[14]- et qu'il ne soit pas en situation de conflit d'intérêt[15].

Certaines fonctions sont citées comme pouvant constituer un tel risque de conflit d'intérêt, et, sous réserve d'un examen au cas par cas, ne devraient ainsi pas pouvoir être cumulées avec la fonction de DPO[16] : directeur général, directeur financier, directeur des ressources humaines, directeur des systèmes d'information.

Fonctionnellement, le DPO du fait de ses missions peut être considéré comme membre à part entière de certains services (juridique, informatique, de documentation,…) et notamment convié aux réunions de service de ces entités.

- **Moyens :**

Le responsable des traitements doit aider le délégué à exercer ses missions par trois axes explicitement cités par le RGPD[17] :

- en lui fournissant les ressources et l'appui collaboratif des services nécessaires pour exercer ses missions (réseau de proximité dans les directions et centres de recherche, comité d'experts de différentes directions participant à la protection des données).

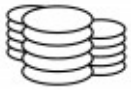
  Le soutien actif, visible et effectif, expression d'une véritable politique d'établissement, pourra être dans certains cas être une ressource suffisante.

  Elle s'exprimera alors, par exemple[18], par un temps de travail suffisant, des moyens logistiques ou en personnels -par exemple un adjoint, notamment dans le cas de structures très importantes, à disciplines sensibles, ou situées sur plusieurs sites-, une lettre de mission, des réunions régulières avec le Directeur général,...

  Ce soutien permettra aussi de s'assurer que le DPO est mis en capacité de remplir ses missions[19], et qu'il n'est pas pénalisé[20] pour l'exercice de ses missions.

  Dans le cas où un budget est attribué au DPO, le CEPD recommande qu'il soit seul responsable de l'utilisation dudit budget[21].

- en lui fournissant l'accès aux données et aux opérations de traitement;



- en lui permettant d'entretenir ses connaissances spécialisées.

  Cela implique de lui permettre de bénéficier de formations spécialisées, d'assister à des manifestations spécialisées (séminaires, conférences, journées d'études,…) ou de participer à des associations professionnelles.

[14] https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_fr
[15] RGPD, art. 38.6 : "*Le responsable du traitement ou le sous-traitant veillent à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts*"
[16] *Guidelines* 16/FR – WP 243 rev.01
[17] RGPD, art. 38.2
[18] *Guidelines* 16/FR – WP 243 rev.01
[19] RGPD, art. 38 : " *Le responsable du traitement et le sous-traitant veillent à ce que le délégué (...) soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données*"
[20] RGPD, art. 38.3 : "*le délégué (...) ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions*"
[21] https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_fr