OBSERVATOIRE DE L'ÉTHIQUE PUBLIQUE

Note. #56

Pour un régime juridique du délégué à la protection des données[1]

RAPHAËL MAUREL

Professeur de droit public à l'Université Bourgogne Europe – CREDIMI
Membre de l'Institut universitaire de France
Directeur du département éthique du numérique de l'OEP

Septembre 2026

[1] La présente note a été rédigée par Raphaël Maurel et n'engage que son auteur.

Sommaire

En bref

Huit ans après l'entrée en application du Règlement général sur la protection des données (RGPD), la fonction de délégué à la protection des données (DPO, pour Data Protection Officer) s'est massivement installée dans le paysage juridique européen : plus de 700 000 organisations ont déclaré un DPO dans l'espace économique européen[2], dont environ 34 250 sont désignés auprès de la CNIL en France[3]. Présentée par le Groupe de l'article 29 puis par le Comité européen de la protection des données (CEPD) comme la « pierre angulaire » du dispositif de responsabilisation[4], cette fonction reste pourtant, en France, dépourvue de tout statut juridique propre. Aucune disposition législative ne précise les conditions d'accès à la profession, aucun ordre professionnel n'en garantit la déontologie, et la protection contre le licenciement n'est garantie qu'indirectement par la jurisprudence européenne. Le contraste est saisissant avec d'autres États membres. L'Allemagne, qui a inventé une fonction proche dès 1977[5], encadre depuis longtemps son exercice par un seuil de désignation obligatoire à vingt salariés, une protection contre le licenciement de douze mois après la fin de mission[6], et un secret professionnel adossé au droit de refus de témoigner. L'Espagne a inscrit dans sa loi organique de 2018 une liste de seize catégories d'organismes tenus de désigner un DPO et un schéma de certification accrédité par l'ENAC selon la norme ISO 17024[7].

[2] Donnée citée par CEPD, 2023 Coordinated Enforcement Action – Designation and Position of Data Protection Officers, rapport adopté le 16 janvier 2024, www.edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf, qui se réfère à une étude IAPP de 2023.

[3] CNIL, « CNIL en bref 2024 », chiffres clés ; v. également CNIL, DGEFP et AFPA, étude « Le délégué à la protection des données (DPO) : un métier de plus en plus représenté dans les petites structures », 1er juillet 2024, www.cnil.fr/fr/observatoire-dpo-enquete-2024, qui mentionne 34 400 DPO désignés en début 2024.

[4] Groupe de travail « Article 29 » sur la protection des données, Lignes directrices concernant les délégués à la protection des données (DPD), WP 243 rév. 01, adoptées le 13 décembre 2016, révisées et adoptées le 5 avril 2017, entérinées par le CEPD lors de sa première séance plénière.

[5] Bundesdatenschutzgesetz (BDSG) du 27 janvier 1977, première loi fédérale allemande de protection des données instituant la fonction de Datenschutzbeauftragter (Bundesgesetzblatt Teil I, 1977, p. 201).

[6] Bundesdatenschutzgesetz (BDSG) du 30 juin 2017, § 6, paragraphe 4, combiné au § 38, paragraphe 2.

[7] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), BOE núm. 294 du 6 décembre 2018, art. 34.

À l'inverse, la France a fait le choix d'un dispositif minimaliste : une certification volontaire portée par la CNIL depuis 2018, une charte de déontologie purement associative publiée par l'AFCDP[8], et aucune protection spécifique. L'action coordonnée du CEPD pour 2023, dont les résultats ont été publiés le 16 janvier 2024 sur la base de plus de 17 000 réponses recueillies par vingt-cinq autorités de protection[9], a confirmé l'ampleur des fragilités : défauts de désignation lorsque celle-ci est obligatoire, ressources insuffisantes, conflits d'intérêts récurrents, lignes hiérarchiques compromises, formation initiale insuffisante.

La présente note plaide pour un changement de paradigme : doter le délégué à la protection des données d'un véritable statut juridique en droit français, articulé autour d'une déontologie codifiée s'inspirant des chartes professionnelles déjà éprouvées dans d'autres professions du numérique et de la conformité, c'est à la fois protéger la fonction, protéger ses titulaires, et protéger ses employeurs. Cette note formule onze propositions concrètes en vue d'un encadrement par la loi ou par décret.

[8] AFCDP, Charte de déontologie des délégués à la protection des données, publiée en 2017 et mise à jour en 2023 à la suite de la décision du Conseil d'État n° 459254 du 21 octobre 2022 ; afcdp.net/charte-de-deontologie-du-dpo/.

[9] CEPD (EDPB), 2023 Coordinated Enforcement Action – Designation and Position of Data Protection Officers, rapport adopté le 16 janvier 2024, www.edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-designation-and-position-data_en.

Une fonction stratégique mais une absence de statut

L'augmentation continue des sanctions prononcées par la CNIL – 87 décisions de sanction en 2024 pour un montant cumulé de plus de 55 millions d'euros, contre 21 en 2022 et 42 en 2023[10] – montre l'intensification de l'exigence de conformité au RGPD, au demeurant attendue huit ans après son entrée en vigueur en 2019. Cette intensification rejaillit directement sur la fonction de délégué à la protection des données, dont le rôle d'intermédiaire entre l'autorité de contrôle, les personnes concernées et les unités opérationnelles des organisations est officiellement reconnu comme « la pierre angulaire » du dispositif européen. La réalité française contraste pourtant avec ce qui précède : dans la pratique, l'exercice de la fonction reste marqué par des fragilités structurelles, dont l'actualité jurisprudentielle, administrative et politique fournit de nombreuses illustrations.

Une pierre angulaire sans statut propre

Les articles 37 à 39 du RGPD[11], complétés par les lignes directrices du Groupe de l'article 29 du 5 avril 2017 (WP 243 rév.01) reprises par le CEPD, posent les fondations communes du régime du DPO : conditions de désignation obligatoire, position au sein de l'organisation, missions, indépendance fonctionnelle, prohibition des sanctions dans l'exercice des missions. Cette base européenne minimale ne suffit toutefois pas à constituer un véritable statut professionnel.

Le RGPD ne crée pas de profession réglementée ; il n'organise ni les conditions d'accès à la fonction, ni les obligations déontologiques de l'ensemble des personnes l'exerçant, ni les mécanismes de discipline. Tel n'est d'ailleurs pas son rôle : il laisse aux États membres, par les clauses d'ouverture, le soin d'aller plus loin (article 37§4) – option dont la France a, jusqu'à présent, fait un usage particulièrement modéré.

Cette modération conduit à un paradoxe. À la fin de l'année 2024, la CNIL recensait environ 34 250 DPO désignés en France[12] sans compter les milliers de DPO informellement et volontairement à l'œuvre dans des organisations qui n'y sont pas contraintes.

[10] CNIL, « Sanctions et mesures correctrices : bilan 2024 de l'action de la CNIL », 5 février 2025, www.cnil.fr/fr/sanctions-et-mesures-correctrices-bilan-2024-de-laction-de-la-cnil ; CNIL, Rapport annuel 2024, publié le 29 avril 2025, www.cnil.fr/fr/rapport-annuel-2024.

[11] Règlement (UE) 2016/679 du Parlement européen et du Conseil 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 (RGPD), JOUE L 119 du 4 mai 2016, art. 37 à 39.

[12] CNIL, rapport annuel 2024.

À l'échelle européenne, l'étude conduite en 2023 par l'International Association of Privacy Professionals (IAPP), citée par le CEPD dans son rapport CEF 2023, faisait état de plus de 700 000 organisations ayant déclaré un DPO dans l'Espace économique européen. Or, ces dizaines de milliers de professionnels exercent dans un cadre juridique qui ne dit rien de leur formation initiale obligatoire, de leur indépendance, de leur déontologie, ni de leurs recours en cas d'atteinte à leur indépendance. Le contraste avec les professions juridiques traditionnelles – avocats, magistrats, notaires, et pour aller plus loin commissaires aux comptes, experts-comptables – qui disposent toutes d'ordres, de codes de déontologie et de juridictions disciplinaires, est frappant.

L'indépendance du DPO, un acquis jurisprudentiel fragile

À défaut de statut national, l'indépendance du délégué à la protection des données a, en grande partie, été construite par la Cour de justice de l'Union européenne. Deux arrêts en constituent les jalons principaux. Le premier, l'arrêt *Leistritz* AG c. LH du 22 juin 2022 (affaire C-534/20)[13], a précisé la portée de l'article 38§3 du RGPD, dont la deuxième phrase interdit au responsable de traitement ou au sous-traitant de relever le DPO de ses fonctions ou de le pénaliser pour avoir exercé ses missions. La Cour a jugé que cette disposition ne s'oppose pas à une réglementation nationale prévoyant des conditions plus strictes que celles du droit de l'Union – en l'espèce, le droit allemand qui réserve le licenciement d'un DPO interne à l'existence d'un «motif grave» et qui maintient cette protection pendant douze mois après la fin de la mission de DPO.

Cet arrêt confirme que les États membres demeurent libres d'élever le niveau de protection qu'ils accordent au DPO. Cette élévation est, en France, inexistante : aucune disposition nationale n'encadre spécifiquement le licenciement d'un DPO, qui demeure un salarié de droit commun ou un prestataire de services.

Le second arrêt majeur, *X-FAB Dresden GmbH & Co. KG* du 9 février 2023 (affaire C-453/21)[14], a permis à la CJUE de se prononcer sur la notion de conflit d'intérêts au sens de l'article 38§6, du RGPD. La Cour y juge qu'un conflit d'intérêts est susceptible d'exister lorsqu'un DPO se voit confier d'autres missions ou tâches qui le conduiraient à déterminer les finalités et les moyens du traitement de données à caractère personnel auprès du responsable du traitement ou de son sous-traitant. L'appréciation doit être faite au cas par cas par le juge national, en tenant compte de l'ensemble des circonstances pertinentes, notamment de la structure organisationnelle. L'arrêt clôt un débat professionnel et juridique mais ouvre, dans le même temps, des zones d'incertitude : à défaut de règles déontologiques opératoires, c'est donc au juge qu'il revient, en aval, de trancher des conflits d'intérêts qui auraient pu être prévenus en amont.

---

[13] CJUE, 22 juin 2022, Leistritz AG c. LH, aff. C-534/20, ECLI:EU:C:2022:495.

[14] CJUE, 9 février 2023, X-FAB Dresden GmbH & Co. KG c. FC, aff. C-453/21, ECLI:EU:C:2023:79.

Les enseignements de l'action coordonnée du CEPD en 2023

L'action coordonnée d'exécution (Coordinated Enforcement Framework) lancée par le CEPD en mars 2023[15] sur le thème de « la désignation et la position des DPO » a réuni vingt-cinq autorités de protection de l'espace économique européen, dont la CNIL et le Contrôleur européen de la protection des données. Plus de 17 000 réponses à des questionnaires adressés à des organisations et à des DPO ont été analysées. Le rapport adopté le 16 janvier 2024[16] identifie sept catégories de difficultés persistantes:

1. le défaut de désignation d'un DPO dans des cas où la désignation est pourtant obligatoire au titre de l'article 37 du RGPD ;
2. le caractère insuffisant des ressources (humaines, budgétaires, en temps) mises à la disposition du DPO pour exercer ses missions ;
3. l'insuffisance des connaissances spécialisées et de la formation continue, la majorité des DPO ne recevant qu'environ 24 heures de formation par an, et 4 % aucune formation ;
4. l'existence persistante de conflits d'intérêts non résolus, en particulier lorsque le DPO cumule sa fonction avec des responsabilités opérationnelles (direction informatique, ressources humaines, conformité, juridique) ;
5. le défaut de remontée hiérarchique au plus haut niveau de l'organisation, pourtant prescrit par l'article 38§3 ;
6. le défaut d'implication du DPO « en temps utile et de manière appropriée » dans toutes les questions relatives à la protection des données (article 38§1) ;
7. l'absence d'indépendance budgétaire, le DPO n'ayant que rarement la maîtrise du budget consacré à la protection des données, ce qui le rend hésitant à critiquer les pratiques de son organisation.

Ces sept faiblesses conduisent à un portrait lucide mains préoccupant d'une fonction structurellement précarisée. Le rapport souligne par ailleurs que le rôle du DPO est en pleine évolution : de nouvelles responsabilités lui sont attribuées au titre des règlements européens récents (règlement sur l'IA (RIA), règlement sur les services numériques (DSA), règlement sur les marchés numériques (DMA), règlement sur les données (Data Act), règlement sur la cyber-résilience (CRA)[17]) sans que les ressources et les protections aient été ajustées en conséquence.

---

[15] CEPD (EDPB), « Launch of coordinated enforcement on the role of data protection officers », 15 mars 2023, www.edpb.europa.eu/news/news/2023/launch-coordinated-enforcement-role-data-protection-officers_en.

[16] CEPD (EDPB), « Coordinated Enforcement Action, Designation and Position of Data Protection Officers », Report, https://www.edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-designation-and-position-data_en.

[17] Règlement (UE) 2024/1689 du 13 juin 2024 (règlement sur l'intelligence artificielle, RIA) ; règlement (UE) 2022/2065 du 19 octobre 2022 (DSA) ; règlement (UE) 2022/1925 du 14 septembre 2022 (DMA) ; règlement (UE) 2023/2854 du 13 décembre 2023 (Data Act) ; règlement (UE) 2024/2847 du 23 octobre 2024 (Cyber Resilience Act).

Des sanctions CNIL qui révèlent des zones grises de la fonction

L'actualité française des deux dernières années offre plusieurs illustrations concrètes des problématiques liées à ce déficit de statut. En 2024, la procédure simplifiée mise en place par la CNIL depuis 2022[18] a permis de prononcer 69 sanctions, pour un total de 715 500 euros d'amendes. Plusieurs décisions ont sanctionné des manquements directement liés à la position du DPO. Dans une affaire rendue publique en mars 2024[19], un organisme a par exemple été sanctionné pour ne pas avoir associé son DPO aux réunions portant sur la protection des données et la sécurité des systèmes d'information ; les coordonnées et les missions du DPO n'avaient pas été communiquées aux employés depuis plusieurs années ; le DPO n'avait pas accès à la messagerie permettant aux personnes concernées d'exercer leurs droits. Le délégué n'était donc pas en mesure d'accomplir correctement ses missions. C'est néanmoins et logiquement l'organisme qui a été sanctionné, et non le mécanisme d'ensemble qui rend globalement possible une telle situation.

La fonction est donc officiellement « la pierre angulaire » du dispositif RGPD, sa centralité est confirmée par la jurisprudence, son périmètre s'étend et est susceptible de s'étendre au gré des nouveaux textes européens, mais son régime juridique demeure, en France, indigent. Cette indigence est d'autant plus singulière qu'elle s'écarte significativement de plusieurs autres droits nationaux européens.

[18]Loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure, art. 33 (créant un nouvel article 22-1 dans la loi n° 78-17 du 6 janvier 1978) ; décret n° 2022-517 du 8 avril 2022 relatif aux modalités de la procédure simplifiée devant la CNIL.

[19]CNIL, « La CNIL a prononcé quinze nouvelles sanctions dans le cadre de la procédure simplifiée depuis janvier 2024 », communiqué du 12 mars 2024, www.cnil.fr/fr/la-cnil-prononce-quinze-nouvelles-sanctions-dans-le-cadre-de-la-procedure-simplifiee-depuis-janvier.

L'insuffisance du régime français du DPO

Pour saisir la spécificité de la situation française, il faut détailler les rares dispositifs existants. Le régime applicable au DPO en France repose aujourd'hui sur quatre étages superposés mais non articulés : le socle européen, la certification volontaire de la CNIL, l'autorégulation associative et le droit commun du travail. Aucun de ces étages ne tient lieu de statut.

Le socle européen : les articles 37 à 39 du RGPD

Le RGPD impose la désignation d'un DPO dans trois cas (article 37§1) : lorsque 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), lorsque 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, et lorsque ces activités consistent en un traitement à grande échelle de catégories particulières de données (au sens de l'article 9) ou de données relatives aux condamnations pénales et aux infractions (au sens de l'article 10).

L'article 38 fixe la position du DPO : il doit être associé « d'une manière appropriée et en temps utile » à toutes les questions de protection des données, recevoir les ressources nécessaires, exercer ses missions « en toute indépendance » sans recevoir d'instructions, ne pas être « relevé de ses fonctions ou pénalisé » pour l'exercice de ses missions, et rendre compte directement au plus haut niveau de la direction. L'article 39 énumère ses missions : informer et conseiller, contrôler le respect du règlement, dispenser des conseils sur l'analyse d'impact relative à la protection des données, coopérer avec l'autorité de contrôle, faire office de point de contact. Ces dispositions, qui s'imposent directement, sont l'ossature minimale du régime mais ne traitent ni des conditions d'accès à la profession, ni de la déontologie, ni de la discipline.

La certification CNIL, un mécanisme volontaire et fragmentaire

Depuis le 20 septembre 2018, la CNIL peut agréer des organismes en vue de délivrer une certification des compétences du délégué à la protection des données.

Le dispositif repose sur deux référentiels complémentaires adoptés par la délibération n° 2018-317 (référentiel d'agrément des organismes)[20] et la délibération n° 2018-318 (référentiel de certification des compétences) du 20 septembre 2018[21], modifiés notamment par la délibération n° 2022-128 du 6 octobre 2022[22], puis par la délibération n° 2023-062 du 13 avril 2023[23].

Le référentiel de certification définit dix-sept compétences et savoir-faire attendus du DPO[24]. Pour être certifié, le candidat doit justifier d'une expérience d'au moins deux ans dans des projets en lien avec les missions du DPO ou de deux ans assortis d'une formation d'au moins 35 heures auprès d'un organisme de formation. L'épreuve écrite comprend 100 questions à choix multiple couvrant trois domaines (réglementation, responsabilité, sécurité) ; la réussite exige 75% de réponses exactes globalement et 50% dans chacun des trois domaines. La certification est valable trois ans et peut être renouvelée à l'issue d'une formation continue. Les organismes certificateurs sont accrédités par le Cofrac selon la norme ISO 17024. Une quinzaine d'organismes, parmi lesquels Apave Certification, Bureau Veritas, PECB et d'autres, sont aujourd'hui agréés.

Le dispositif présente toutefois deux limites majeures. D'une part, la certification est strictement volontaire : aucun texte ne fait obligation à un DPO d'en bénéficier pour exercer. La CNIL elle-même précise sur sa page consacrée que « la certification n'est pas obligatoire pour exercer les fonctions de délégué à la protection des données »[25]. D'autre part, le dispositif ne fait pas obstacle à ce qu'un organisme certifie ses propres DPO « sur la base de son propre référentiel de certification, non approuvé par la CNIL». Le marché de la formation et de la certification est donc juridiquement fragmenté : on peut être DPO sans certification, et l'on peut être certifié hors du cadre de référence de la CNIL. À la différence des avocats, des médecins, des experts-comptables ou des commissaires aux comptes, aucun examen ni stage probatoire n'est imposé par la loi.

---

[20] CNIL, délibération n° 2018-317 du 20 septembre 2018 portant adoption des critères du référentiel d'agrément d'organismes de certification pour la certification des compétences du délégué à la protection des données (DPO).

[21] CNIL, délibération n° 2018-318 du 20 septembre 2018 portant adoption des critères du référentiel de certification des compétences du délégué à la protection des données (DPO).

[22] CNIL, délibération n° 2022-128 du 6 octobre 2022 modifiant la délibération n° 2018-317.

[23] CNIL, délibération n° 2023-062 du 13 avril 2023 modifiant les délibérations n° 2018-317 et n° 2018-318.

[24]Norme ISO/IEC 17024:2012, Évaluation de la conformité – Exigences générales pour les organismes de certification procédant à la certification de personnes ; agréments délivrés par le Comité français d'accréditation (Cofrac), www.cofrac.fr.

[25] CNIL, « La certification des compétences du délégué à la protection des données », www.cnil.fr/fr/la-certification-des-competences-du-delegue-la-protection-des-donnees.

La charte de déontologie de l'AFCDP : une autorégulation associative

À défaut de réglementation, la profession a tenté de s'autoréguler. L'Association française des correspondants à la protection des données à caractère personnel (AFCDP), qui regroupe une part importante des DPO français, a adopté en juin 2017 une Charte de déontologie des délégués à la protection des données[26]. Une mise à jour a été décidée en 2023, notamment pour tenir compte de la décision du Conseil d'État du 21 octobre 2022[27]. Le texte formule des règles de conduite relatives aux qualités personnelles et professionnelles attendues (probité, impartialité, compétences relationnelles, formation continue, secret professionnel), aux relations avec le responsable de traitement et le sous-traitant (confiance, franchise, intégrité, honnêteté, diligence), et à la fin de mission (poursuite « au moins de la carrière qu'il aurait eue s'il n'avait pas occupé la fonction de Délégué à la protection des données »).

La charte présente plusieurs vertus pédagogiques et professionnelles indéniables, et l'initiative doit être saluée. Elle a contribué à centraliser et structurer au sein de l'AFCDP le débat sur l'éthique du DPO, à sensibiliser les responsables de traitement à leurs propres obligations en regard de l'indépendance du DPO, et à fournir une grille de lecture pratique pour un certain nombre de situations délicates. Néanmoins, une charte de déontologie n'est pas un document sanctionné par l'État et reste un texte rédigé et approuvé par les organismes qui défendent les intérêts d'une profession non réglementée ; l'adhésion au texte est volontaire, gratuite, et nécessite la signature conjointe du DPO et du responsable de traitement ou du sous-traitant. Aucune sanction disciplinaire n'est prévue pour les manquements, aucune juridiction professionnelle n'est instituée. Le DPO qui adhère à la charte engage moralement sa parole, mais pas sa carrière.

Le droit commun du travail, une protection par défaut

Au-delà de la certification et de la charte associative, c'est le droit commun du travail français qui s'applique naturellement prioritairement au DPO interne, et le droit commun des contrats au DPO externe, lorsque celui-ci est un prestataire extérieur facturant ses interventions et missions. À la différence de l'Allemagne qui prévoit une protection spécifique – le licenciement n'est possible que pour « motif grave » (wichtiger Grund), et il existe une protection pendant douze mois après la fin de la mission –, la France n'a inscrit dans le code du travail aucune disposition particulière relative au licenciement du DPO.

---

[26] AFCDP, « La Charte AFCDP de déontologie des DPO : un engagement ouvert à TOUS les Délégués à la protection des données, membres de l'AFCDP comme non-membres », https://afcdp.net/charte-de-deontologie-du-dpo/.

[27] Conseil d'État, 10e et 9e chambres réunies, 21 octobre 2022, n° 459254, publié au recueil Lebon, ECLI:FR:CECHR:2022:459254.20221021.

Celui-ci n'est pas un salarié protégé au sens des articles L. 2411-1 et suivants du code du travail[28] ; sa protection ne s'étend pas au-delà des prohibitions résultant directement de l'article 38§3, du RGPD, telles qu'interprétées par la jurisprudence *Leistritz* du 22 juin 2022 (affaire C-534/20).

Cette situation a des conséquences pratiques importantes. Un DPO interne qui s'oppose à un projet présenté par sa direction – par exemple un projet de surveillance des salariés contrevenant au RGPD – peut être licencié pour un motif de réorganisation qui ne se rattache pas formellement à l'exercice de ses missions. Il devra alors démontrer, devant la juridiction prud'homale, que le motif réel du licenciement est lié à l'exercice de sa fonction, ce qui implique une charge probatoire difficile à assumer et de longues procédures moralement complexes. La jurisprudence *Leistritz* autorise pourtant, comme on l'a vu, les États à élever le niveau de protection du DPO.

[28] Code du travail français, articles L. 2411-1 et suivants relatifs aux salariés protégés.

Comparaison européenne : des marges de manœuvre françaises

Pour mesurer pleinement le retard français, on peut présenter, sans prétention à l'exhaustivité, le régime applicable au DPO dans quelques États européens. Trois modèles peuvent être relevés : les États qui ont élargi l'obligation de désignation au-delà du seuil du RGPD, ceux qui ont prévu une protection spécifique contre le licenciement, et ceux qui ont structuré la profession par voie associative ou réglementaire. Parmi eux, on retiendra surtout l'Allemagne et l'Espagne qui présentent des modèles plus aboutis que le droit français.

L'Allemagne : le berceau historique de la fonction

L'Allemagne est l'État européen ayant la plus longue tradition de DPO : la fonction y existe depuis le *Bundesdatenschutzgesetz* de 1977, soit plus de quarante ans avant le RGPD. Le BDSG actuel, dans sa version résultant de la réforme du 30 juin 2017 et de ses modifications ultérieures[29], prévoit à son §38 une obligation de désignation plus large que celle du RGPD : tout responsable de traitement ou sous-traitant du secteur privé qui emploie « en règle générale » au moins vingt personnes occupées en permanence au traitement automatisé de données à caractère personnel doit désigner un DPO. Cette obligation s'ajoute aux cas de désignation obligatoire en cas d'analyse d'impact (article 35 du RGPD) ou de traitement commercial à des fins de transfert, de transfert anonyme, ou d'études de marché ou d'opinion. Le seuil avait initialement été fixé à dix salariés ; il a été relevé à vingt par la loi du 20 novembre 2019[30].

La protection allemande contre le licenciement est exemplaire. Le §6, paragraphe 4, du BDSG, combiné au §38, paragraphe 2, dispose que le contrat de travail d'un DPO interne ne peut être rompu que s'il existe « un motif justifiant la résiliation pour cause grave sans préavis » (« wichtiger Grund »). Cette protection se poursuit pendant douze mois après la fin de la fonction de DPO. Le § 6, paragraphe 5[31], prévoit en outre un secret professionnel spécifique : le DPO est tenu au secret sur l'identité des personnes concernées et sur les circonstances permettant d'en tirer des conclusions, et dispose d'un droit de refuser de témoigner dans les mêmes conditions que celles applicables au responsable de l'organisme. L'association professionnelle BvD (Berufsverband der Datenschutzbeauftragten Deutschlands) regroupe par ailleurs plus de 1800 DPO et a élaboré un code de pratique professionnelle en concertation avec les autorités de protection.

[29] Bundesdatenschutzgesetz (BDSG) du 30 juin 2017 (BGBl. I p. 2097), entré en vigueur le 25 mai 2018 en même temps que le RGPD.

[30] Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU) du 20 novembre 2019 (BGBl. I p. 1626), relevant à 20 salariés le seuil de désignation obligatoire prévu au § 38 BDSG.

[31] Bundesdatenschutzgesetz (BDSG), § 6, paragraphes 5 et 6, relatifs au secret professionnel du DPO et au droit de refuser de témoigner.

En Espagne, un encadrement exhaustif

L'Espagne a choisi de prolonger le RGPD par une loi organique. La Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) du 5 décembre 2018 dresse, à son article 34, une liste de seize catégories d'organismes tenus de désigner un DPO, dont : les ordres professionnels, les établissements éducatifs de tout niveau et les universités publiques et privées, les opérateurs de communications électroniques traitant des données à grande échelle de manière régulière et systématique, les prestataires de services de la société de l'information procédant à du profilage à grande échelle, les établissements de crédit, les compagnies d'assurance et de réassurance, les sociétés d'investissement, les distributeurs de gaz et d'électricité, les entités publiant des fichiers de solvabilité, les opérateurs de jeux de hasard, les entités de sécurité privée, ou encore les fédérations sportives traitant des données de mineurs.

Sur le plan de la qualification professionnelle, l'Agencia Española de Protección de Datos (AEPD) a, en coopération avec l'Entidad Nacional de Acreditación (ENAC), mis en place dès 2018 un schéma de certification des DPO accrédité selon la norme ISO 17024, le « Esquema AEPD-DPD »[32]. Les évaluateurs des organismes certificateurs doivent eux-mêmes justifier d'un diplôme universitaire et d'au moins cinq ans d'expérience en protection des données ou en sécurité de l'information. Un registre public des DPO est tenu par l'AEPD ; la non-désignation a déjà donné lieu à plusieurs procédures de sanction, dont, par exemple, une amende administrative de 25 000 euros à l'encontre de Glovo en 2020 (procédure PS/00417/2019) pour défaut de désignation d'un DPO[33].

La France parmi les États les moins protecteurs

Sans entrer dans le détail des législations étrangères, on peut relever quelques lignes de force. Premièrement, plusieurs États (Allemagne, Espagne, Italie[34], République tchèque[35], Finlande[36], Hongrie[37] au moins) ont fait usage de la clause d'ouverture pour élargir l'obligation de désignation, de manière générale ou sectorielle : la France ne l'a pas fait. Deuxièmement, l'Allemagne offre une protection contre le licenciement spécifique au DPO (« motif grave », prolongée d'un an après la fin de la mission) : la France n'a aucun équivalent.

---

[32] AEPD–ENAC, « Esquema AEPD-DPD » – Esquema de Certificación de Delegados de Protección de Datos, juin 2018, www.aepd.es ; certification accréditée selon la norme ISO/IEC 17024.

[33] Agencia Española de Protección de Datos (AEPD), procédure de sanction PS/00417/2019 contre Glovoapp23, S.L., amende de 25 000 € pour défaut de désignation d'un DPO (référence rapportée par la doctrine spécialisée ; décision consultable sur www.aepd.es).

[34] V. les articles du Codice in materia di protezione dei dati personali (D.lgs. 196/2003) modifié par le D.lgs. 101/2018.

[35] V. l'article 14 de loi tchèque n° 110/2019 sur le traitement des données à caractère personnel.

[36] V. la loi 1050/2018 sur la protection des données, qui rend obligatoire la désignation d'un DPO pour les prestataires de services de soins de santé.

[37] V. la loi hongroise CXII de 2011 modifiée, qui impose la désignation d'un DPO pour les institutions financières, ou encore les opérateurs de télécommunications.

Troisièmement, l'Espagne a institué un schéma national de certification accrédité par la norme ISO 17024 avec des exigences strictes ; la France a un schéma comparable mais entièrement volontaire et sans monopole de l'organisme public. Quatrièmement, plusieurs États ont structuré la profession par voie associative depuis les années 1980-2000 ; la France a, de ce point de vue, une association active (AFCDP), mais aucun ordre professionnel spécifique ni reconnaissance étatique officielle de cet activisme associatif bienvenu. Cinquièmement et toutefois, aucun État européen, à ce jour, n'a réglementé la profession comme une profession ordinale au sens des avocats, médecins ou experts-comptables, ce qui fait du DPO une profession en construction à l'échelle de l'Union.

Quelques sources possibles pour un statut français du DPO

Le déficit français peut être comblé en s'appuyant à la fois sur les meilleures pratiques européennes (le modèle allemand pour la protection, le modèle espagnol pour la certification), sur les chartes déontologiques de plusieurs professions du numérique et de la conformité, et sur les enseignements de l'action coordonnée du CEPD en 2023. L'AFCDP a posé un certain nombre de fondations ; il revient au législateur ou au pouvoir réglementaire de les consolider.

S'inspirer des chartes déontologiques professionnelles

Plusieurs professions juridiques et techniques disposent déjà de codes ou chartes déontologiques susceptibles d'inspirer l'encadrement du DPO. La profession d'avocat est encadrée par le Règlement intérieur national (RIN) du Conseil national des barreaux[38], opposable et adossé à des juridictions disciplinaires. Les magistrats administratifs sont régis par la Charte de déontologie de la juridiction administrative, publiée par le Conseil d'État en 2017 et mise à jour en 2020[39]. Les experts-comptables disposent d'un code de déontologie annexé au décret n° 2012-432 du 30 mars 2012[40], opposable par l'Ordre. Les commissaires aux comptes sont soumis à un code de déontologie homologué par décret (décret n° 2005-1412 du 16 novembre 2005, modifié[41]), placé sous la surveillance du Haut Conseil du commissariat aux comptes. Les notaires sont régis par le décret du 19 décembre 1945[42] et leur règlement national. Les médecins, par le code de déontologie médicale codifié aux articles R. 4127-1 et suivants du code de la santé publique[43].

Dans le secteur numérique en particulier, plusieurs initiatives méritent d'être mentionnées. La Charte de déontologie de l'AFCDP, publiée en décembre 2017 et mise à jour en 2023, est la référence en matière de DPO.

[38] Conseil national des barreaux, Règlement intérieur national de la profession d'avocat (RIN), version consolidée, www.cnb.avocat.fr.

[39] Conseil d'État, Charte de déontologie des membres de la juridiction administrative, édition de septembre 2017, mise à jour de septembre 2020, www.conseil-etat.fr/content/download/156277/file/charte-deontologie-septembre2020.pdf.

[40] Décret n° 2012-432 du 30 mars 2012 relatif à l'exercice de l'activité d'expertise comptable, annexe portant code de déontologie.

[41] Décret n° 2005-1412 du 16 novembre 2005 portant approbation du code de déontologie de la profession de commissaire aux comptes, modifié.

[42] Ordonnance n° 45-2590 du 2 novembre 1945 relative au statut du notariat et décret n° 45-0117 du 19 décembre 1945 pris pour son application.

[43] Code de la santé publique, articles R. 4127-1 et suivants (code de déontologie médicale).

Le Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) en Allemagne, l'Asociación Profesional Española de Privacidad (APEP) en Espagne, et ASSO DPO en Italie ont publié, on l'a dit, des codes professionnels comparables. Au-delà, des références transversales existent : code de déontologie des responsables de la sécurité des systèmes d'information (RSSI) porté par le CESIN, code de bonne conduite de l'Association des correspondants de la conformité de l'AFEP-Medef pour les compliance officers, code professionnel international du Chartered Institute of Information Security (CIISec) au Royaume-Uni. Tous ces textes convergent vers quelques principes structurants : **indépendance du DPO, intégrité, confidentialité, formation continue, conflit d'intérêts, devoir d'alerte, devoir de réserve, et obligations vis-à-vis de l'autorité de contrôle ou du régulateur sectoriel.**

Pour une codification par voie législative ou réglementaire

Au regard du droit comparé et des chartes déontologiques existantes, le législateur comme le pouvoir réglementaire disposent de plusieurs leviers. La voie la plus évidente consiste à **compléter la loi n° 78-17 du 6 janvier 1978[44] par un titre nouveau consacré au statut du DPO** ; à défaut, un décret en Conseil d'État pris en application des articles 8 et 30 de la même loi pourrait **fixer les éléments essentiels du régime.**

Nous formulons ici onze propositions visant à doter le délégué à la protection des données d'un véritable statut juridique en droit français, en s'inspirant des meilleures pratiques européennes (BDSG allemand, loi organique espagnole 3/2018, chartes du BvD, de l'APEP, d'ASSO DPO et de l'AFCDP). Les mesures proposées articulent une **extension de l'obligation de désignation du DPO** à des secteurs critiques (OIV, OSE, plateformes DSA, santé, banque-assurance), **une protection renforcée contre le licenciement** inspirée du modèle allemand (motif grave uniquement, maintien pendant douze mois après la mission), **la codification d'obligations déontologiques** opposables (indépendance, intégrité, prévention des conflits d'intérêts, devoir d'alerte, loyauté), **une obligation de secret professionnel spécifique, et une certification CNIL rendue obligatoire** pour les organismes les plus exposés. Sont également proposées **une garantie d'autonomie budgétaire et matérielle, une formation continue annuelle obligatoire** de 20 à 35 heures couvrant des volets juridique, déontologique et géopolitique, ainsi qu'un **encadrement strict des cumuls de fonctions** à la lumière de la jurisprudence de la CJUE et des bonnes pratiques étrangères. Enfin, on préconise l'instauration d'une **voie de saisine simplifiée de la CNIL** en cas d'atteinte à l'indépendance du DPO, et la constitution, par cette autorité, **d'un registre public consolidé doublé d'un comité consultatif de la déontologie** réunissant associations professionnelles, universitaires, partenaires sociaux et hauts magistrats. À titre subsidiaire, un référentiel déontologique unique tenu par la CNIL permettrait de progresser sans modification législative immédiate.

[44] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée notamment par la loi n° 2018-493 du 20 juin 2018 et par l'ordonnance n° 2018-1125 du 12 décembre 2018.

11 PROPOSITIONS EN VUE D'UN STATUT JURIDIQUE DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Nous proposons à titre principal de *doter le délégué à la protection des données d'un véritable statut juridique en droit français*, articulé autour d'une déontologie codifiée s'inspirant des meilleures pratiques européennes et des chartes professionnelles déjà éprouvées dans d'autres professions du numérique et de la conformité, par voie législative ou, à défaut, par décret en Conseil d'État.
À titre subsidiaire, à défaut d'une telle codification, l'adoption d'un référentiel déontologique unique opposable et tenu à jour par la CNIL, accompagné d'un dispositif de saisine simplifiée en cas d'atteinte à l'indépendance du DPO, permettrait de progresser sans modification législative immédiate.

01

Consacrer le statut juridique du DPO par voie législative
Compléter la loi n° 78-17 du 6 janvier 1978 par un titre nouveau intitulé « Du délégué à la protection des données » fixant les éléments essentiels du statut : conditions d'accès à la fonction, obligations déontologiques, protection contre le licenciement, secret professionnel, conditions de fin de mission, modalités de saisine de la CNIL en cas de manquement à l'indépendance. À défaut d'adoption législative dans des délais brefs, un décret en Conseil d'État pris en application des articles 8 et 30 de la même loi pourrait fixer un socle minimal applicable dès sa publication.

Étendre par la loi l'obligation de désignation à des secteurs critiques
Faire usage de la clause d'ouverture de l'article 37§4, du RGPD pour étendre l'obligation de désignation à plusieurs catégories d'organismes pour lesquels la sensibilité des traitements le justifie : opérateurs d'importance vitale et opérateurs de services essentiels, opérateurs de communications électroniques traitant des données à grande échelle, plateformes en ligne au sens du règlement (UE) 2022/2065 (DSA), établissements de santé, organismes de crédit et d'assurance, ordres professionnels, fédérations sportives traitant des données de mineurs. L'architecture pourrait utilement s'inspirer de l'article 34 de la loi organique espagnole 3/2018.

02

03

Protéger spécifiquement le DPO contre le licenciement et la rupture du contrat

Inscrire dans le code du travail français (par exemple à un article L. 2411-25 nouveau) une protection spécifique du DPO interne contre le licenciement, sur le modèle du § 6, paragraphe 4, du BDSG allemand : le licenciement ne pourrait intervenir que pour motif grave, et la protection serait maintenue pendant les douze mois suivant la fin de la mission. Une protection équivalente devrait être prévue, pour le DPO externe, à l'égard de la résiliation unilatérale du contrat de prestation de service par le responsable de traitement.

Codifier les obligations déontologiques du DPO par décret

Adopter, après consultation de la CNIL et des associations professionnelles, un code de déontologie du DPO sous la forme d'un décret. Ce code reprendrait, en les rendant opposables, les principes déjà consacrés par la Charte AFCDP de décembre 2017 mise à jour en 2023 et par les chartes comparables du BvD allemand, de l'APEP espagnole et d'ASSO DPO italienne : indépendance fonctionnelle et intellectuelle, intégrité et probité, secret professionnel renforcé, prévention des conflits d'intérêts, devoir de formation continue, devoir d'alerte interne avant saisine de l'autorité de contrôle, devoir de loyauté à l'égard de l'organisme et des personnes concernées.

04

05

Joindre une obligation renforcée de secret professionnel au statut du DPO

Reconnaître à la charge du DPO une obligation de secret professionnel spécifique, sur le modèle du § 6, paragraphes 5 et 6, du BDSG allemand : le DPO serait tenu au secret sur l'identité de toute personne concernée et sur les circonstances permettant de tirer des conclusions d'un dossier ou d'une situation, sauf autorisation expresse par les personnes concernées. Lorsque les informations parviennent au DPO dans des conditions justifiant un droit de refuser de témoigner pour le responsable de traitement, ce droit devrait s'étendre au DPO. Ce secret professionnel garantirait la confiance des personnes concernées dans la fonction et renforcerait l'indépendance du DPO.

06

Rendre obligatoire la certification CNIL des DPO dans les organismes les plus exposés

Maintenir le caractère volontaire de la certification CNIL pour la généralité des DPO, mais la rendre obligatoire pour les DPO désignés par les organismes les plus exposés au risque comme les administrations centrales, les autorités administratives indépendantes, les opérateurs d'importance vitale, les plateformes très grandes au sens du DSA ainsi que (liste non exhaustive) les organismes traitant à grande échelle des catégories particulières de données au sens de l'article 9 du RGPD. Cette obligation pourrait être inscrite dans la loi du 6 janvier 1978 ou passer par décret. Elle reposerait sur les délibérations CNIL n° 2018-317 et n° 2018-318 modifiées et leurs versions ultérieures, et sur l'accréditation ISO 17024 délivrée par le Cofrac.

07

Garantir l'autonomie budgétaire et matérielle du DPO

Inscrire dans la loi ou adopter par décret l'obligation pour les organismes désignant un DPO de lui allouer un budget propre, identifié dans la comptabilité de l'organisme et placé sous sa responsabilité fonctionnelle, ainsi que des moyens humains et techniques proportionnés à la taille et à la complexité des traitements. Cette obligation répond directement aux insuffisances identifiées par le rapport CEF 2023 du CEPD adopté le 16 janvier 2024, qui rappelle que l'absence de maîtrise budgétaire compromet l'indépendance du DPO.

08

Imposer une formation continue obligatoire annuelle

Inscrire dans le statut une obligation de formation continue annuelle d'une durée minimale – à fixer par arrêté, sur recommandation de la CNIL – de l'ordre de 20 à 35 heures par an, harmonisée avec les exigences existantes pour le renouvellement de la certification. Cette obligation viserait à corriger la situation décrite par le rapport CEF 2023, selon laquelle une majorité de DPO recevait en 2023 environ 24 heures de formation annuelle et 4 % aucune. La formation comprendrait un volet juridique relatif à l'évolution de la jurisprudence européenne, nationale et comparée mais aussi un volet déontologique et un volet géopolitique destiné à anticiper les risques futurs. Elle devrait s'accompagner d'un droit individuel à la formation imputable sur le budget consacré à la protection des données.

09

Encadrer strictement les cumuls de fonctions susceptibles de créer un conflit d'intérêts

Préciser, par voie réglementaire ou à défaut par lignes directrices de la CNIL, la liste indicative des fonctions incompatibles avec celle de DPO. Cette liste s'appuierait sur la jurisprudence X-FAB Dresden de la CJUE du 9 février 2023 (affaire C-453/21) et sur les sanctions déjà prononcées au niveau européen, dont la sanction Proximus de 50 000 euros (Autorité de protection des données belge, décision n° 42/2020) pour cumul avec la fonction de responsable de la conformité, du *risk* management et de l'audit interne. La liste pourrait notamment inclure les fonctions de direction générale, de direction des systèmes d'information, de direction des ressources humaines, de direction juridique ayant pouvoir de décision sur des traitements, et de président d'un comité d'entreprise traitant des données à caractère personnel.

10

Instituer une voie de saisine simplifiée de la CNIL en cas d'atteinte à l'indépendance

Créer, par voie législative ou réglementaire, une voie de saisine simplifiée de la CNIL ouverte au DPO lorsqu'il estime que son indépendance est compromise, son accès aux informations limité, ou ses recommandations délibérément ignorées sans motivation. Cette saisine pourrait donner lieu à une enquête simplifiée, à des recommandations adressées au responsable de traitement, voire à une mise en demeure. Elle compléterait utilement la procédure simplifiée de sanction de la CNIL instituée en 2022, qui a permis 69 sanctions en 2024. Elle s'inspirerait du mécanisme de saisine des autorités allemandes par le DPO en cas de difficulté.

11

Confier à la CNIL la tenue d'un registre public consolidé et l'animation d'un comité de la déontologie

Consolider, dans le prolongement du registre des DPO déjà tenu par la CNIL, un registre public unique – sur le modèle des registres tenus par l'AEPD espagnole ou par l'Autoriteit Persoonsgegevens néerlandaise – mentionnant pour chaque DPO la date de désignation, l'existence ou non d'une certification, et le secteur d'activité. Confier à la CNIL l'animation d'un comité consultatif de la déontologie du DPO, composé de représentants des associations professionnelles (AFCDP notamment), d'universitaires spécialisés, de représentants des organisations syndicales et patronales, de membres de la CNIL et le cas échéant de membres du Conseil d'État et de la Cour de cassation. Ce comité serait chargé d'éclairer la CNIL sur l'application du code de déontologie, de proposer ses évolutions, et de formuler des avis sur les situations litigieuses transmises par les DPO ou par les responsables de traitement.

CONTACT

contact@observatoire-ethique-publique.com

07-68-46-86-01

9 rue Auguste Angellier - 59 000 Lille

https://www.observatoireethiquepublique.com/

OBSERVATOIRE DE L'ÉTHIQUE PUBLIQUE