Du Correspondant informatique et libertés (CIL) au Délégué à la protection des données (DPD) : entre continuité et changements

BÉNÉDICTE FAUVARQUE-COSSON

Professeur à l'Université Panthéon-Assas, Paris 2

Codirectrice du diplôme d'Université « Délégué à la protection des données personnelles »

EMMANUEL JOUFFIN

Docteur en droit
Responsable juridique de banque

L'un des acteurs phares de la mise en conformité avec le règlement est le Délégué à la protection des données (*Data Protection Officer*). Héritier du Correspondant informatique et libertés, celui-ci voit sa fonction et ses missions en grande part définies par le règlement européen.

Le Règlement 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[1] (ci-après « RGPD ») a été publié au *Journal Officiel de l'Union européenne* le 4 mai 2016. Il s'appliquera à partir du 25 mai 2018 (article 99).

Selon ses propres termes, ce règlement pose, dans l'Union, un cadre de protection des données « *solide* » et « *cohérent* ». L'objectif est notamment de « *susciter la confiance qui permettra à l'économie numérique de se développer dans l'ensemble du marché intérieur* » (considérant 7).

La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental, protégé par la Charte des droits fondamentaux de l'Union européenne (art. 8, par. 1). Il en résulte que ce règlement « *devrait s'appliquer aux personnes physiques, indépendamment de leur nationalité ou de leur lieu de résidence, en ce qui concerne le traitement de leurs données à caractère personnel* » (considérant 14). En conséquence, un large champ territorial d'application est conféré au droit européen et le règlement s'applique aux établissements d'un responsable du traitement ou d'un sous-traitant établi sur le territoire de l'Union « *que le traitement ait lieu ou non dans l'Union* » (article 3.1). Il s'applique même en l'absence d'établissement du responsable du traitement ou du sous-traitant dans l'Union, le critère étant alors celui du ciblage par « *l'offre de biens ou de services* » dans l'Union ou par le suivi « *d'un comportement qui a lieu au sein de l'Union* » (article 3.2)[2].

Une période transitoire de deux ans a été prévue pour que les entreprises se mettent en conformité avec les nouvelles règles qui s'appliqueront à compter du 25 mai 2018. Compte tenu du vaste champ d'application du règlement, de la forte augmentation des obligations imposées aux responsables de traitement (notification des violations de données, réalisation d'études d'impact, tenue d'une documentation prouvant la mise en conformité, etc.) et du montant élevé des sanctions financières encourues en cas de violation du règlement, cette période transitoire n'est pas trop longue.

L'un des acteurs phares de la mise en conformité avec le règlement est le délégué à la protection des données (ci-après DPD) ou DPO, pour *Data Protection Officer*. Héritier du Correspondant informatique et

1. Règlement n° 2016-679 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 (règlement général sur la protection des données) du 27 avril 2016 JOUE du 4 mai 2016.

2. Sur les aspects internationaux et l'application extraterritoriale du règlement, v. F. Jault-Seseke, « Le règlement n° 2016-679 relatif aux données personnelles, Aspects de droit international privé », *Recueil Dalloz* 2016, p. 1874.

libertés, le délégué à la protection des données voit sa fonction et ses missions en grande part définies par le règlement.

DU CIL AU DPD : QUELS CHANGEMENTS ?

Tandis que dans la loi informatique et libertés, la nomination d'un CIL était optionnelle, le règlement rend obligatoire la présence d'un DPD dans les cas énumérés par l'article 37, paragraphes 1 à 3[3]. Cette obligation n'incombe pas qu'aux structures privées et le premier cas envisagé par l'article 37 est même celui du traitement « *effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle* »[4].

Les « *responsables de traitement* » sont les personnes physiques ou morales, de droit public ou privé, qui déterminent les finalités et moyens de traitement (article 4, paragraphe 7). Les structures dans lesquelles un Correspondant informatique et libertés (CIL) est déjà en place pourront confier ces nouvelles missions au DPD, tandis que les autres devront soit former un collaborateur, soit en recruter un ou s'attacher les services d'un professionnel externe[5].

L'article 37.5 indique simplement 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* ». D'après les *Guidelines* du G 29 sur les DPO, adoptées le 13 décembre 2016, le niveau d'expertise requis devrait être d'autant plus élevé que l'activité en question est complexe, que les données sont nombreuses ou qu'elles font l'objet de transferts internationaux[6].

LE DPD : QUELLE INDÉPENDANCE POUR QUELLES FONCTIONS ?

L'article 38 est relatif à la « *Fonction du délégué à la protection des données* ». Ce texte donne compétence au DPD pour « *toutes les questions relatives à la protection des données à caractère personnel* » (article 38-1). L'article 38 précise que le responsable du traitement et le sous-traitant fournissent au DPD « *les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement* »[7] ; ils doivent aussi lui permettre « *d'entretenir ses connaissances spécialisées* » (article 38-2).

L'indépendance du DPD est garantie par l'article 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. 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* ». On peut toutefois se demander ce qu'apportera de plus l'obligation d'indépendance consacrée par le règlement, le DPD étant déjà tenu, en vertu du droit du travail et même du droit commun des obligations, d'un devoir de loyauté dû envers son employeur (art. L. 1222-1 Code du travail ; v. aussi le nouvel article 1104 du Code civil, qui consacre de manière large le principe général de bonne foi).

Le règlement précise que le DPD doit pouvoir exprimer son opinion dissidente si les responsables du traitement ou le sous-traitant, responsables de la conformité au règlement, prennent des décisions incompatibles avec le respect du RGPD[8]. Cette disposition soulève diverses questions. Au lieu de chercher activement des solutions (même imparfaites) avec sa direction, un DPD pourrait-il simplement écrire un « *dissenting opinion* », se cachant derrière son « *indépendance* » ? Ce serait, à notre sens, trahir l'esprit du règlement qui impose au DPD un devoir d'assistance et de conseil envers le responsable de traitement. La possibilité pour le DPD d'exprimer son désaccord ne doit pas se transformer en solution de facilité pour le DPD et son employeur. Mais alors, quel risque le DPD prendra-t-il en exprimant son désaccord avec telle ou telle décision ? Tout dépend de ce que signifie précisément l'interdiction de relever de ses fonctions ou de pénaliser le DPD « *pour l'exercice de ses missions* ». Le DPD deviendrait-il un salarié protégé ? Les *Guidelines* précisent que le DPD pourrait certes être relevé de ses

3. Article 37 : « *Désignation du délégué à la protection des données*
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. »
Sur la notion d' « activités de base » (*core activities*), v. sur les *Guidelines* du G 29 sur les DPO, adoptées le 13 décembre 2016, 16/EN WP 243 (ci-après G 29 WP 243). »

4. Le règlement ne définit pas les termes « *autorité publique* » ou « *organisme public* », qui sont donc définis par chaque État membre. Les *Guidelines* mettent en exergue le fait que ce sont alors toutes les activités, et non seulement celles « *de base* » qui sont visées. Elles recommandent aux entreprises privées qui exercent une mission de nature publique de désigner un DPO pour toutes les activités, y compris celles non liées à cette mission (G 29 WP 243, 2.1.1).

5. Tandis que l'article 37 (1) du règlement définit les cas dans lesquels le responsable du traitement et le sous-traitant désignent « *en tout état de cause* » un délégué à la protection des données, l'article 37(4) vise quant à lui d'autres hypothèses, où cette nomination peut avoir lieu, ou même doit se faire (notamment si le droit d'un État membre l'exige).

6. G 29 WP 243, 2.4.

7. Sur la nécessité d'impliquer, au plus tôt, le DPD, v. G 29 WP 243, 3.1

8. G 29 WP 243, 3.3. Les *Guidelines* ne précisent pas quelle forme devrait prendre cette opinion dissidente.

fonctions, mais pour des raisons qui ne tiennent pas à l'exercice de ses fonctions, (par exemple en cas de vol ou harcèlement).

D'autres questions se posent encore. Si le DPD est autorisé à exécuter d'autres missions, celles-ci ne doivent pas entraîner de conflits d'intérêts (article 38.6). Le seul risque d'un conflit d'intérêts, en lien avec l'exigence d'indépendance du DPD, devrait donc l'empêcher d'exercer certaines fonctions ou missions au sein de l'entreprise[9]. Cependant, l'obligation d'indépendance ne crée-t-elle pas en elle-même un risque de conflit d'intérêts pour le DPD dont le devoir de loyauté s'exerce certes envers son employeur mais aussi envers l'autorité de contrôle qui peut lui ordonner de lui notifier les failles de sécurité (Art. 58.1 du RGPD) ? Cependant, là encore, le rôle du DPD est d'assister son employeur, le responsable du traitement, et non de se substituer à lui dans la notification des violations.

Rattaché au plus haut niveau hiérarchique, le DPD, détenteur d'une expertise attestée 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* » (article 38.5). Dès lors, le DPD peut-il, et doit-il, dénoncer les violations dont il est témoin ?

LE DPD : ACTEUR D'UNE APPROCHE PAR LES RISQUES ET DÉTENTEUR D'UNE MISSION STRATÉGIQUE AU SEIN DE L'ENTREPRISE

L'article 39 est relatif aux « *Missions du délégué à la protection des données* ». Un socle commun est posé. Ces missions sont énumérées de manière non limitative et d'autres peuvent s'y ajouter, dans le respect de l'article 38.6 (absence de conflits d'intérêts).

Tandis que la loi informatique et libertés reposait sur un régime de déclaration/autorisation, le règlement innove en introduisant une logique de responsabilisation et d'autoévaluation pour le responsable de traitement. L'analyse des risques pour la protection des données est au cœur du métier du DPD (art. 39.2). Les *Guidelines* du G29 soulignent ainsi que le DPD est le maître d'œuvre d'une « *approche par les risques* »[10] et qu'il doit adopter une approche « *sélective* » et « *pragmatique* », qui le conduit à traiter prioritairement des questions qui présentent les risques les plus élevés en matière de protection des données.

Au-delà de son rôle de conseiller du responsable du traitement, du sous-traitant, des employés et plus généralement de toutes les « *personnes concernées* » qui peuvent prendre contact avec lui (art. 38.4), le délégué à la protection des données contrôle le respect du droit de l'Union et du droit des États, « *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* » (article 39-1-b).

En tant que conseiller de la direction, le rôle du DPD est assez proche de celui du directeur juridique. Il est également proche du directeur de la conformité (*Chief Compliance Officer*). Comme lui, il identifie, évalue, et contrôle le risque de non-conformité de l'établissement, à cette différence près qu'il est tenu d'intervenir au plus tôt, dans l'élaboration de nouveaux produits et services (*privacy by design*). Par conséquent, il doit être associé « *en temps utile* » à toutes les questions de protection des données personnelles et être de ce fait informé d'un traitement portant sur les données personnelles, avant sa mise en œuvre.

Le DPD aura donc toute sa place dans les comités de pilotage de la mise en œuvre de grands projets impliquant le traitement de données et devra assurer la réalisation des études d'impact (*Privacy Impact Assessments*), obligatoires pour tout projet à risque.

Par sa contribution à la mise en œuvre des éléments essentiels du RGPD, tels que les principes relatifs au traitement des données[11], la protection des droits des personnes concernées[12], la « *privacy by design* » et « *by default* »[13], l'enregistrement des traitements[14], la sécurité de ces derniers[15], et la notification des violations[16], le DPD exercera un rôle essentiel dans la promotion d'une culture de la protection des données au sein de l'entreprise. Il lui incombera de développer et piloter la stratégie de gouvernance de l'entreprise en matière de données. Pour cela, le DPD aura besoin du soutien d'un réseau de personnes sensibilisées aux risques, qui relaieront sa mission au sein des directions, notamment juridique, informatique et des ressources humaines. Les défis sont nombreux, à commencer par celui-ci : gagner la confiance des différentes directions au sein de l'entreprise et convaincre chacun que la protection des données personnelles est non seulement une contrainte mais un objectif à poursuivre dans l'intérêt de tous, y compris de l'entreprise. Un nouveau métier, qui nécessite de multiples compétences, est apparu[17].

9. Pour plus de précisions, v. *Guidelines* préc., par. 3.5.

10. G 29 WP 243, 4.3. « *Risk-based approach* », p. 17.

11. Chapitre II du RGPD.
12. Chapitre III du RGPD.
13. Art. 25 du RGPD.
14. Art. 30 du RGPD.
15. Art. 32 du RGPD. Cf., dans ce même numéro, C. Boutonnet, « La sécurité des données », p. 52.
16. Art. 33 et 34 du RGPD.
17. Pour répondre aux besoins de formation des DPD, l'Université Panthéon-Assas, Paris 2 vient de créer un diplôme d'université dont l'objectif est de permettre aux professionnels d'assumer pleinement ces nouvelles fonctions.

I. COMPARAISON CIL V/S DPD (PAR EMMANUEL JOUFFIN)

	CIL	DPD
Rattachement hiérarchique	Il « *ne reçoit aucune instruction pour l'exercice de sa mission* » ; art. 46, al. 2, du décret n° 2007-451 du 25 mars 2007 modifiant le décret n° 2005-1309 du 20 octobre 2005[18]. Pas de précision sur le niveau de rattachement.	Art. 38-3 du RGPD : le DPD ne doit rendre des comptes qu'« *au niveau le plus élevé de la direction du Responsable du traitement ou du sous-traitant* » et ne doit recevoir « *aucune instruction en ce qui concerne l'exercice de ses missions* »[19]. *Idem*, art. 45-3 de la proposition de « *règlement traitement par les institutions européennes* »[20] : le DPD fait directement rapport au niveau de gestion le plus élevé.
DPD interne (Groupe) ou externe	Fiche 7 du guide CIL[21] s'agissant du CIL externe.	Art. 37-2 du RGPD : 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[22]. Art. 37-6 du RGPD : le DPD 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[23].
Informations relatives à la prise de fonctions du DPD	Art. 45 du décret de 2005 : la désignation d'un CIL est, préalablement à sa notification à la CNIL, portée à la connaissance de l'instance représentative du personnel compétente par le responsable des traitements, par lettre remise contre signature. Fiche 8 du guide CIL 2011 de la CNIL.	Art. 37 du RGPD : 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[24].
Exercice d'autres fonctions – Conflit d'intérêts	Art. 46, al. 4, du décret n° 2007-451. Les fonctions ou activités exercées concurremment par le correspondant ne doivent pas être susceptibles de provoquer un conflit d'intérêts avec l'exercice de sa mission. Fiche n° 4 § 1 du Guide CIL 2011 de la CNIL.	Art. 38 -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* ». Pour le G29[25], la nomination d'un DPD à temps partiel est acceptable, mais avec une attention particulière portée aux risques de conflit d'intérêts[26] et aux ressources nécessaires. Le G29 suggère quelques bonnes pratiques : – établir un pourcentage de temps dévolu à la fonction de DPD ; – assurer un accès direct du DPD aux plus hautes instances de l'entreprise[27] ; – assurer un soutien efficace du DPD en termes financiers, de moyens matériels et humains ; – communiquer la désignation du DPD auprès du personnel ; – assurer l'accès aux fonctions supports (IT, RH, juridique…) ; – assurer la formation permanente du DPD afin de maintenir une expertise continue ; – inclure le DPD précocement dans toutes les activités relatives à la protection des données[28] ; – établir un énoncé de mission clair et transparent ; – création d'un corps de règles (liste des fonctions incompatibles, règles internes en matière de conflits d'intérêts…)[29] ; – établir des rapports annuels.

18. Tel que modifié par le décret n° 2007-451 du 25 mars 2007.

19. § 3.1. et 3.3., *Guidelines on Data Protection Officer* WP 243 adoptées le 13 décembre 2016.

20. *Proposal for a regulation ot the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation* (EC) No 45/2001 and Decision No 1247/2002/EC, 2017/0002 (COD), 10 janvier 2017. Bien que le périmètre de ce réglement soit restreint, il n'en comporte pas moins des éléments illustratifs intéressants. Ce texte est distinct de la proposition de règlement *e-privacy* (*Proposal for a regulation ot the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal data in Electronic Communications and Repealing Directive* 2002/58/EC (*Regulation on Privacy and Electronic Communications*, également du 10 janvier).

21. Guide du correspondant informatique et libertés, 2011 : https ://www.cnil.fr/sites/default/files/typo/document/CNIL_Guide_correspondants.pdf

22. Cf. G 29 *Guidelines on Data Protection Officer* (« DPOs ») WP 243, adoptées le 13 décembre 2016, spéc. p. 10 § 2.3. Le G29 souligne que la disponibilité du DPD, soit physiquement, soit par une hotline ou tout autre moyen de communication sécurisé, est essentielle. *Idem* art. 44 de la proposition de règlement traitement par les institutions européennes.

23. *Idem*, article 44-4 de la proposition de règlement traitement par les institutions européennes.

24. Cf. Art. 44- 5 de la proposition de règlement traitement par les institutions européennes : publicité des coordonnées du DPD et communication au contrôleur européen de la protection des données.

25. G 29 *Guidelines* WP 243, spéc. § 3.2 et § 3.5.

26. Art. 45-6 de la proposition de règlement traitement par les institutions européennes : le DPD peut remplir d'autres « *tâches et devoirs* », sous réserve de l'absence de conflit d'intérêts.

27. Le G29 vise le « *board level* ».

28. *Ibid.* § 3 « *Position of the DPO* ».

29. *Ibid.* § 3.5 « *conflict of interests* ».

	CIL	DPD
Désignation du responsable de traitement en tant que DPD – Responsabilité	Art. 46, al. 3, du décret de 2005 précise que le responsable, ou son représentant légal, ne peut pas être désigné comme CIL. Pour la CNIL, une personne participant aux décisions relatives aux traitements relevant du périmètre du CIL ne peut occuper cette fonction - Fiche n° 4 § 1 du Guide CIL 2011 de la CNIL § 3. Le Cil doit être protégé de tout conflit d'intérêts.	Aucune précision dans le RGPD – Ce qui vaut pour le CIL vaut certainement à l'identique pour le DPD (cf. art. 38-3 du RGPD). Le G29 rappelle que le DPD n'est pas personnellement responsable en cas non-conformité au RGPD, cette responsabilité étant celle du responsable de traitement[30].
Immunité disciplinaire sauf manquements graves	Principe d'immunité du CIL (Art. 22-III al. 3 loi informatique et libertés) : « *sauf en cas de manquements graves dûment constatés et qui lui sont directement imputables* » – Fiche n° 4 § 4 du Guide CIL 2011 de la CNIL.	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 (Art. 38-3 du RGPD)[31]. L'immunité disciplinaire ne dissipe pas les interrogations sur l'éventuelle responsabilité personnelle du DPD à l'égard des amendes administratives[32].
Possibilité de délégation de pouvoirs	Absence de délégation de pouvoirs avec transferts du risque pénal auprès du CIL au risque de confondre sa fonction avec celle du responsable de traitements, ce qui est proscrit par l'article 46 du décret de 2005 énonçant que le responsable des traitements ou son représentant légal ne peuvent être désignés comme CIL.	Absence de précision sur le sujet de la possibilité d'une délégation de pouvoirs avec transfert du risque pénal. Ce qui vaut pour le CIL vaut identiquement pour le DPD en vertu de la distinction entre sa responsabilité et celle du responsable de traitement[33].
Secret professionnel		Il est lié par le secret professionnel ou la confidentialité dans l'accomplissement de ses tâches - Art. 38-5 du RGPD[34].
Compétences	Le correspondant est une personne bénéficiant des qualifications requises pour exercer ses missions (art. 22-III loi I & L – Fiche 3 § 2 du guide CIL).	Désignation sur la base des qualités professionnelles et, en particulier, des 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 (art. 37-5 du RGPD)[35]. Au vu de ceci, le CIL n'a pas vocation à devenir automatiquement délégué à la protection des données personnelles.
Moyens		Art. 38-2 : 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 et l'autonomie nécessaires[36] 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. Art. 45-2 de la proposition de « *règlement traitement par les institutions européennes* » : le DPD doit disposer, dans l'exécution de ses missions, des ressources nécessaires, ainsi que l'accès aux données à caractère personnel et aux traitements.
Durée des fonctions (*nouveauté de la proposition de règlement traitement par les institutions européennes*)		Art. 45-8 de la proposition de règlement traitement par les institutions européennes. Le DPD est désigné pour une durée de trois à cinq ans et peut être renouvelé. Cette limitation, évoquée lors des travaux relatifs au RGPD puis rejetée, semble contraire à la nécessité d'assurer la stabilité et la continuité de l'action du DPD.

30. *Ibid.* § 6, p. 4.
31. *Ibid.* § 3.4 « *Dissmissal or penalty for performing DPO tasks* ». Art. 45-3 de la proposition de règlement traitement par les institutions européennes : le DPD ne peut être ni licencié ni sanctionné par le responsable du traitement ou le transformateur pour l'exécution de ses tâches.
32. Cf., dans ce même numéro, F. Boucard, « Règlement général relatif à la protection des données personnelles – Le régime novateur des sanctions », spécialement « I.2. Les personnes susceptibles d'être sanctionnées ».
33. *Ibid.* § 1, p. 4. « *DPOs are not personally responsible in case of non-compliance with the GDPR.* [...] *Data protection compliance is a responsibility of the controller or the processor* ».
34. Ce qui ne peut empêcher le DPD de contacter la CNIL pour obtenir un avis. G 29 *Guidelines* WP 243, spéc. p. 10, § 2.3 *in fine*.
35. Considérant 97 : « *Le niveau de connaissances spécialisées requis devrait être déterminé notamment en fonction des opérations de traitement de données effectuées et de la protection exigée pour les données à caractère personnel traitées par le responsable du traitement ou le sous-traitant. De tels délégués à la protection des données, qu'ils soient ou non des employés du responsable du traitement, devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance* ». Le G 29 (*Guidelines* WP 243, spéc. p 11 « *professionnal qualities* ») précise qu'il est pertinent que le DPD ait une expertise réglementaire nationale et européenne en matière de protection des données, une connaissance du secteur d'activité concerné et, enfin, des compétences techniques (compréhension des traitements, des systèmes d'information et des besoins en matière de sécurité et de protection des données). Idem article 44-3 de la proposition de règlement traitement par les institutions européennes.
36. G 29 WP 243, spéc. p 4.

II. LES MISSIONS DU CIL ET DU DPD

Missions	CIL	DPD	Commentaires
Registre des traitements	Le responsable du traitement doit fournir au CIL « *tous les éléments lui permettant d'établir et d'actualiser régulièrement une liste des traitements automatisés mis en œuvre au sein de l'établissement, du service ou de l'organisme au sein duquel il a été désigné* » (Art. 47 du décret de 2005). Dans les trois mois de sa désignation, le CIL dresse la liste mentionnée à l'article 47 (art. 48 du décret de 2005).	Le DPD n'est pas en charge de la tenue du registre des traitements prévu par le RGPD – Il est garant du respect de la réglementation[37].	Le registre est tenu par le responsable du traitement qui le tient à disposition de l'autorité de contrôle. Ce registre participe à l'*accountability*. La tenue par le DPD n'est pas envisageable car il conduirait à un conflit d'intérêts s'agissant d'une tâche incombant au responsable du traitement.
Contrôle de l'application de la réglementation – contrôle des règles internes en la matière	Art. 49, al. 1er, du décret de 2005 : veille au respect de la loi informatique et libertés et fait toutes recommandations.	Art 39 a du RGPD : informe et conseille le responsable du traitement ou le sous-traitant, ainsi que leurs employés procédant au traitement, sur les obligations qui leur incombent en vertu du Règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données. Art. 39 b du RGPD : contrôle le respect : – du 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. Art. 46-2 de la proposition de « *règlement traitement par les institutions européennes* » : le DPD peut formuler des recommandations en vue d'améliorer la protection des données. Conduire des enquêtes sur les faits et événements directement liés ses fonctions et en faire rapport.	Le DPD doit être associé en amont aux travaux concernant les produits et services mettant en jeu les données à caractère personnel (notamment, le comité des nouveaux produits)[38]. Art. 45-1 de la proposition de « *règlement traitement par les institutions européennes* » : le DPD doit intervenir de manière appropriée et en temps voulu dans toutes les questions relatives à la protection des données à caractère personnel. Les *Guidelines* du G29 soulignent que le DPD est le maître d'œuvre d'une « *approche par les risques* »[39]. Cf. *supra* responsabilité.
Information du responsable du traitement des manquements constatés avant saisine de la CNIL – Formation – Sensibilisation	Art. 49, al. 2, du décret de 2005 : possibilité de faire des recommandations auprès du responsable des traitements. Art. 49 al. 5 du décret de 2005 : Informe le responsable des traitements des manquements constatés avant toute saisine de la CNIL.	Art. 39-1-b du RGPD : contrôle du respect du présent Règlement. Proposition de règlement traitement par les institutions européennes Art. 46-1-A : informer et conseiller le responsable du traitement, le sous-traitant et les employés à propos du RGPD et des autres textes relatifs à la protection des données. Art. 46-1-b : veiller, de manière indépendante, à l'application du RGPD, des textes relatifs à la protection des données, ainsi que des règles internes et assurer la sensibilisation et la formation du personnel impliqué dans le traitement des données. Art. 46-1 c : s'assurer que les personnes concernées sont informées de leurs droits et obligations.	

37. Art. 30-1 du RGPD. G 29 WP 243 §4.4. The DPO's role in record-keeping, p. 18.

38. Cf. art. 38-1 du RGPD. - « *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* ».

39. G 29 WP 243, 4.3. « *Risk-based approach* », p. 17.

Missions	CIL	DPD	Commentaires
Réception des réclamations	Art. 49, al. 4, du décret de 2005 et fiche 5 § 2 du Guide CIL : le correspondant reçoit les réclamations et requêtes des personnes concernées par les traitements pour lesquels il a été désigné, s'assure de leur transmission aux services intéressés et leur apporte son conseil.	Art. 38-4 du RGPD : les personnes concernées peuvent prendre contact avec le DPD au sujet de toutes les questions relatives au traitement de leurs données et à l'exercice des droits que leur confère le RGPD.	Art. 41-c du RGPD : le suivi des réclamations peut faire l'objet d'un code de conduite interne.
Bilan annuel	Art. 49, dernier alinéa : « *il établit un bilan annuel de ses activités qu'il présente au responsable des traitements qu'il tient à la disposition de la commission* ».	Aucune disposition dans le RGPD.	À titre de bonne pratique, la rédaction d'un bilan annuel de l'action du DPD est envisageable.
Coopération avec la CNIL	Art. 51 du décret de 2005 : la CNIL peut être saisie à tout moment par le CIL pour toute difficulté rencontrée à l'occasion de l'exercice de ses missions. La CNIL peut à tout moment solliciter les observations du correspondant à la protection des données ou celles du responsable des traitements (art. 50 al. 2 du décret de 2005).	Art. 39-d et e du RGPD : le DPO coopère avec l'autorité de contrôle et sert de point de contact.	
Analyse d'impact (EIPD)		Création du RGPD – Art. 35 et 36 du Règlement : analyse nécessaire dans certains cas et, principalement, lorsque le projet présente des risques importants pour les droits des individus si le responsable du traitement ne prend pas de mesures pour les atténuer. Cette analyse est sous la responsabilité du responsable du traitement (art. 35-1 du RGPD), ce dernier demandant à cet effet conseil au DPD (art. 35-2 du RGPD). Art. 39-2 du RGPD : le DPD tient 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. Art. 46-e de la proposition de « *règlement traitement par les institutions européennes* » : fournir des conseils en ce qui concerne les études d'impact et consulter le contrôleur européen de protection des données en cas de doute quant à la nécessité d'une évaluation d'impact protection données (cf. *infra* au sujet de la consultation du contrôleur européen).	Art. 35 et 36 : seul vestige des autorisations préalables, l'EIVP est nécessaire pour les traitements comportant des risques particuliers pour les personnes[40]. Cette étude doit comprendre[41], outre une description des opérations de traitement et de leurs finalités, une évaluation de ces opérations au regard de la finalité poursuivie et des risques pour les individus, ainsi qu'une description des mesures de protection envisagées. La consultation de l'autorité de contrôle n'est obligatoire qu'en présence d'un risque élevé qui ne peut-être atténué par des moyens raisonnables (cf. considérant 94 du RGPD). La CNIL établira et publiera une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise (art 35-4).
Consultation du DPD / Alertes (*nouveauté de la proposition de règlement traitement par les institutions européennes*)		Art. 45-7 : le responsable de la protection des données peut être consulté « sans passer par les voies officielles », sur toute question concernant l'interprétation ou l'application du règlement traitement par les institutions européennes[42]. Absence de sanctions en cas d'alerte du DPD en raison d'une question portée à son attention au sujet d'une violation des dispositions de la proposition de règlement traitement par les institutions européennes[43].	

Missions	CIL	DPD	Commentaires
Sécurité des données à caractère personnel (*nouveauté de la proposition de règlement traitement par les institutions européennes*)		Art. 16-d : fournir des conseils en ce qui concerne la nécessité d'une notification ou d'une communication en cas de violation de données à caractère personnel.	

40. Art. 35 et 36 du RGPD : *Scoring*, données sensibles, vidéosurveillance, données génétiques ou biométriques, usage de nouvelles technologies.
41. Art. 36-3 du RGPD.
42. *Idem* d'une violation du RGPD.
43. *Idem supra*.

Enfin, l'article 38-4 du RGPD prévoit une amende d'un montant maximum de 10 millions d'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, en cas de défaut de nomination et non-respect de la fonction et des missions du DPD. ■