DÉLÉGUÉ À LA PROTECTION DES DONNÉES PERSONNELLES (DPD)

Délégué à la protection des données personnelles (DPD) - SACC - Commissaire aux comptes nommé DPD d'une entité dont il certifie les comptes (non) – Commissaire aux comptes nommé DPD pour les entités de la chaîne de contrôle de l'entité auditée (non) – Mission de diagnostic de conformité au RGPD avec formulation de recommandations (possible sous réserve que les travaux ne conduisent pas le commissaire aux comptes ou son réseau à réaliser une consultation juridique).

(CEP 2018-13)

Questions :
Le commissaire aux comptes peut-il être nommé délégué à la protection des données personnelles (DPD) par l'entité dont il certifie les comptes ? Peut-il être nommé DPD pour les entités de la chaîne de contrôle de l'entité dont il certifie les comptes ? Peut-il faire des missions de diagnostics de conformité au RGPD avec formulation de recommandations ?

***
*

La Commission d'éthique professionnelle, qui s'est prononcée avant la publication de la loi n° 2019-486 du 22 mai 2019, dite « loi PACTE », souligne en premier lieu qu'il est clair qu'un commissaire aux comptes peut démontrer qu'il a les qualités professionnelles et les connaissances juridiques pour remplir le rôle de délégué à la protection des données personnelles (DPD), et de plus, qu'il exerce son mandat de commissaire aux comptes en toute indépendance et sans conflit d'intérêts. Pour autant, il apparait que les caractéristiques de la mission de DPD la rendent incompatible avec un mandat de commissariat aux comptes.

La Commission rappelle que les articles 10 et 10-1 du code de déontologie (en annexe) interdisent au commissaire aux comptes d'une entité de réaliser au profit de cette entité, des entités qui la contrôlent ou qui sont contrôlées par elle, qu'elle soit entité d'intérêt public (EIP) ou non :

- des services qui supposent d'être associé à la gestion ou à la prise de décision de l'entité contrôlée,
- des prestations de conseil en matière juridique,
- des services juridiques incluant la négociation au nom de l'entité contrôlée ou la défense de l'entité contrôlée,
- la prise en charge même partielle d'une prestation d'externalisation.

Ces interdictions qui s'appliquent au commissaire aux comptes s'appliquent également aux membres de son réseau pour les services à rendre à l'entité dont les comptes sont certifiés (entités EIP et non EIP), et pour les entités EIP, aux sociétés françaises les contrôlant ou contrôlées par elles.

1/ Le DPD et les prestations de conseil en matière juridique et d'externalisation

L'article 37, paragraphe 5, du RGPD prévoit que le DPD « est 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 les missions visées à l'article 39 ».

La Commission constate que les principales missions du DPD sont des missions de conseil en matière juridique :

- mission générale d'information et de conseil auprès de l'entreprise sur ses obligations en matière de protection des données ;
- mission de contrôle du respect du RGPD et des autres dispositions applicables en matière de protection des données.

En pratique, même s'il n'existe pas de profil type du DPD, qui peut être une personne issue du domaine technique, juridique ou autre, il apparait que le choix par l'entreprise d'un DPD ayant des compétences juridiques est recommandé, en particulier, compte tenu de l'importance du volet juridique (décryptage et explicitation du droit applicable, conseil sur la mise en œuvre de la réglementation en conformité avec le règlement), et parce qu'il est l'interlocuteur de l'autorité de contrôle (en France, la CNIL), dans le cadre de consultations techniques ou de coopération avec elle. Ce rôle d'interlocuteur principal de l'autorité de contrôle, au nom de l'entreprise, tel que prévu aux articles d) et e) de l'article 39 met en évidence la fonction de représentation du DPD et la prise en charge d'une fonction de l'entreprise, même partielle par le DPD, prestataire externe.

2/ Le DPD rapporte à la gouvernance de l'entreprise en ce qui concerne le respect de cette réglementation

La Commission d'éthique professionnelle observe que le DPD est le chef d'orchestre de la conformité en matière de protection des données personnelles.

Il est notamment chargé :

- de mettre en œuvre les mesures techniques et organisationnelles pour s'assurer et être en mesure de démontrer que les traitements effectués par l'entreprise le sont conformément au RGPD ; du recensement des traitements à grande échelle réalisés par l'entreprise, de leur justification, de leur durée de conservation, de l'établissement et, en pratique, de la tenue du « registre de traitement des données » ;
- de l'évaluation des pratiques de l'entreprise et la mise en place de procédures pour la mise en conformité avec le règlement,
- de l'identification des risques associés aux opérations de traitement (analyses d'impact),
- de la proposition de stratégies ou mesures pour réduire les risques,
- de l'établissement et la communication d'une politique de protection des données personnelles au sein de l'entreprise.

Il exerce un rôle opérationnel au sein de l'entreprise.

3/ Le DPD doit agir en toute confidentialité et a une obligation de secret professionnel

La Commission d'éthique professionnelle constate que le DPD a une obligation de secret professionnel (article 38-5 du RGPD en annexe). Cependant, celle-ci est levée vis-à-vis de l'autorité de contrôle. Ces interactions avec l'autorité de contrôle pourraient l'amener à présenter des situations, communiquer des informations de l'entreprise, qu'un commissaire aux comptes ne pourrait pas diffuser. Le secret professionnel du commissaire aux comptes est absolu et ne peut être levé que par un texte législatif particulier, applicable au commissaire aux comptes, dans le cadre de sa mission de commissaire aux comptes. Le cumul des deux fonctions pourrait le conduire en tant que DPD à révéler des informations qui seraient couvertes par son obligation de secret professionnel en qualité de commissaire aux comptes.

4/ Le DPD ne doit pas exercer d'autres missions susceptibles de générer un conflit d'intérêts

La Commission d'éthique professionnelle constate que le DPD doit exercer ses missions en toute indépendance (article 38.3 du RGPD en annexe).

Plusieurs garanties lui permettent d'agir en toute indépendance :

- l'interdiction d'instruction sur ses missions de DPD de la part des entités l'ayant désigné comme DPD ;
- l'interdiction pour l'entité ayant désigné le DPD de le sanctionner pour l'exercice de ses missions.

Par ailleurs, l'article 38.6 du règlement européen n° 2016/679 lui interdit les situations de conflits d'intérêts avec ses autres missions et tâches.

La Commission d'éthique professionnelle relève qu'en pratique, l'interdiction de conflit d'intérêts du DPD avec ses autres missions et tâches signifie en particulier que le DPD ne peut exercer au sein de l'entité l'ayant désigné une fonction qui l'amènerait à déterminer les finalités et les moyens d'un traitement de données personnelles.

La Commission d'éthique professionnelle souligne que le commissaire aux comptes d'une entité met en œuvre, dans le cadre de ses missions (certification des comptes, services autres que la certification des comptes) des traitements de données personnelles. Il effectue ces traitements en qualité de responsable de traitement (cf. les travaux et clauses types publiées par le CNCC en matière de données personnelles) : le commissaire aux comptes est responsable de traitement distinct de l'entité auditée pour les traitements qu'il met en œuvre dans le cadre de sa mission, compte tenu de son obligation déontologique d'indépendance, de son degré d'expertise et d'autonomie élevé, du fait qu'il détermine les finalités et les moyens des traitements opérés en application de la législation et des normes professionnelles qui lui sont applicables.

Pour cette raison, la Commission d'éthique professionnelle considère qu'il peut être difficile d'être à la fois DPD d'une entité et de réaliser pour celle-ci ou des entités de sa chaîne de contrôle d'autres missions le conduisant à traiter dans le cadre d'une mission de certification des comptes ou de services autres que la certification des comptes, des données personnelles relevant de sa mission de DPD.

En conclusion, la Commission d'éthique professionnelle estime qu'un commissaire aux comptes ne peut pas accepter d'être nommé DPD :

- de l'entité dont les comptes sont certifiés (qu'elle soit EIP ou non EIP),
- des entités françaises et européennes la contrôlant, ou contrôlées par cette entité.

La Commission d'éthique professionnelle considère également que les membres du réseau du commissaire aux comptes ne peuvent pas être nommés DPD :

- de l'entité dont les comptes sont certifiés (qu'elle soit EIP ou non EIP),
- des entités françaises la contrôlant, ou contrôlées par cette entité lorsque l'entité auditée est EIP.

La nomination d'un membre du réseau en qualité de DPD d'une entité contrôlant ou contrôlée par l'entité auditée lorsque celle-ci est non EIP, ne parait pas strictement interdite par l'article 10-1.III du code de déontologie, mais requiert une analyse du respect des principes fondamentaux d'indépendance (article 5 du code de déontologie en annexe) et de l'article 38.6 du règlement européen (en annexe), qui conduisent généralement à considérer que ces missions ne peuvent être menées concomitamment.

En revanche, la Commission d'éthique professionnelle estime qu'une mission de diagnostic de conformité au RGPD, avec émission de recommandations générales, n'est pas interdite, à condition que les travaux ne conduisent pas à réaliser une consultation juridique qui serait interdite au commissaire aux comptes ou à son réseau dans les mêmes conditions que le mandat de DPD.

ANNEXE

Articles du code de déontologie :

Article 5 C. déontologie :

« *I. – Le commissaire aux comptes doit être indépendant de la personne ou de l'entité dont il est appelé à certifier les comptes. Cette exigence s'applique durant l'exercice contrôlé, la réalisation des travaux de contrôle des comptes et jusqu'à la date d'émission de son rapport.*
Toute personne qui serait en mesure d'influer directement ou indirectement sur le résultat de la mission de certification des comptes est soumise aux exigences d'indépendance mentionnées au précédent alinéa.
II. – L'indépendance du commissaire aux comptes s'apprécie en réalité et en apparence. Elle se caractérise par l'exercice en toute objectivité des pouvoirs et des compétences qui sont conférés par la loi. Elle garantit qu'il émet des conclusions exemptes de tout parti pris, conflit d'intérêts, risque d'autorévision ou influence liée à des liens personnels, financiers ou professionnels.
III. – Le commissaire aux comptes veille à ce que son indépendance ne soit pas compromise par un conflit d'intérêts, une relation d'affaires ou une relation directe ou indirecte, existante ou potentielle, entre ses associés, salariés ou toute autre personne qui serait en mesure d'influer directement ou indirectement sur la mission de certification, ainsi que les membres de son réseau, d'une part, et la personne ou l'entité dont il est chargé de certifier les comptes d'autre part.
IV. – Tant à l'occasion qu'en dehors de l'exercice de sa mission, le commissaire aux comptes évite de se placer dans une situation qui compromettrait son indépendance à l'égard de la personne ou de l'entité dont il est appelé à certifier les comptes ou qui pourrait être perçue comme de nature à compromettre l'exercice impartial de cette mission ».

Article 10 C. de déontologie :

« *Outre les services mentionnés au II de l'article L. 822-11, regardés comme portant atteinte à l'indépendance du commissaire aux comptes et comme tels interdits, sont également interdits dans les mêmes conditions :*
1° Les services ayant pour objet l'élaboration d'une information ou d'une communication financière ;
2° La prestation de conseil en matière juridique ainsi que les services qui ont pour objet la rédaction des actes ou la tenue du secrétariat juridique ;
3° Les missions de commissariat aux apports et à la fusion ;
4° La prise en charge, même partielle, d'une prestation d'externalisation ;
5° Le maniement ou le séquestre de fonds ».

Article 10-1 C. déontologie :

« *I. – Pour l'application du 1er alinéa du III de l'article L. 822-11, sont interdits les services mentionnés à l'article 10.*
II. – Pour l'application de la première phrase du second alinéa du III de l'article L. 822-11 sont interdits les services mentionnés à l'article 10.
III. – Pour l'application de la deuxième phrase du second alinéa du III de l'article L. 822-11, l'indépendance du commissaire aux comptes est affectée par la fourniture, par un membre de son réseau à la personne qui contrôle ou qui est contrôlée par la personne dont les comptes sont certifiés, de l'une des prestations suivantes :
1° Les services ayant pour objet la tenue de la comptabilité, la préparation et l'établissement des comptes et l'élaboration d'une information ou une communication financière, lorsqu'ils sont inclus dans les comptes consolidés soumis à la certification du commissaire aux comptes ;
2° La conception et la mise en œuvre de procédures de contrôle interne ou de gestion des risques relatives à l'élaboration ou au contrôle des informations comptables ou financières incluses dans les comptes consolidés soumis à la certification du commissaire aux comptes ;
3° Les services qui supposent d'être associé à la gestion ou à la prise de décision de l'entité dont les comptes sont certifiés ».

Article du règlement européen (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016

Article 37 du règlement européen (UE) n° 2016/679 :

« *1. Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque :*
a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;
b) 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 et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou

c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.
2. Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'un délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement.
3. Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille.
4. Dans les cas autres que ceux visés au paragraphe 1, le responsable du traitement ou le sous-traitant ou les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent désigner ou, si le droit de l'Union ou le droit d'un État membre l'exige, sont tenus de désigner un délégué à la protection des données. Le délégué à la protection des données peut agir pour ces associations et autres organismes représentant des responsables du traitement ou des sous-traitants.
5. Le délégué à la protection des données est 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 les missions visées à l'article 39.
6. Le 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.
7. Le responsable du traitement ou le sous-traitant publient les coordonnées du délégué à la protection des données et les communiquent à l'autorité de contrôle ».

Article 38 du règlement européen n° 2016/679 :

« *1. Le responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.*
2. Le responsable du traitement et le sous-traitant aident le délégué à la protection des données à exercer les missions visées à l'article 39 en fournissant les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées.
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. Le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions. Le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant.
4. 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 le présent règlement.
5. Le délégué à la protection des données est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions, conformément au droit de l'Union ou au droit des États membres.
6. Le délégué à la protection des données peut exécuter d'autres missions et tâches. Le responsable du traitement ou le sous-traitant veillent à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts ».

Article 39 du règlement européen n° 2016/679 :

« *1. Les missions du délégué à la protection des données sont au moins les suivantes:*
a) informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données;
b) contrôler le respect du présent règlement, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant 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;
c) 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 en vertu de l'article 35;
d) coopérer avec l'autorité de contrôle;
e) faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet.
2. Le délégué à la protection des données 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 ».