Il faut sauver le soldat DPO !

Par Bruno RASLE
bruno_rasle@halte-au-spam.com

Paris, le 5 mai 2023

Title:Saving Private DPO!
Author: Bruno Rasle (bruno_rasle@halte-au-spam.com)
Abstract: The Data Protection Officer job is exciting. It can also be stressful, due to a heavy workload, a lack of resources, insufficient support, or tensions with certain business departments or even with the data controller himself. But there are situations where the DPO is under so much pressure that he or she loses self-confidence, abdicates his or her independence, finds himself or herself isolated, pushed to leave, or even is dismissed. Some of them even fall into depression. Based on the study of emblematic cases, the author attempts to list the various root causes and to identify the lessons that can be drawn from them: what can be done to avoid reaching this point and how to manage these situations if they occur?
Keywords: Data Protection Officer (DPO), GDPR, Data Privacy Officer

Le métier de DPO (Délégué à la Protection des Données) est passionnant. Il peut être également stressant, du fait d'une forte charge de travail, d'un manque de moyen, d'une insuffisance de soutien ou d'écoute, voire de tensions avec certaines directions Métier, voire même avec le responsable de traitement. Mais il est des situations où le DPO est soumis à une telle pression qu'il perd confiance en lui, abdique son indépendance, se retrouve « placardisé », isolé, poussé au départ, voire licencié. Certains d'entre eux vont jusqu'à tomber en dépression. À partir de l'étude de cas emblématiques, l'auteur tente de lister les différentes causes racines et d'identifier les enseignements qui peuvent en être tirés : que faire pour éviter d'en arriver là et comment gérer ces situations si, malgré tout, elles se produisent ?

L'étude : son origine, sa portée, ses objectifs, ses limites, la méthode suivie

Après s'être investi, alors qu'il était délégué général de l'AFCDP[1] (Association Française des Correspondants à la protection des Données Personnelles), dans la création du code de déontologie du DPO[2], avoir participé à la conception de la première enquête de l'AFPA sur le métier[3] dans laquelle il a suggéré l'insertion de questions liées au stress et fait intervenir un psychothérapeute à l'occasion de l'Université AFCDP 2020 des DPO sur le thème « *Le DPO n'est ni un paillasson ni un ennemi* », l'auteur a interviewé en toute confidentialité plusieurs confrères et consœurs qui ont vécu des situations traumatisantes, et dont certains ont mis plusieurs mois pour s'en remettre.

Des délégués à la protection des données internes ont accepté de se confier longuement à lui. Qu'ils en soient ici vivement remerciés. Sans qu'il soit possible d'assurer que ces témoignages fournissent une représentation exhaustive du phénomène étudié, ils permettent de lever un voile sur des situations anormales sur lesquelles règne l'omerta.

Ce silence, couplé à la solitude du DPO, explique en partie l'épuisement intellectuel de plusieurs des professionnels interrogés. À l'issue de la plupart des interviews – souvent douloureuses pour les personnes concernées, encore traumatisées par la mauvaise expérience vécue – l'auteur a souvent entendu des réactions telles que « *J'avoue que c'est encore très difficile pour moi d'en parler, mais je réalise que cela était nécessaire* » ou « *À l'époque, il m'était impossible d'échanger avec mon entourage, y compris familial. Cet isolement a sûrement empiré les choses* ».

L'étude se limite au sort des délégués à la protection des données internes, désignés auprès de l'autorité de contrôle française – la CNIL – au titre de l'article 37 du RGPD (La situation des DPO externes est donc volontairement rarement abordée). L'auteur a posté deux appels à témoignages, sur *Linkedin* et au sein du réseau social privé de l'AFCDP. Un peu moins d'une trentaine de professionnels se sont rapprochés de lui et ont relaté ce qu'ils avaient vécu. L'auteur leur a ensuite communiqué la transcription de leur témoignage, pour leur permettre de l'amender ou de l'enrichir. Tout élément permettant de les identifier a été retiré de l'étude autant que possible (et le projet leur a été soumis, afin qu'ils puissent le vérifier). L'étude *« Cyber stress : une grande étude sur le stress des Responsables Cyber*[4] », menée par le CESIN[5] (Club des Experts de la Sécurité de l'Information et du Numérique) et Advens Cybersecurity et publiée en septembre 2021, a également été étudiée afin d'établir des parallèles et des différences entre la situation des RSSI[6] et de celle des DPO. L'auteur a bénéficié d'échanges fructueux avec les pilotes de cette étude.

Le premier objectif visé était de découvrir s'il existait des cas dans lesquels des DPO internes avaient été mis en très grande difficulté. Comme l'auteur le précisait dans son appel à témoignages, il ne s'agissait pas des freins qui font le quotidien du métier (« *Personne ne m'écoute* », « *Je n'ai aucun soutien de la direction* », « *Je n'ai pas de budget* », *« On m'évite soigneusement et on met en œuvre des traitements qui ne sont pas conformes au RGPD* », *« Je suis considéré comme un empêcheur de tourner en rond, voire comme un espion de la CNIL* », etc.) mais bien des situations dans lesquelles le délégué à la protection des données interne a été poussé à la démission ou licencié, voire

[1] www.afcdp.net

[2] Les termes DPO, DPD, délégué à la protection des données, délégué seront utilisés indifféremment dans ce document pour désigner les professionnels désignés auprès de la CNIL au titre de l'article 37 du RGPD.

[3] La troisième édition (et dernière en date) de cette étude de grande ampleur réalisée chaque année auprès des DPO par l'AFCDP avec la contribution de la CNIL, l'AFCDP et l'ISEP est disponible sur le site web de l'Agence nationale pour la formation professionnelle des adultes. https://www.afpa.fr/actualites/le-delegue-a-la-protection-des-donnees-dpo-un-metier-en-forte-evolution

[4] https://www.advens.fr/wp-content/uploads/2022/06/advenscesin-etudecyberstress-septembre2021-0-comprime-4.pdf

[5] www.cesin.fr

[6] Responsable de la Sécurité du Système d'Information

victime de harcèlement moral : « *Je recherche des DPO qui ont été mis au placard (et ont préféré partir) - voire qui ont été « remerciés » - ou qui ont fait l'objet d'atteintes à leur indépendance* ».

Le deuxième objectif était d'essayer de prendre connaissance des causes à l'origine de ces cas. Retrouve-t-on les mêmes ? De quels ordres sont-elles ? Cette étape doit permettre – et c'est là le troisième objectif visé – de formuler des propositions pour éviter d'en arriver là (démarche pro-active) et pour gérer ces situations si, malgré tout, elles se produisent (démarche corrective).

La réflexion se focalise sur les spécificités liées à la qualité de délégué à la protection des données officiellement désigné auprès de la CNIL. Au sein des organismes, ce salarié n'est pas le seul à connaître les situations traumatisantes évoquées. En revanche, rares sont les fonctions qui présentent des caractéristiques similaires, telle que l'indépendance prévue par le RGPD (mais sans avoir toutefois le statut de salarié protégé).

À qui s'adresse cette étude ? En premier lieu, aux milliers de DPO internes désignés auprès de la CNIL par les responsables de traitement, afin qu'ils sachent détecter à temps les signes qui méritent d'être pris au sérieux et agir en conséquence. En second lieu à l'autorité de contrôle, auprès de laquelle les personnes concernées se confient trop rarement[7]. Enfin, aux responsables de traitement. N'est-il pas désolant de voir des délégués licenciés ou poussés au départ, car leurs actions ont déplu ou bousculé quelques mauvaises habitudes, alors que ces DPO se sont pleinement investis pour réduire leur risque juridique ? On verra *infra* qu'en réalité, la faute en revient souvent au cadre à qui l'on a confié la « supervision » du délégué à la protection des données et qui n'a pas su assurer à ce dernier un environnement propice à un exercice serein de la fonction. Dans une proportion importante, les témoignages recueillis montrent que, si les DPO interviewés étaient enthousiastes à l'idée de rejoindre une entreprise ou un projet, ils les ont souvent fuis à cause de leur hiérarchie directe. L'auteur recommande donc aux DPO internes de communiquer la présente étude à leur N+1 et à leur responsable de traitement.

Cette étude a été initiée avant que le CEPD[8] ne retienne comme sujet, pour l'initiative conjointe européenne pour l'année 2023, la vérification des conditions d'exercice des DPO. Il est prévu, qu'à l'occasion des contrôles effectués par les *Data Protection Authorities*, le respect des critères listés dans les articles 37, 38 et 39 du RGPD soit vérifié. Il est probable que cette campagne s'inspire de l'initiative menée courant 2019 par la CNPD luxembourgeoise et qui a donné lieu à plusieurs délibérations publiées en 2021. À titre d'exemple, dans sa délibération n° 30FR/2021 du 4 août 2021[9], cette autorité avait reproché à un responsable de traitement « *l'absence de ressources suffisantes allouées au DPO au regard de la sensibilité, de la complexité et du volume de données traitées et la non-implication du DPO en amont sur les projets impliquant le traitement de données* ».

Le document est ainsi structuré : dans un premier temps, les témoignages recueillis sont transcrits afin d'en faire ressortir les points saillants (Partie I). En 2014, l'AFCDP avait interviewé Alex Türk, le « père » du Correspondant Informatique et Libertés, précurseur du DPO[10]. L'ancien Président de la CNIL, revenant sur la grandeur de la fonction, ne sous-estimait pas les difficultés que rencontraient déjà à cette époque les CIL : « *Bien sûr, il y a des moments de doute, de grande solitude et même d'adversité. C'est lié à la fonction* ». Les témoignages qui suivent montrent que l'adversité peut quelquefois déboucher sur des situations inacceptables.

Des tentatives d'analyse des témoignages (Partie II) et de taxonomie des causes sources (Partie III) sont ensuite réalisées. Des comparaisons sont également réalisées avec des fonctions qui présentent quelques

[7] L'auteur a été reçu par la CNIL pour un échange de vues très fructueux.
[8] Comité Européen à la Protection des Données (successeur du G29)
[9] https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-30FR-2021-sous-forme-anoymisee.pdf
[10] https://afcdp.ubicast.tv/permalink/v12663724a5ab93dyz3u/iframe/

similitudes avec celle de DPO. L'étude se termine par une évocation des perspectives possibles (Partie IV), dans l'hypothèse d'une poursuite des travaux dans le cadre de la principale association qui regroupe et représente les DPO en France, l'AFCDP. Cinq annexes viennent compléter ce document : 1) une proposition de méthode permettant à un DPO d'évaluer son niveau de stress et d'en identifier les causes ; 2) une analyse des réponses apportées au sondage réalisé en mars 2023 auprès des membres de l'AFCDP sur le sujet de l'indépendance du délégués à la protection des données ; 3) une synthèse des points de contrôles sur les conditions d'exercice du DPO, sur la base de l'analyse des contrôles menés par la CNPD luxembourgeoise ; 4) les trente-six questions soulevées par la CNIL dans le cadre de l'opération conjointe européenne 2023 sur les conditions d'exercice du DPO ; 5) un auto-quiz permettant à un délégué à la protection des données de juger de son assertivité.

Partie I - Témoignages recueillis

Des promesses non tenues

Vingt-six témoignages ont été recueillis entre juillet 2022 et février 2023, lors de longs échanges téléphoniques auprès de douze femmes et quatorze hommes. Quelques entretiens ont été menés auprès de personnes qui ont connu des difficultés majeures avant même d'être officiellement désignées DPO, alors que cela était prévu ou leur avait été promis. Passons en revue pour commencer ces cas spécifiques.

À l'approche de l'entrée en application du RGPD, une personne en poste depuis plusieurs années, représentant du personnel, se voit proposer le futur poste de DPO. L'entreprise s'engage à financer une formation. Pour éviter tout conflit d'intérêt, il lui est demandé en contrepartie de ne pas se représenter aux élections qui approchent. Attirée par la thématique de la conformité au RGPD et par le métier de DPO, cette personne accepte. Elle va rapidement se confronter à deux écueils. Le premier est une exigence de résultats quasi-immédiats : « *Alors ? Nous ne sommes pas encore totalement conformes ? Comment cela est-ce possible ?* ». Tout le monde semble s'imaginer que la conformité au RGPD et à la loi Informatique et Libertés est obtenue par la grâce de la seule présence du DPO et que le travail de celui-ci se limite à « mettre un coup de tampon » ou à inscrire dans un tableau *Excel* quelques malheureux traitements. Mais surtout, la personne se retrouve la cible de la vindicte d'un membre de la direction qui visait également le poste de DPO et qui ne se sent nullement tenu par les engagements formulés. Bien que fort peu compétent sur le sujet, c'est ce « concurrent » qui sera finalement officialisé comme délégué à la protection des données. Après quelques mois de « placard » et un arrêt maladie, le témoin quitte l'entreprise dans le cadre d'une transaction.

Un autre témoin postule à un poste de DPO au sein de l'entité d'un groupe. La description du poste est alléchante et l'échange avec le DPO groupe enthousiasmant. Hélas… trois jours à peine après son arrivée, ce dernier démissionne sur fond de lutte interne entre son équipe et la direction juridique. Le témoin découvre alors une gouvernance kafkaïenne selon laquelle le DPO ne doit s'occuper que de la gestion des demandes de droit des personnes, de la conformité des traitements Ressources humaines et de la réalisation des PIA. La direction juridique s'arroge tout le reste, dont l'encadrement des flux transfrontières et la gestion des violations de données. Par ailleurs, il lui est refusé l'accès aux informations qui lui sont indispensables, comme celui aux contrats établis avec les sous-traitants. Enfin, il n'est pas convié aux réunions clés. Son interpellation du directeur général à qui il signifie qu'il lui semble impossible d'assurer la conformité au RGPD des traitements dans ces conditions restant sans réponse, il se met en arrêt maladie et demande la fin de sa période probatoire, ce qui lui est refusé. Ce n'est qu'à la fin de son arrêt que l'employeur lui signifie finalement la fin de sa période d'essai, sans qu'aucun entretien n'ait eu lieu.

Etudions maintenant le cas d'une personne qui était CIL (Correspondant Informatique et Libertés) avec un rattachement hiérarchique de bon niveau[11]. Comme beaucoup d'autres pionniers, elle s'est investie sans compter pour établir les fondations d'une solide conformité et établir une relation de confiance avec tous les directeurs. À l'occasion d'un rapprochement avec une structure comparable et une période transitoire, un directeur juridique qui vient d'intégrer le nouveau groupe se désigne en tant que délégué à la protection des données, alors qu'il avait peu de connaissances sur le sujet et que le témoin avait toute légitimité pour briguer ce poste (il n'a pas été sollicité ni informé). À la suite de cette désignation, le témoin se retrouve « rétrogradé » en N-7 et intégré à une équipe qui lui fait comprendre que le fait qu'il ne soit pas juriste est rédhibitoire (« *Rends-toi compte, tu n'es même pas juriste !* »). L'ambiance se tend, l'ancien CIL perd alors sa motivation, est arrêté par son médecin avec un début de dépression. Quelques entretiens sont réalisés avec sa hiérarchie, au cours desquels aucun reproche n'est formulé à son encontre mais qui sont truffés d'incitations à aller voir ailleurs… Le témoin est seul, sans soutien. La direction laisse trainer les choses pendant six mois avant de consentir à une rupture conventionnelle.

Des stagiaires exploités

Trois autres témoignages émanent de stagiaires à qui on faisait miroiter à terme l'éventualité d'une embauche au poste de DPO interne.

Nous sommes tout d'abord au sein d'un sous-traitant qui propose ses prestations à des acteurs du secteur du jeu vidéo. Lors de son stage, le témoin constate des pratiques visant à permettre à des mineurs de réaliser des achats d'options avec la carte bancaire de leurs parents, à l'insu de ces derniers. Après avoir émis une remarque à ce sujet, l'interruption de son stage lui est immédiatement signifiée.

Nous voici ensuite au sein d'une entreprise industrielle. Un nouvel actionnaire avait conditionné son entrée au capital – entre autres- par la vérification de la conformité au RGPD. Un audit externe s'était soldé par un plan d'action jugé irréaliste par la direction. Personne ne voulant se saisir du sujet, une bonne âme suggère de confier cela à un stagiaire, avec un défraiement de quelques centaines d'euros par mois. Lors du parcours de sélection, on a assuré au témoin qu'il bénéficierait d'une supervision (comme cela est dû à tout stagiaire[12]) et d'un travail « *main dans la main avec le cabinet d'avocats* » à qui l'audit avait été confié. Aucune de ces promesses ne sera tenues. Dès son arrivée, il est officiellement présenté comme DPO (alors qu'il n'a jamais été désigné auprès de la CNIL). L'entreprise - concernée par l'obligation de désignation – était donc sur ce point en non-conformité. Sous une très forte charge, sans aucun soutien et sans qu'aucune feuille de route ne lui soit communiquée, le stagiaire entame un chantier titanesque, dont la rédaction de BCR (*Binding Corporate Rules*). Tout semble cependant bien se passer jusqu'au jour où il émet la recommandation de réaliser un PIA (analyse d'impact) sur une nouvelle application qu'il juge sensible. Accord lui est donné, mais sous réserve que l'exercice débouche obligatoirement sur un résultat positif même si les risques résiduels sont encore trop élevés. Réalisant que sa présence ne servait que pour légitimer une conformité de façade vis-à-vis de l'actionnaire et des clients, il demande que son stage soit interrompu avant son terme. Le témoin estime qu'il a été exploité et abusé. En revanche, l'épisode a été très formateur, y compris concernant la gestion des relations avec la hiérarchie : « *Ça m'a tanné le cuir : j'ai appris à être dur et à gérer des échanges musclés* ».

Terminons avec un stage réalisé au sein d'un acteur du secteur santé. Là encore, ce qui était demandé au témoin excédait largement les taches d'un stagiaire. Il s'est retrouvé seul pour préparer la totalité de la

[11] L'article 46 du décret n°2005-1309 du 20 octobre 2005 disposait que « *Le correspondant à la protection des données à caractère personnel exerce sa mission directement auprès du responsable des traitements* ».
https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000241445

[12] Voir, par exemple, *Accueil d'un stagiaire : quelles règles devez-vous respecter ?* (Ministère de l'économie, des finances et de la souveraineté industrielle et numérique) https://www.economie.gouv.fr/entreprises/recruter-accueil-stagiaire-regles-gratification#

conformité au RGPD d'un projet ambitieux, en totale contradiction avec ce qui lui avait été dit lors de sa sélection. À chaque réunion, on attendait de lui un « point RGPD », ce qui lui donnait l'occasion de faire état de non-conformités, à commencer par l'absence de DPO désigné auprès de la CNIL (alors que l'entreprise est soumise à l'obligation prévue par l'article 37.1 du RGPD) ou les questionnements liés à l'hébergement des données chez des sous-traitants non immunisés contre les lois extracommunautaires[13]. Aucun des analyses documentées du témoin n'a reçu de retour de la direction, celle-ci « *n'ayant pas le temps de s'en occuper* ». Après son départ, le témoin a appris que ce responsable de traitement avait fait appel à un autre stagiaire, puis à un prestataire externe. Une seule journée par ce dernier acteur était facturée l'équivalent de deux mois de son défraiement, fixé au minimum légal[14]. Le témoin se destinait initialement au métier de délégué à la protection des données. Désabusé, il envisage désormais de devenir avocat.

« L'important, c'est de ne pas faire de vague »

Etudions maintenant les plus emblématiques des autres témoignages recueillis pour pouvoir ensuite en tirer quelques enseignements.

Le premier témoin est embauché en tant qu'assistant du délégué interne d'un groupe du secteur Santé. Peu après son arrivée, le DPO quitte l'entreprise, en mauvais termes avec la direction. On propose au témoin de prendre le relais. Il relève le défi.

La prise de poste se fait dans la douleur : la personne découvre que la conformité n'était qu'apparente (absence de procédure et de politique, absence d'action de sensibilisation, etc.). De plus, l'accueil de la Direction est glacial et le témoin ne dispose ni de budget ni d'aide : il n'est pas remplacé dans son poste d'assistant de DPO et se retrouve donc seul pour assurer la conformité d'un acteur qui traite des données de santé de plusieurs dizaines de millions de personnes. Livré à lui-même, sans aucune supervision, il comprend que la direction considère la conformité au RGPD uniquement comme une contrainte dont elle se passerait volontiers.

Malgré ces constats, le témoin prend cela comme une opportunité et s'investit pleinement, avec des semaines extrêmement chargées (certaines de quatre-vingt heures). Sa pertinence et la qualité de sa production est remarquée et appréciée des clients de l'entreprise mais totalement ignorée en interne. À peine désigné en qualité de DPO, il se voit reprocher le retour très critique de la CNIL du projet de BCR (*Binding Corporate Rules*) rédigé par le précédent délégué et auquel il n'a pris aucune part.

Arrive une nouvelle direction, auquel le délégué se voit rattaché. Le témoin demande à être reçu par cette personne et prépare à son attention une présentation de qualité professionnelle (constats, plan d'action, priorités, urgences, besoins, etc.). C'est la douche froide. Le nouveau directeur découvrait visiblement le sujet et semblait mécontent qu'on lui ait rattaché le DPO, ce dont il n'a que faire (« *L'important, c'est de ne pas faire de vague* »). Durant l'intervention du délégué, il réalise des recherches sur Internet jusqu'à tomber sur une publication de la CNIL qui dit en substance qu'elle se montrera magnanime durant les premières années suivant l'entrée en application du RGPD[15], ce qu'il interprète aussitôt comme une invitation à ne pas

[13] Telles que les *CLOUD Act*, *Patriot Act* et *Executive Order 12333*.

[14] Cela n'est-il pas suffisant pour permettre au stagiaire d'initier un contentieux pour solliciter une requalification en CDI de sa convention de stage ?

[15] Voir, par exemple, l'interview qu'avait donnée Mme Isabelle Falque-Pierrotin (Présidente de la CNIL) au journal La Tribune le 27 Mars 2018 : « ... *nous souhaitons faire preuve de pragmatisme et de bienveillance pour les principes nouveaux du règlement .../... Dans un premier temps, nous privilégierons l'accompagnement et l'explication* ». https://www.latribune.fr/technos-medias/internet/isabelle-falque-pierrotin-cnil-le-rgpd-remet-les-acteurs-europeens-et-internationaux-a-egalite-de-concurrence-773097.html

s'investir sur ce sujet. Dès lors, le témoin est contraint de poursuivre seul son effort (absence d'encadrement, de suivi, de soutien).

Le DPO a d'excellentes relations avec les Métiers, mais les interactions sont exécrables avec la Direction juridique, au point que cette dernière interdit au délégué à la protection des données de formaliser des notes d'analyses juridiques. Lors d'une violation de données, le témoin avait conseillé à la direction de procéder à une notification auprès de la CNIL. La direction juridique y était opposée (« *Mieux vaut nous faire oublier* »). Finalement, c'est l'avis du DPO qui sera suivi.

À force d'insister, le témoin obtient un créneau lors d'une réunion de direction afin de présenter les sujets qu'il porte. À cette occasion, la direction découvre qu'une action qui incombait à la direction juridique n'a pas été réalisée. Dès la sortie de la réunion, le responsable juridique téléphone au DPO pour l'insulter longuement. Dès lors, commence un harcèlement qui ne prendra fin qu'avec le départ du témoin et qui se traduisait par des attaques incessantes, un dénigrement systématique, la mise en doute de ses compétences[16], son isolement, un refus de lui communiquer la moindre information.

Compte-tenu d'un environnement de travail toxique, le témoin prenait soin de tout consigner par écrit et de mettre les membres de la direction en copie de ses signalements les plus importants. Il formalisait également un bilan annuel mais sans qu'il ne génère aucune remarque ni décision de la part de la direction, alors qu'il comportait plusieurs non-conformités, dont certaines criantes.

Le témoin apprend alors incidemment le licenciement de son supérieur hiérarchique et se reprend à espérer l'arrivée d'un responsable avec lequel une synergie pourrait être établie. Lors de son premier échange avec ce nouvel interlocuteur, celui-ci l'interrompt au bout de quelques minutes, lui signifiant que tout cela lui importe peu. Pour lui, l'essentiel est que le DPO déménage pour rejoindre un site très éloigné, ce qui n'est pas prévu dans son contrat de travail. Il précise que, s'il refuse, « *il dégage* ». Deux semaines plus tard, le DPO reçoit à son domicile une lettre recommandée de l'entreprise qui évoque une faute professionnelle. On lui reproche d'avoir répondu à une sollicitation du comité d'entreprise (sur un point de conformité au RGPD), sans en avoir référé à sa direction. Le DPO va voir la direction des ressources humaines, qui lui indique clairement que, de toute façon, « *son compte est bon* ». Il demande à être reçu par la grande direction, qui oppose une fin de non-recevoir : « *Vous inventez des problèmes… Vous êtes le problème* ».

De très difficile, le travail quotidien devient impossible, le DPO étant « placardisé ». Il ne dormait plus correctement déjà depuis plusieurs mois, connaissait un niveau de stress élevé, avait fréquemment les larmes aux yeux, allait au travail la boule au ventre. Le comité d'entreprise ne lui a été d'aucune aide, lui-même étant soumis à des pressions constantes de la part de la direction. Le DPO démissionne. La société lève la clause de non-concurrence et consent à raccourcit la durée du préavis. Ce témoin a ensuite connu une période délicate de six mois, avec suivi psychologique. Malgré cette expérience choquante, il a conservé son amour pour cette fonction (« *C'est le métier de ma vie !* »).

Confrontation avec le DGS

Ce nouveau témoin prend un poste de DPO mutualisé pour un ensemble de collectivités aux missions et tailles très diverses. Essayant durant la procédure de recrutement d'avoir un échange avec le délégué qu'il est censé remplacer, on lui indique que cela n'est pas possible. Il apprendra très rapidement, dès sa prise de poste, que son prédécesseur était très mal vu de la direction, malgré la qualité de son travail.

[16] On peut redouter l'utilisation par les directions Métier de ChatGPT pour obtenir des réponses à des questions telles que « *Quelle doit être la durée de conservation de ces données personnelles ?* » ou « *Faut-il réellement notifier cette violation de données à la CNIL ?* ». ChatGPT apparaissant comme « magique », il est à craindre que ses réponses soient perçues comme « meilleures » que celles apportées par le DPO…

D'emblée, le DGS (Directeur Général des Services[17]) auquel il est rattaché, lui indique clairement ce qu'il pense du RGPD et de la conformité : *« J'en n'ai rien à foutre [sic] de la CNIL... et de toute façon, le risque de contrôle est très faible »*. Le témoin a proposé au DGS de l'agglomération un projet de lettre de mission, inspiré de celle dont bénéficiait son prédécesseur. Il découvre que, dans la version qui lui revient, on lui interdit toute action de sensibilisation auprès des édiles (Finalement, cette lettre de mission n'a jamais été soumise pour signature au Président de la collectivité).

Le nouveau DPO a demandé à rencontrer les élus, pour se présenter à eux, s'enquérir de leurs besoins et priorités et répondre à leurs éventuelles questions, demande très mal reçue par le DGS. Ces entretiens se sont toutefois très bien passés, les élus assurant donner « carte blanche » à leur nouveau DPO. L'un d'entre eux croit bon toutefois d'ajouter un commentaire : « *De toute façon, je connais personnellement l'un des Commissaires de la CNIL…* ».

Le témoin obtient une intervention lors d'un comité de direction afin d'être présenté aux directeurs. À peine a-t-il commencé à s'exprimer, qu'il constate que son responsable hiérarchique passe son temps à se prendre en *selfie* et que plusieurs directeurs tiennent des conciliabules, ne prêtant aucune attention à son intervention. De plus, l'introduction prononcée par son responsable hiérarchique avait confirmé sa non-compréhension du rôle d'un DPO. Précisons qu'au bout d'un an, certaines personnes ignoraient toujours que le témoin était le délégué désigné, le projet de note de service pour le faire savoir n'ayant jamais été validé (et n'ayant donc jamais été diffusé au personnel).

Il était prévu des réunions régulières entre le DPO et le DGS. Finalement, compte-tenu des crispations constantes concernant la conformité au RGPD, elles ne se tiendront que rarement. Le témoin s'est rapidement rendu compte que, dans l'esprit du DGS, un DPO est une sorte de « super-secrétaire » qui fait tout seul, avec comme mission principale, la saisie du registre, et qui ne doit pas déranger les opérationnels (aussi n'est-il pas étonnant que l'inventaire n'ait pas pu être mené à bien, du fait de l'absence de réponse de la part des services).

D'une façon générale, le DGS ne répondait aux sollicitations du témoin qu'à de rares occasions, et jamais par écrit. Et, systématiquement, il se comportait de façon très désagréable avec le témoin. Il lui reprochera notamment « *de se comporter comme un auditeur indépendant »* (dans sa bouche, c'était visiblement un défaut, alors que tout bon DPO devrait l'interpréter comme un compliment, comme une reconnaissance de son autonomie et de son intégrité).

Lors du recrutement, il avait été indiqué au témoin qu'il disposerait d'un budget (au demeurant très limité). En fait, il n'a jamais réussi à obtenir les clés de répartition de celui-ci entre les entités pour lesquelles il était désigné. De plus, il n'a jamais pu le dépenser. Après avoir obtenu des devis (notamment pour faire réaliser des PIA), ses demandes de commandes de prestations sont restées lettres mortes. Au final, aucun PIA n'avait été réalisé lors du départ du témoin.

Constatant des écarts, le témoin aurait voulu mettre en conformité les traitements du périmètre Ressources humaines, mais on l'en a fortement dissuadé (« *Ce n'est pas une priorité* »). Quelques incidents de sécurité étaient signalés au DPO par des membres du service informatique, sur leur propre initiative, mais sans qu'aucun d'entre eux n'aboutisse à une notification de violation à la CNIL par absence de décision de la direction. Le témoin a finalement préféré quitter ce poste et cette collectivité.

[17] Au sein d'une collectivité territoriale, le directeur général des services est un cadre supérieur d'administration et un collaborateur du chef de l'exécutif. Il est chargé de diriger l'ensemble des services et d'en coordonner l'organisation.

« Votre prédécesseur n'y voyait aucun inconvénient, lui »

Passons maintenant à l'expérience vécue par un DPO interne au sein d'un acteur du logement social. Déjà salarié de cet organisme, le témoin abandonne ses anciennes responsabilités et accepte de remplacer le DPO qui vient de démissionner (celui-ci se plaignait de ne pas disposer d'assez de moyens pour réaliser pleinement ses missions).

Il bénéficie d'un très court tuilage avec le DPO qu'il remplace, mais, découvrant le sujet, il prend un maximum de notes sans forcément toujours comprendre. Dans la foulée, il suit une formation de cinq jours - là également sans être sûr de bien tout assimiler - et décroche la certification des compétences du DPO. En revanche, aucune création de poste n'est prévue pour l'épauler.

En tant que nouveau DPO, il détermine trois priorités : la sensibilisation de l'ensemble du personnel, la gestion des demandes de droits d'accès et la gestion des violations de données. Réaction laconique de la direction : « ... *du moment que cela ne gêne pas l'activité* ». Au total, il a sensibilisé plusieurs centaines de collaborateurs sans que, malheureusement, les cadres dirigeants ne fassent l'effort d'y assister (« *Le directeur des systèmes d'information ne croyait ni au RGPD ni au DPO, ni au risque d'amendes de la CNIL dans le secteur du logement social* »). Sa procédure de gestion des violations de données a été utilisée à quelques reprises, notamment à l'occasion d'une intrusion informatique par un pirate qui a usurpé les droits d'accès *Microsoft 365* d'un collaborateur, ce qui lui a permis d'avoir accès à des pièces sensibles, dont des documents d'identité. Le DPO a dû faire appel à un avocat (sur son budget propre) pour convaincre la direction de notifier la violation à la CNIL et de la communiquer aux personnes concernées.

En revanche, il n'a pas eu le temps de s'attaquer aux analyses d'impact (PIA), même s'il se préparait à en réaliser une première sur le traitement des signalements formulés par les lanceurs d'alertes au titre de la loi Sapin II (mais le référent commençait déjà à se braquer à cette perspective, considérant « *qu'il en avait déjà assez fait* »).

Il s'aperçoit rapidement que, bien que le directeur général l'assure de son soutien, la conformité était ressentie unanimement comme une gêne et qu'il n'était jamais sollicité (« *Personne ne voulait entendre parler du RGPD* »). Très tôt, le témoin se heurte à la priorité donnée aux objectifs métiers, considérés comme supérieurs aux exigences de conformité. Ainsi, lorsqu'il questionne la légitimité de certaines transmissions de données personnelles de locataires vers des collectivités, cela lui vaut de fortes réactions : « *On a toujours fait ainsi* », « *Nous devons conserver de bonnes relations avec le Maire* », « *Votre prédécesseur n'y voyait aucun inconvénient, lui* ».

Avec le recul, le témoin indique qu'il manquait du recul (en tant que DPO) qui lui aurait permis de traiter en temps réel les objections (des directions Métiers, de la direction) qui lui étaient systématiquement opposées. Il estime que la formation qu'il a suivie était trop courte pour lui permettre d'être en meilleure posture pour gérer les oppositions (« *La certification et la formation de cinq jours ne sont pas suffisantes, il faut du vécu* »). Ses tentatives pour s'appuyer sur le risque de sanction sont restées vaines et il n'a jamais eu l'occasion de rencontrer le responsable de traitement. Par ailleurs, aucun point régulier n'était tenu avec son supérieur hiérarchique.

Au final, le témoin se sentait en situation d'inconfort permanent, seul et insuffisamment préparé au métier de DPO. De plus, se posait la question de la valeur donnée à ses efforts : « *Est-ce que ce que je fais intéresse quelqu'un au sein de l'entreprise ? Mon travail a-t-il un sens ?* ». Aussi, quand on lui propose d'assurer en sus la conformité d'autres entités sans lui accorder plus de moyens, il oppose un clair refus. La direction est surprise de cette décision, considérant que la mise en conformité au regard du RGPD est « *facile* » et que cela se limite à tenir à jour quelques « *paperasses* ». Il quitte alors l'organisme pour rejoindre une autre entreprise, dans laquelle il a repris des fonctions liées à sa formation initiale, très éloignée du monde de la conformité. Ce

témoin indique « *ne plus croire au métier de DPO* », qu'il trouve « *extrêmement ennuyeux et trop gratte-papier* », notamment par l'obligation de tenir un registre des traitements.

Le témoin suivant a été « chassé » pour travailler dans le contrôle interne dans une entreprise de taille moyenne, familiale. À l'occasion du départ du CIL désigné auprès de la CNIL et de l'entrée en application du RGPD, on lui propose de prendre en plus la fonction de DPO. Au début, tout se passe bien, notamment auprès des salariés qui comprennent bien les règles devant être suivies et les acceptent. Tout commence à changer quand il recommande de notifier une violation de données à la CNIL (refus avec le commentaire « *Niet. On ne notifiera pas, jamais* », position érigée en dogme) et met en évidence plusieurs non-conformités. La tension monte quand, lors d'un séminaire de direction, le témoin formule des remarques touchant à la conformité pour le moins « perfectible » des axes stratégiques qui étaient évoqués. Par ailleurs, le directeur général est très autoritaire : on a le droit d'avoir un avis, du moment que c'est le sien.

Ces conditions de travail le mettant dans l'impossibilité de faire correctement son métier, le témoin préfère quitter l'entreprise pour prendre un nouveau poste de DPO interne (Ce malheureux épisode n'ayant pas amoindri son intérêt pour le métier). Globalement, tout se passe bien au sein de ce nouvel employeur... Jusqu'au jour où il a été forcé de modifier son avis et d'abaisser le niveau d'un risque. Il a gardé par précaution tous les éléments qui montreraient sa bonne foi et son professionnalisme en cas de litige (l'entreprise pourrait soudain ne plus se souvenir de la pression qu'elle a exercée sur son délégué et l'incriminer). Il trouve également regrettable que son responsable hiérarchique ne l'ait pas soutenu à cette occasion.

Revenons dans le secteur de la Santé, pour un autre témoignage. Ce nouveau témoin répond à une offre de poste de DPO interne. Lors des entretiens de recrutement, on lui indique que la désignation d'un délégué à la protection des données est l'une des exigences des investisseurs. Bien que désigné auprès de la CNIL dès son arrivée, il a rapidement constaté que la conception de la conformité de l'entreprise était très éloignée de son éthique : sa fonction n'est qu'apparence (« *Il s'agissait en fait de RGPD washing* »). Il a notamment rencontré une forte opposition de la part d'un chef de service qui considérait que l'arrivée d'un DPO remettait en cause ses prérogatives et refusait ouvertement de prendre en compte les objectifs de conformité. Considérant l'écart trop important pour espérer faire bouger les choses, il n'a pas été jusqu'au bout de sa période d'essai. Il épaule désormais un DPO au sein d'une entreprise dans un autre secteur d'activité.

Le témoin suivant est promu DPO interne au sein d'une entreprise dont l'avenir n'est pas assuré, ce qui entraînait de fortes tensions. Il juge élevés les risques résiduels que présente un projet présenté comme capital, malgré l'attitude du chef de projet laissant entendre qu'il ne possédait pas les connaissances techniques lui permettant d'apprécier les risques à leur juste valeur. Interdiction lui est faite de prendre contact avec la CNIL pour lever le doute.

Après avoir formulé par écrit son analyse, la direction lui demande de ne plus rédiger de tels documents. N'ayant pas procédé à une embauche pour remplacer le témoin à son poste précédent, la direction lui demande alors d'assurer les taches associées, en sus de celles de DPO. Cette démarche qui vise à le « noyer » sous une très forte charge (sans doute pour réduire son activité dans le champ de la conformité) participe de son stress intense.

Prenant acte qu'il lui était impossible d'exercer ses missions de DPO dans des conditions correctes – tenant compte entre autres d'une logique « business » implacable, de l'absence de dialogue, des résistances au changement et d'une ambiance lourde -, il a préféré quitter l'entreprise pour trouver un nouveau poste.

Chassé par un cabinet de recrutement, le témoin suivant accepte un poste de DPO interne après un bon entretien avec le responsable juridique, son futur supérieur hiérarchique. Surprise : durant son préavis, il reçoit un message émanant d'un tout nouveau directeur juridique, qui « *l'attend avec impatience car il y a beaucoup à faire* ». Et, effectivement, à sa prise de fonction, il constate que tout reste à mettre en place.

Il se rend vite compte que, dans cette entreprise, tout doit être extrêmement rapide. Le dirigeant a d'ailleurs l'habitude de proclamer « *Je ne veux pas que ma société marche, je veux qu'elle coure* ». Le témoin commence par formaliser des projets de procédures et les soumet au directeur juridique, qui ne lui fera jamais aucun retour ni aucune critique. Aucun objectif n'est fixé au nouveau DPO.

Celui-ci a rapidement la surprise de voir son supérieur lui dicter son plan d'action et ses priorités. Ainsi, alors que le délégué voulait travailler en priorité sur le respect des durées de conservation et les PIA les plus urgents, on lui ordonne de se concentrer sur l'encadrement des sous-traitants. Le directeur juridique impose une forte pression sur le témoin, en lui dictant ses tâches jour par jour (le plus souvent impossibles à réaliser dans le temps imparti) et sans jamais lui proposer d'aide.

Lors de son premier entretien annuel, il est reproché au DPO de ne pas avoir atteint les objectifs (pour rappel, aucun n'a été fixé lors de la prise de poste). Le témoin fait observer que, sans interlocuteur et sans réponse de la part des Métiers, il peut difficilement avancer comme il le souhaiterait.

Les demandes initiales du DPO pour bénéficier d'une aide sont repoussées... jusqu'à ce que le directeur juridique lui annonce qu'il va être épaulé par un prestataire. En fait, ce dernier lui est imposé comme nouveau responsable hiérarchique. Dès son arrivée, ce dernier adopte la même posture que le directeur juridique et inflige au délégué une pression renouvelée, en exigeant, à plusieurs reprises, une réactivité immédiate. Le DPO est alors « convié » à une réunion au cours de laquelle un point d'avancement devait être fait sur quelques dossiers. En fait, pendant plus de deux heures, le directeur juridique et le prestataire vont le mettre sur le gril, en insistant sur le fait que plusieurs des chantiers de conformité n'étaient pas clos, et en faisant porter la responsabilité de ces retards uniquement sur le DPO.

Le témoin connait un début de dépression et est arrêté. Il reçoit à son domicile une lettre d'entretien préalable avant licenciement. Le témoin est finalement licencié pour « *insuffisance professionnelle* » au motif qu'il n'a pas achevé la mise en conformité de l'entreprise au premier anniversaire de sa présence dans l'entreprise[18].

Du rêve au cauchemar

Le témoignage suivant décrit le passage d'une situation nominale à une franche dégradation des conditions d'exercice du DPO.

Dans un premier temps, le témoin est délégué à la protection des données (après avoir été CIL). Soutenu par la direction, il a pu réaliser beaucoup de choses. Ayant pour responsable hiérarchique le directeur général adjoint (également DSI), il présente au directeur général son bilan annuel, que ce dernier endosse.

Arrive un nouveau directeur général. Dès son arrivée, s'installe un climat général qui vise à « changer les têtes ». Lors de son allocution prononcée lors de ses vœux, le nouvel arrivant demande à tous d'être « plus efficace » et se moque des européens qui freinent l'innovation et le business ... et de prendre pour exemple le RGPD. Cette déclaration, faite devant l'ensemble des salariés et en présence du DPO, sape la sensibilisation réalisée jusqu'alors et traduit un manque de soutien de la direction. C'est une véritable douche froide.

[18] Naturellement, les menées pour pousser son délégué à la protection des données ne datent pas de l'entrée en application du RGPD. Dans sa thèse professionnelle soutenue en 2009, Aurélie Goyer rapporte le cas d'un CIL qui avait été poussé vers la sortie après avoir présenté son bilan à son responsable de traitement et avoir signalé à ce dernier plusieurs non-conformités majeures qu'il convenait de corriger. [A. Goyer, « *Donne-t-on les moyens au Correspondant informatique et libertés d'être efficace ?* », thèse professionnelle soutenue dans le cadre du Mastère spécialisé « Management et Protection des Données Personnelles » de l'ISEP, promotion 2008-2009, Tuteur de thèse B. Rasle]

Lors de son premier entretien avec le nouveau directeur général, le témoin présente son bilan, ses indicateurs et son plan d'action, qu'il compte poursuivre. Alors qu'il demande avoir besoin de plus de temps pour assurer la conformité de l'entreprise, le nouveau directeur général lui indique qu'au contraire il demande à ce qu'il ne consacre que 10 % de son temps à son poste de DPO : « *Tu es un centre de coût… non rentable… Tu as assez travaillé dessus, c'est bon, on est déjà conforme, pas besoin d'en faire plus...* ».

De plus, il sera désormais supervisé par le responsable des audits : on lui interdit de contacter le directeur général adjoint (son précédent superviseur) et de déranger le directeur général avec des problématiques de conformité. Dès lors, le DPO sacrifie plusieurs chantiers qu'il comptait entamer, comme la réalisation de PIA, la vérification des purges des données et l'enrichissement du registre avec les traitements issus d'entités récemment intégrées, pour ne plus gérer que les priorités, c'est-à-dire la réponse aux sollicitations des collègues *(« Je prenais sur mon temps personnel pour ne pas les laisser tomber* »).

Un an après, le témoin présente son bilan au directeur général et commence par présenter les indicateurs liés à la gouvernance. Du fait de l'absence de soutien de la direction, ceux-ci sont négatifs. Le directeur général est furieux et s'en prend au délégué : « *Tu vas me changer cela ! Le simple fait que tu sois là montre mon implication* ». Sous la menace, le DPO modifie son bilan et en transmet par courriel la nouvelle version au dirigeant (qui reste sans réaction).

Survient la pandémie liée au Covid 19 et le premier confinement. Le délégué propose de communiquer en interne pour rappeler les risques liés à cette situation et pour inciter les salariés à prendre quelques précautions en posture de télétravail. Refus du directeur général (« *Ce n'est pas la priorité* »).

Un peu plus tard, il est convoqué à une réunion à distance avec le dirigeant, sans que son objet lui soit annoncé. On lui annonce alors que, comme il se déclare dans l'incapacité d'assurer la conformité au RGPD et de réaliser son plan d'action dans le temps qui lui est imparti, la qualité de DPO va lui être retirée. C'est un nouvel arrivant (qui n'a aucune connaissance dans le domaine de la conformité au RGPD) qui serait désigné à sa place. Le témoin est abasourdi : « *Mon univers s'est effondré… Cette hypothèse était pour moi inconcevable… Quel gâchis. Tout mon investissement n'aura servi à rien…* ». Après avoir remarqué qu'il se met à pleurer facilement, le témoin consulte un médecin qui diagnostique un épuisement professionnel, lui prescrit un traitement ainsi qu'un arrêt de travail : « *Ma fierté en a pris un coup* ».

Craignant de voir ses compétences s'étioler s'il accepte de devenir la « petite main » du futur DPO, il quitte l'entreprise. Il est intéressant de noter que le témoin a tenu par la suite à obtenir la certification des compétences du DPO afin de se rassurer sur ses connaissances : le harcèlement dont il avait été la victime avait réussi à saper sa confiance en lui-même.

Des DPO en grande souffrance

Le témoin suivant, désireux de quitter la région parisienne, postule à un poste de DPO interne que propose une entreprise basée en région.

Dès son arrivée, il se retrouve seul dans un bureau, isolé. On lui remet uniquement les livrables laissés par un consultant qui a participé à son entretien d'embauche. Ces documents sont limités et de qualité médiocre : le nouveau DPO se demande comment le prestataire a fait pour ne pas relever plusieurs non-conformités évidentes. C'est là une première difficulté : il ne partage pas les conclusions formulées par le consultant et considère le niveau réel de conformité inférieur aux constats de ce dernier. Mais c'est son analyse que l'on met en doute et il doit batailler pour faire valoir son point de vue.

Le nouveau délégué à la protection des données comprend rapidement qu'on attend de lui principalement des indicateurs qui soient de la « bonne » couleur et en progression constante. Rien d'autre. Et surtout il lui

est interdit de générer de la charge pour les autres salariés de la société. Or il est impossible au témoin de réaliser ses missions de DPO sans, *a minima*, interagir avec les différentes directions, ne serait-ce que pour obtenir les réponses à ses questions.

Par ailleurs, le directeur général ne porte aucun intérêt à la conformité, qu'il ne perçoit que comme une contrainte. Dès l'une des premières réunions, durant laquelle le DPO ose soulever une question, on lui fait clairement comprendre qu'il devrait éviter à l'avenir de prendre de telles initiatives. Le témoin observe également des pratiques qui ne correspondent pas à sa conception du métier (ni aux exigences du RGPD et du Code du travail). Ayant peur de ne pas retrouver rapidement un poste dans la région, il reste encore quelques temps au sein de l'entreprise, dans des conditions d'exercice totalement anormales. Il perd confiance en lui-même, perd la conscience même du métier de DPO, se sent impuissant. En souffrance psychologique, il donne finalement sa démission.

Il rejoint ensuite une société de la région, mais se sent en situation de fragilité dès son arrivée (victime du syndrome de l'imposteur) et met du temps à retrouver confiance et goût de la mission. Mais il s'effondre lors du premier entretien avec son supérieur hiérarchique, à l'évocation d'une difficulté qui, en temps normal, aurait été traitée sans heurt. Il entre alors en *burnout* (en fait, il en prend conscience) et bénéficie d'un suivi médical. Son nouvel employeur lui apporte son soutien et l'accompagne sur le chemin du retour à une situation « normale ».

Passons maintenant au secteur de la grande distribution. Le témoin y est DPO interne. Il rencontre les difficultés malheureusement trop fréquentes dans un tel poste (dont la difficulté à obtenir des réponses de la part des opérationnels et l'absence de fiche de poste).

Il subit une charge de travail extrême (« *Toujours sur le pont, j'avais des horaires de dingue*… »), qui s'explique partiellement par un double rattachement (cause d'une gouvernance défaillante, dysfonctionnelle). Par ailleurs, le témoin se retrouve fréquemment en situation délicate, avec des relations professionnelles sans complaisance, agressives : un responsable lui lance « *Tu n'y connais rien !* », voire des propos vexants tenus à son égard (« *Voilà encore l'oiseau de mauvais augure* »). De plus, il lui était souvent demandé de « *trouver des solutions* », au lieu de rester dans une posture d'observation, d'analyse et de conseil prévue par le RGPD.

Quand il a voulu faire état de ses conditions de travail, notamment pour disposer d'un budget lui permettant de se faire aider, son encadrement s'est montré outré par la démarche : on lui a clairement fait comprendre que son niveau hiérarchique et son statut ne lui permettait pas une telle initiative ! Par la suite, on lui a interdit de s'adresser au Président Directeur Général.

L'un de ses deux superviseurs le bombarde de directives visant à le surcharger encore plus – en imposant des délais de réalisation irréalistes. Même quand le DPO y répond en prenant sur son temps personnel, les documents qu'il produit tombent dans un trou noir. Le témoin a toujours été dans l'impossibilité de débattre sereinement des sujets RGPD avec ses superviseurs et avec le responsable de la sécurité du système d'information. Surchargé, il n'a pas pu s'investir dans les PIA. Concernant les violations de données, il n'avait pas toujours accès aux informations pertinentes qui lui aurait permis de conseiller le responsable de traitement.

Certains de ses collègues avaient remarqué sa fatigue et lui en avait fait part, inquiets pour sa santé. Il a alors consulté un médecin qui lui a prescrit un arrêt de travail pour épuisement professionnel. Il a démissionné mais en veillant à transmettre tout document utile à ses successeurs. Le témoin apprendra plus tard que deux personnes ont été recrutées pour réaliser les tâches qu'il était seul à réaliser.

Une lune de miel de courte durée

Le témoin suivant prend un poste de DPO interne dans le secteur de l'énergie. Durant la phase de recrutement, on lui indique clairement que « *tout reste à faire* » en matière de conformité au RGPD, mais en lui promettant une aide.

À la grande surprise du témoin, l'entreprise confirme son embauche immédiatement, sans attendre la fin du préavis. Le poste était alléchant sur le papier, mais ce fut en fait une expérience malheureuse. Aucune des promesses n'est tenue. La lune de miel fut de très courte durée et le délitement très rapide. Dès les premiers échanges, on nie son autonomie de DPO (« *Ça partait dans tous les sens, je n'ai jamais pu établir mes priorités* ») et on le cantonne au traitement de toutes les réclamations des clients qui se disent mécontents des méthodes commerciales de l'entreprise. L'encadrement direct était maltraitant (déluge de demandes urgentes avec l'injonction de « *performer sans jamais franchir la ligne rouge* »). Au bout d'une année, le témoin quitte cet environnement malsain. Il dit avoir été « abimé » par cette mauvaise expérience (« *Ça laisse des traces…* ») et indique qu'il commençait à douter de lui-même.

Toujours dans le secteur de l'énergie, un DPO qui a amené son entreprise à un niveau satisfaisant de conformité se voit convoqué par son superviseur pour s'entendre dire, estomaqué : « *Dans deux mois, tu n'es plus notre Délégué à la Protection des Données. On en discute dans quelques semaines, lors de ton entretien annuel et j'ai d'ores et déjà pris rendez-vous pour toi auprès de la DRH afin qu'elle te trouve un autre poste* ».

Passons maintenant dans le secteur associatif. Le témoin postule au poste de DPO interne, avec un rattachement à la direction juridique.

Le DPO commence à sensibiliser les différentes directions mais se heurte à deux obstacles : Le directeur des systèmes d'informations a eu un profond désaccord avec la direction juridique et ne veut plus interagir avec elle... et donc n'accepte pas que le DPO sensibilise ses équipes ou cherche à les contacter. De son côté, la direction des dons lui claque la porte au nez et refuse d'être « *embêtée* » par un DPO.

Survient une cyberattaque qui touche un sous-traitant de l'association. Le délégué l'apprend incidemment et s'attend à travailler sur une éventuelle violation de données. Mais la direction des dons s'oppose à ce qu'il participe à la cellule de crise, en suspectant le DPO « *d'être capable d'en parler à la CNIL* ». La direction juridique rédige un projet de courriel destiné à être envoyé au sous-traitant. On sollicite le DPO afin qu'il valide d'urgence ce projet. Le témoin suggère quelques modifications et demande à recevoir une nouvelle version du projet avant de formuler son avis final. Surprise ! Il découvre que le message a été envoyé sans qu'il puisse le relire, mais surtout sous sa signature de DPO et de sa boîte email ! Il n'avait jamais été question de cela et n'en n'a pas été averti. Il fait part de sa vive surprise de voir usurpée son identité et sa qualité professionnelle. Par la suite, le DPO ne parviendra pas à savoir s'il y avait réellement violation de données et si l'association l'a notifiée à la CNIL.

Outré d'avoir été tenu à l'écart de la cellule de crise par manque de confiance à son égard, il adresse un message à la direction (qu'il n'a jamais eu l'occasion de rencontrer depuis sa désignation). En réaction, la direction demande immédiatement qu'il soit licencié. Il est aussitôt mis à pied et reçoit sa convocation pour l'entretien préalable. Lors de cet entretien, le DRH lui hurle dessus et déclare « *qu'il connait personnellement les membres des Prud'hommes et de la CNIL* ». Il est licencié pour faute grave, car il aurait accusé à tort (selon la direction) un collègue d'avoir usurpé son identité pour envoyer l'email évoqué *supra*. Le témoin tombe en dépression et est arrêté par son médecin.

Un autre témoin, également DPO interne au sein d'une ONG, a eu la surprise de constater que des courriels étaient envoyés à son insu de sa boite *mail* professionnelle, sous son nom et sa qualité de délégué à la protection des données, avec des avis de conformité positifs…

Le témoin suivant était CIL quand il a été rattaché hiérarchiquement à un nouveau cadre supérieur qui s'est avéré être un pervers narcissique. Celui-ci lui a mis une très forte pression pour le pousser au départ et empêcher qu'il ne devienne DPO dans la perspective de l'entrée en application du RGPD. De façon répétée, le témoin devait endurer des critiques ouvertes de son professionnalisme et de sa maîtrise professionnelle.

Alors que le CIL déployait son plan d'action pour préparer l'entreprise au RGPD, son *manager* a commandité un audit à un prestataire, dans l'espoir de mettre en difficulté le témoin. Espoir déçu, car ce dernier avait mis un point d'honneur à être irréprochable (procédures, documentation, plan d'action, indicateurs, comité conformité, etc.). Lors des réunions destinées à formaliser des points réguliers concernant la préparation de l'entreprise avec le RGPD, le témoin laissait s'exprimer un prestataire qu'il faisait intervenir sur son propre budget, ce qui lui permettait de ne pas constituer la « cible » du cadre harceleur. Par ailleurs, et plus que d'habitude, il a veillé à tout porter par écrit, notamment au sein de son bilan annuel.

Mois après mois, il a « *serré les dents* » et a veillé à ne laisser aucun interstice dans lequel le pervers aurait pu s'engouffrer. Il a aussi adapté son comportement pour ne pas donner prise à la posture de son harceleur : « *Les pervers narcissiques se nourrissent des réactions de leur victime. Ils cherchent à démotiver ou à faire sortir leurs cibles de leurs gonds pour jouir du pouvoir qu'ils ont sur elles. Il me fallait donc rester impassible et ne jamais céder à aucune de ses provocations* ».

C'est sa passion du métier de DPO, son éthique et sa volonté de ne pas abandonner tout ce qu'il avait bâti jusque-là qui l'ont soutenu. Il n'en reste pas moins que cette période a été pour lui très difficile à vivre. Le délégué a finalement réussi à ce que le directeur général soit informé de cette maltraitance. La direction a alors retiré le sujet « Conformité RGPD » du périmètre du *manager* pour le prendre sous son égide. Même une fois le cadre maltraitant parti de l'entreprise, il a fallu du temps au témoin pour « *baisser la garde* », cesser d'être sur le qui-vive en permanence et retrouver une posture plus normale.

« On ne va voir le DG qu'avec de bonnes nouvelles ! »

Le témoin suivant a réorienté sa carrière en considérant que l'entrée en application du RGPD lui fournissait une opportunité de reconversion. Il suit une formation courte et décroche une certification des compétences du DPO. Il obtient un poste de DPO interne, dans une entreprise qui traite des données sensibles. Avant son embauche, la conformité au RGPD de l'entreprise était prise en charge par un DPO externe (pour lequel tout était en conformité parfaite).

Le témoin était rattaché à la direction juridique et est d'emblée fortement mobilisé pour répondre aux nombreuses sollicitations des ingénieurs commerciaux et des acheteurs afin de finaliser les contrats, avec une exigence forte de réactivité. Ceci l'a tellement accaparé qu'il n'a pas pu entreprendre plusieurs des actions stratégiques que doit mener un DPO.

Dès son arrivée, on le somme de finaliser un plan stratégique pour le présenter au directeur général en un temps très court. Le nouveau DPO s'exécute et formalise un plan sans disposer du recul suffisant et en prenant des engagements précis et datés.

Quand, phagocyté par le quotidien et ne disposant d'aucune aide, il se rend compte qu'il ne lui sera pas possible de tenir les engagements figurant dans le plan qu'il a présenté au directeur général, il veut en faire part à ce dernier. Cette démarche lui est strictement interdite par son superviseur, selon lequel « *On ne va voir le DG qu'avec de bonnes nouvelles !* ».

Le témoin constate que son responsable hiérarchique est très directif vis-à-vis de lui, respectant peu l'indépendance du DPO. Ainsi, le superviseur exige qu'il mène immédiatement un audit alors que le DPO aurait préféré laisser passer plus de temps pour mener d'abord des actions de fond (comme la

sensibilisation). L'audit porte sur le respect des durées de conservation des données personnelles. Réalisé dans des conditions délicates, avec une réticence des directions sollicitées, ses conclusions ont été mal reçues (« *Le DPO nous met des bâtons dans les roues !* »).

Lors de l'un des entretiens que le DPO avait régulièrement avec son supérieur, celui-ci fait part de son insatisfaction concernant les résultats des actions menées par le témoin, qui ferait « *mal* » son travail. Le délégué reçoit à son domicile, par lettre recommandée, un « Plan d'amélioration des performances », outil sensé donner à un employé dont les résultats sont jugés insuffisants la possibilité de réussir. Ce plan lui impose une énorme pression en exigeant qu'il réalise en un temps extrêmement court des actions dont certaines ne sont pas de son ressort (comme la revue de l'intégralité d'un contrat et non pas seulement la partie relative à la conformité au RGPD) ou qui nécessite un soutien de la direction et des moyens qui n'ont jamais été mis à sa disposition (comme, par exemple, faire signer la charte de sécurité à l'intégralité des salariés).

Le DPO prend alors contact avec la CNIL, dont les représentants conviennent qu'il est impossible pour le témoin de réaliser les tâches décrites dans le plan en un temps aussi court. Malgré cela, et sur son temps personnel, le témoin réalise certaines des actions qui sont exigées, ce qui ne l'empêche pas de recevoir une lettre de convocation à un entretien préalable à son licenciement pour faute. La lettre se focalise sur le fait qu'il aurait « *refusé délibérément de faire son travail* ». Démoralisé, il ne se présente pas à cet entretien et est remercié. Quelques mois plus tard, consultant les données ouvertes publiées par la Commission[19], il constate qu'il est toujours officiellement le délégué à la protection des données de son ancien employeur, la CNIL n'ayant visiblement pas été informée de son départ.

Faux et usage de faux

Terminons cette revue au sein d'un acteur public. Le dernier témoin y travaille de longue date et est désigné CIL auprès de la CNIL. L'équipe de direction est à l'écoute du correspondant et soutient les démarches de conformité. Il sensibilise les nouveaux embauchés ainsi que le personnel en fonction. Il s'investit dans ses fonctions, bénéficie d'une aide à plein temps, anime un réseau de référents, formalise son bilan annuel et participe au comité de direction. Il suit la totalité des ateliers de la CNIL, mais une formation longue et diplômante pour renforcer ses connaissances en matière de conformité lui est refusée avec ce commentaire « *Tu crois vraiment que cela en vaut encore la peine à ton âge ?* ». Il devient DPO, car c'est une suite logique à son investissement personnel. Le témoin qualifie cette période « d'heureuse ».

Tout change quand arrive une nouvelle direction. D'emblée, celle-ci indique clairement n'accorder aucune priorité aux sujets portés par le DPO et supprime le poste de la personne qui l'épaulait. Quand le témoin fait remarquer que cela va l'obliger à réaliser le travail de deux personnes, il s'entend dire « *Estimez-vous heureux, j'aurais pu envisager de vous ajouter une fonction supplémentaire.* ». Des consignes sont données aux responsables des différents services pour n'accorder qu'un minimum de temps aux sujets portés par le témoin, dont les missions sont sacrifiées. Du fait des signaux très clairs diffusés par la direction, le réseau des référents s'étiole et perd de son efficacité. Si on l'autorise à intervenir de manière sporadique en comité de direction, on le relègue systématiquement en fin de réunion, quand le temps devient limité (« *Allez à l'essentiel !* ») et l'attention des participants pour le moins affaiblie.

Le délégué à la protection des données n'est alors quasiment jamais informé en amont des projets et est considéré comme une simple chambre d'enregistrement, dont les analyses doivent forcément aboutir à un avis positif. Il n'a pas les moyens de finaliser les PIA devant être obligatoirement accomplis. Il en entame

[19] https://www.cnil.fr/fr/opendata

plusieurs mais ne peut les terminer faute de participation des Métiers. Il est d'ailleurs présenté à eux comme « *la personne qui empêche de travailler* ».

La situation empire lors du premier confinement. Le DPO est sollicité de toute part… avant que la direction admoneste les services qui ont osé braver les consignes et contacter directement le témoin. Ils doivent dorénavant obligatoirement passer par la voie hiérarchique.

Enfin, à l'approche de contrôles de la CNIL, on lui demande de se prononcer de toute urgence sur la conformité de plusieurs traitements pour lesquels il n'avait jamais été sollicité. La direction se dit surprise d'entendre le DPO réclamer la description détaillée des traitements en question, car ce qui est attendu de lui ce sont « juste » des avis positifs – rien de plus. Sa hiérarchie lui laisse deux heures pour étudier la conformité des traitements. Sous cette forte pression, le DPO revient vers la direction avec un avis réservé sur la moitié des traitements qui lui ont été soumis (en réalité, il aurait souhaité prononcer un avis négatif). Il reçoit alors simultanément un appel de son responsable hiérarchique, un SMS de la grande direction et un appel du secrétariat de cette dernière, l'informant de sa convocation à une réunion l'après-midi même.

Le délégué pressentait qu'il s'agissait probablement d'une réunion « piège » au cours de laquelle il lui serait demandé de « verdir » ses avis. Déjà pris par un engagement, le DPO décline « l'invitation » et consulte son médecin qui le met en arrêt maladie et l'aiguille vers un psychiatre. Ce dernier diagnostique un *burnout* (anxio-dépressivité sévère). Le soir même, à son domicile, il apprend par un collègue que ses analyses, qui portent toujours son nom, font désormais état d'une conformité parfaite au RGPD.

Ce témoin se dit touché dans ses valeurs et sa dignité : « *Ce qui m'était demandé allait à l'encontre de ma déontologie, ce qui m'a conduit à l'épuisement professionnel. Le fond a été atteint lorsque mon supérieur a falsifié mes analyses de conformité tout en y laissant figurer mon nom.* ». Le CHSCT s'est montré à l'écoute mais s'est heurté à un refus des salariés de témoigner en faveur du DPO, par crainte de représailles de la part de la direction. Le témoin est resté plus de deux ans en arrêt de travail avant d'être licencié, après plus de quarante ans d'ancienneté et à quelques années de la retraite. Inscrit à Pôle Emploi, il travaille quelques heures par semaine dans un commerce de proximité, à l'opposé de ses précédentes missions.

Exit, le *Privacy by Design* !

Ajoutons à ces témoignages le seul cas dont la presse s'est faite l'écho. Aux Pays-Bas, une tension entre un responsable de traitement et son délégué à la protection des données a été rendu publique récemment : elle a opposé l'Université d'Utrecht à M. Artan Jacquet. C'est à l'occasion du départ négocié du délégué à la protection des données (après que l'Université a envisagé de le licencier), début 2023, que les causes en sont apparues[20].

Au début, M. Jacquet (qui travaillait au préalable au sein du service Ressources humaines de l'Université) s'est épanoui dans ce rôle de porte-drapeau de la vie privée, organisant de nombreuses réunions d'information au cours desquelles des centaines d'employés ont appris ce que le RGPD signifiait pour eux. Mais, au fil du temps, certains administrateurs de l'Université et directeurs de service ont commencé à ne pas apprécier ses analyses et conseils concernant des projets dans lesquels un traitement de données à caractère personnel était en jeu. Le fait que le DPD ait communiqué son avis au Conseil d'administration de l'Université avant même que le Bureau exécutif n'ait pu prendre une décision sur l'un de ces projets semble avoir mis le feu aux poudres. Cette initiative a été perçue comme une entrave au processus de prise de décision. Pour Artan Jacquet, « *Il semble que le conseil d'administration préférerait ne pas entendre de ma bouche que l'institution s'apprêtait à ne pas respecter les règles. Le fait de ne pas être totalement conforme n'est pas une honte en soi. De*

[20] *Data Protection Officer Artan Jacquet left Utrecht University this month after a long legal battle,* par Xander Bronkhorst, DUB, 23 février 2023 https://dub.uu.nl/en/depth/why-independent-supervisor-had-leave-uu

nombreuses institutions ne le sont pas. Mais il faut alors expliquer comment on compte améliorer les choses. En revanche, en tant que délégué à la protection des données, je suis un superviseur, pas un réparateur. ». Mis sous pression, M. Jacquet n'a pas cédé le moindre pouce, soutenu par ses homologues désignés au sein d'autres universités et institutions du pays, ainsi que par l'Autorité des données personnelles néerlandaise.

Selon M. Jacquet, la confrontation est encore montée d'un cran lorsque la direction a cherché à inclure dans son dossier la plainte formulée par le directeur d'un service de l'Université, en désaccord avec l'une de ses analyses de conformité. En outre, M. Jacquet nie avoir eu un comportement inapproprié à l'égard du directeur en question ou d'autres employés de l'université. « *Avant de devenir DPD, mes évaluations annuelles toujours bonnes et je n'ai jamais reçu de commentaires négatifs sur ma façon de communiquer* ». De plus, sa personnalité décrite par beaucoup comme aimable lui a permis d'être en bons termes avec presque tous les membres de l'université. Son pot de départ en est l'illustration : même le recteur de l'Université n'a eu que des mots d'appréciation à son égard. Finalement, pour éviter une bataille juridique longue et couteuse, les deux parties ont décidé d'un accord de départ.

Une nouvelle politique de protection de la vie privée au sein de l'université a été élaborée. Le DPD sortant, M. Jacquet, s'en félicite car le document aborde deux sujets sur lesquels il avait insisté : la sensibilisation des personnels et une meilleure définition des responsabilités de chacun. En revanche, il est en désaccord total avec un aspect clé de la nouvelle politique qui veut que le délégué à la protection des données ne peut plus désormais que juger *rétrospectivement* si la conception d'un projet était conforme au RGPD ! Le DPD n'est donc plus censé donner des conseils à un stade précoce d'un projet. Pour M. Jacquet, cette situation n'est pas conforme au principe de *Privacy by Design* et à ce que devrait être le rôle d'un délégué. Selon lui, fournir des conseils en temps opportun afin que des ajustements puissent être effectués en amont fait tout simplement partie des obligations légales. « *Cela démontre que la direction souhaite maintenir le DPD à distance. Il ne reste plus à mon successeur qu'une position de croquemitaine : il ne peut formuler une analyse négative qu'a posteriori* ». Pour le recteur, qui a une perception particulière du rôle du délégué à la protection des données, « *Nous ne sommes pas d'accord pour dire que le DPD doit toujours être impliqué et être au courant de tout dès le début des projets* ». La réaction de l'autorité néerlandaise est attendue avec impatience.

Essayons désormais d'analyser ces témoignages au regard des exigences du RGPD.

Partie II - Analyse des témoignages

La présente étude étant qualitative, il n'est pas tenté de tirer la moindre estimation chiffrée des interviews recueillies. Par ailleurs il est pris soin de ne pas confondre les situations habituelles de conflits au sein des entreprises (les causes de friction ne manquent jamais dans le milieu professionnel, personne ne pouvant être du même avis en permanence) et les situations anormales décrites par plusieurs témoins.

Une première tentative d'analyse

Remarquons tout d'abord qu'à part un cas dans lequel le DPO a fait face et est resté en poste, toutes les situations se sont terminées au désavantage du témoin (On ne peut réagir que de quatre manières face à une situation oppressante : partir, se « décaler » - par exemple en prenant une autre fonction au sein de l'organisme-, accepter et subir, se défendre- voire attaquer en justice).

Dans la quasi-totalité des cas, le harcèlement était vertical : c'est le supérieur direct qui s'est rendu coupable d'agissements hostiles dont certains, pris isolément, pourraient sembler anodins, mais dont la répétition a eu des effets pernicieux. Pour quelques témoins, la direction a explicitement soutenu la démarche. Dans les autres cas, la non-intervention face à de tels agissements a le même effet qu'une autorisation : qui ne dit mot consent. Le seul cas positif dans lequel la grande direction a écarté le pervers narcissique démontre qu'il est pourtant possible de procéder autrement. Plusieurs témoins ont également souffert d'une composante

horizontale, quand quelques directions métiers renforcent la pression ou participent au dénigrement du DPO (« *Rends toi compte, tu n'es même pas juriste !* »). À l'inverse, pour quelques témoins, les relations de confiance qu'ils avaient réussi à tisser avec les autres salariés leur ont permis de tenir plus longtemps.

Plusieurs des agissements caractéristiques du harcèlement sont présents dans les témoignages recueillis. Ainsi en est-il du dénigrement des victimes et la critique de leur travail (« *Tu es un centre de coût, non rentable* », « *Voilà encore l'oiseau de mauvais augure* », « *Tu nous mets des bâtons dans les roues* », « *Le DPO, la personne qui empêche les autres de travailler* »). L'attitude du supérieur qui passe son temps ostensiblement à se prendre en photo pendant que le délégué tente d'obtenir l'attention des membres du comité de direction afin de les intéresser à ses missions est également à classer parmi ces pratiques. C'est peut-être même la pire, la manifestation du mépris étant alors publique. Mais que dire de l'agression, comme dans le cas du témoin qui a dû essuyer les insultes proférées par un responsable juridique ? Un témoin s'est dit choqué de l'attitude de ses *managers*, dont l'un a été jusqu'à lui demander s'il était juif. « *Et pourquoi cette question ?* » - « *Parce que tu négocies tout comme un juif !* ».

Pour plusieurs des professionnels interviewés, ce travail de sape a fini par miner la confiance en eux (« *À force d'entendre des critiques permanentes sur mes actions et mes analyses, j'avais fini par me dire qu'ils avaient peut-être raison…* »). Même une personne sûre d'elle-même peut être déstabilisée et finir par s'autodéprécier. Comme on l'a vu, l'un des témoins s'est d'ailleurs empressé de décrocher la certification des compétences du DPO peu après son départ pour se rassurer de ce point de vue. Le manque d'écoute, de reconnaissance, de soutien est également fréquent (« *Est-ce que ce que je fais intéresse quelqu'un au sein de l'entreprise ? »).*

Le syndrome du « mauvais coucheur » se retrouve également à plusieurs reprises. On reproche au délégué d'ergoter, de ne pas être aussi compréhensif que son prédécesseur, bref, on veut faire croire à la personne que *c'est elle* la source du conflit (« *Vous inventez des problèmes… Vous êtes le problème* »).

Des DPO mis en quarantaine

L'isolement du DPO est également mis en œuvre. Il peut être vis-à-vis du responsable de traitement, matérialisé par l'interdiction de s'adresser au Président Directeur Général ou la réticence du DGS quand le délégué l'informe de son intention de rencontrer les élus (Le « *On ne va voir le DG qu'avec de bonnes nouvelles !* » appartient à la même famille). On peut aussi couper le DPO des métiers, à qui l'on interdit de communiquer avec le témoin. Par le passé, l'auteur avait recueilli auprès d'un Correspondant Informatique et Libertés l'anecdote suivante : pour éviter que les salariés aillent le voir pour l'informer des nouveaux projets et, éventuellement, lui signaler des non-conformités, on avait déplacé son bureau au sein du service informatique... protégé par un contrôle d'accès physique qui pouvait uniquement être franchi par les membres de la DSI. Des cas d'isolement du délégué à la protection des données vis-à-vis de ses anciens collègues (en cas de promotion interne) ont même été identifiés : interdiction de discuter avec lui, considéré désormais comme un « traitre » en puissance (au service de la CNIL). L'isolement est renforcé quand le DPO n'est plus informé (et encore moins convié) aux réunions clés et ne reçoit plus d'information.

Dans plusieurs témoignages, on identifie la pratique qui consiste à museler le délégué, notamment en lui interdisant de formuler des analyses écrites – et encore moins de les diffuser en interne !

On cherche également à écraser le délégué à la protection des données sous une très forte charge : « *Toujours sur le pont, j'avais des horaires de dingue…* », « *J'étais obligé de prendre sur mon temps personnel* », « *Il m'est arrivé de faire des semaines de quatre-vingt heures* ». La remarque du supérieur qui enjoint le délégué de s'estimer heureux (après lui avoir retiré une aide) en lui disant « *J'aurais pu envisager de vous ajouter une fonction supplémentaire.* » est emblématique, de même que le temps extrêmement court laissé au délégué à la protection des données à qui on laisse une dernière chance avec un « Plan d'amélioration des performances » impossible à satisfaire. L'un des témoins se refuse désormais à travailler à son domicile : « *Je ne veux plus d'ondes négatives chez moi – elles*

doivent rester au bureau ». Il se montre critique envers l'excès du recours au télétravail pour un DPO interne : « *Rien ne vaut le contact pour détecter les signaux faibles et échanger avec les opérationnels* ». En revanche, pour pouvoir se concentrer sur certains dossiers, l'entreprise devrait pouvoir lui mettre à disposition un lieu pour s'isoler et ne pas être interrompu.

Remarquons que plusieurs superviseurs toxiques enferment le DPO dans une impossible équation : ceux-ci doivent – seuls, sans aucune aide ni soutien et sans jamais perturber les autres salariés – amener l'organisme à un niveau nominal de conformité au RGPD : « *Alors ? Nous ne sommes pas encore totalement conformes ? Comment cela est-ce possible ?* ». Une contradiction similaire est observée quand la direction exige que le délégué à la protection des données détermine lui-même les solutions … mais s'insurge quand le DPO formule des recommandations (« *Tu ne vas tout de même pas nous apprendre notre métier et nous dire quoi faire !* »).

Plusieurs témoignages font état de pressions pour que le DPO modifie ses avis. Ces menaces plus ou moins voilées semblent efficaces, car certains témoins avouent s'être autocensurés à plusieurs reprises. Dans les cas extrêmes, l'encadrement va jusqu'à falsifier les documents, mais en en laissant la paternité au délégué à la protection des données.

Des relations qui empirent rapidement

Nous observons, dans les témoignages recueillis, des différences quant à la vitesse avec laquelle la situation se dégrade. Dans la majorité des cas, le voile de fumée s'évapore rapidement et la vérité nue s'impose au DPO. Mais, dans d'autres circonstances, le changement intervient plus tard, lors de l'arrivée d'un nouveau supérieur hiérarchique ou de façon progressive. On passe ainsi du « *C'est assez pénible d'avoir été obligé de désigner un DPO* » à « *Nous devons trouver un moyen économique de nous en débarrasser* » en passant par « *Il n'est pas fait pour travailler avec nous !* ». Souvent, deux situations mettent le feu aux poudres : les violations de données qu'il faut notifier et la réalisation de PIA honnêtes. Concernant la première, on relèvera les propos qu'a tenu Giuseppe d'Acquisto lors de la conférence « *EDPS-ENISA Conference: Towards assessing the risk in personal data breaches* » le 4 avril 2019[21] : « *For notification we need very skilled and authoritative DPOs* ».

Minoritaires sont les témoins qui ont pu rencontrer le responsable de traitement lors de leur prise de poste ou peu de temps après. Précisons que certains n'ont pas essayé, ce qui fait que le premier conflit majeur constituait la première interaction avec la grande direction. Le cas le plus marquant est celui du directeur général qui, à la réception du tout premier message que lui adresse son délégué demande immédiatement à ce qu'il soit licencié. Encore plus rares sont les témoins qui ont formalisé un véritable plan stratégique, comportant un état des lieux, des objectifs et des priorités, une feuille de route et un plan d'action. Un seul d'entre eux bénéficiait d'une lettre de mission. De même, un seul a tenté de faire signer au responsable de traitement la charte de déontologie du DPO[22] (sans succès).

Seuls quatre des témoins prenaient soin de rédiger un bilan annuel du délégué (nous reviendrons également *infra* sur ce point). Force est de constater que ces documents n'intéressaient visiblement pas les responsables de traitement, auxquels pourtant ils étaient destinés. Comme on l'a vu, dans un cas, sa présentation a donné l'occasion au dirigeant de laisser éclater sa colère et d'obliger le DPO à modifier ses écrits.

Le rôle des services de gestion des ressources humaines laisse également songeur. Celui qui a clairement indiqué au DPO venu demander son aide que, de toute façon, « *son compte était bon* » a-t-il oublié que le Code

[21] « *Pour la notification des violations, nous avons besoin de DPO très compétents et sachant s'imposer* »
https://www.enisa.europa.eu/events/edps-enisa-conference/giuseppe-dacquisto-italian-dpa
[22] La Charte de déontologie du DPO, librement accessible sur le site web de l'AFCDP (https://afcdp.net/charte-de-deontologie-du-dpo/), doit également être signée par le responsable de traitement.

du travail stipule, dans son article L. 4121–1[23] que l'employeur a l'obligation de préserver la sécurité et la santé de ses travailleurs ? Les représentants du personnel n'ont pas non plus été d'une grande aide. Dans un cas, l'un d'entre eux qui a assisté le délégué à la protection des données mis sur la sellette et qui l'a vraiment soutenu lors de l'entretien préalable, n'a plus donné signe de vie alors qu'il s'était engagé à fournir un témoignage écrit.

Dans le cadre de l'intervention de Lucy Savary (déléguée à la protection des données mutualisée) intitulée « *Guide de survie du DPO : comment (re) trouver du temps pour l'essentiel ?* » et dispensée lors de l'Université AFCDP 2023 des DPO, un sondage préparatoire avait été proposé aux DPO internes membres de l'association. À la question « *Dans l'exercice de vos fonctions, quelle est la pire difficulté que vous ayez rencontrée* ? », on trouve des réponses qui entrent en résonnance avec les situations décrites par les témoins : « *Je travaille dans une ambiance permanente de défiance et de confrontation* », « *Des considérations politiques et hiérarchique entravent mes actions en tant que DPO* », « *Mon superviseur empêche l'information de remonter. Et quand il le fait, il arrive qu'elle soit biaisée et faussée* », « *Dès que mon responsable de traitement ne partage pas l'une de mes analyses de conformité, je sens son hostilité croître* », « *Mon métier de DPO perd tout sens, car la conformité est impossible à appliquer dans notre structure* », « *On remet en cause systématiquement tout ce que je dis : c'est usant, fatigant* ».

Des DPO victimes d'épuisement professionnel

Dans douze cas, on observe des impacts sur la santé des témoins : arrêt maladie, dépression, *burnout*, suivi psychologique et médical, épuisement professionnel, sont les termes utilisés par les témoins. Ce sont généralement les cas où l'on observe l'accumulation de plusieurs facteurs évoqués *supra* et sur une longue période.

Le *burnout* figure dans la classification internationale des maladies de l'Organisation Mondiale de la Santé dans le chapitre qui liste les facteurs impliquant un recours aux services de santé. Il est considéré comme un syndrome lié à un stress chronique au travail. Dans leur livre *« The Truth About Burnout: How Organizations Cause Personal Stress and What to Do About It*[24] », Christina Maslach et Michael Leiter décrivent le burnout au travers de « *l'écartèlement entre ce que les gens sont et ce qu'ils doivent faire. Il représente une érosion des valeurs, de la dignité, de l'esprit et de la volonté – une érosion de l'âme humaine. C'est une souffrance qui se renforce progressivement et continûment, aspirant le sujet dans une spirale descendante dont il est difficile de s'extraire...* ». Il n'est pas étonnant de constater que ces témoins ont subi sur une période relativement longue la situation malsaine qui leur était imposée. Ajoutons que la plupart d'entre eux n'ont été en mesure de se rendre compte de leur état que bien trop tard : dans un cas, nous l'avons vu, c'est à son arrivée dans son poste suivant que le témoin a craqué. À l'inverse, aucun des témoins qui ont quitté rapidement leur employeur, de façon volontaire ou contrainte, n'a fait part de signes cliniques.

C'est dans les années 1980 que Heinz Leymann, psychosociologue allemand, chercheur à l'université de Stockholm, a formalisé la notion de harcèlement moral[25] : « *Cela désigne une relation conflictuelle sur le lieu de travail, aussi bien entre collègues qu'entre supérieurs et subordonnés. La personne harcelée – la victime – est agressée de façon répétitive sur une période de six mois au moins, le but étant de l'exclure* ». Il précise la notion : « *Toute conduite abusive se manifestant notamment par des comportements, des actes, des gestes, des écrits unilatéraux, de nature à porter atteinte à la personnalité, à la dignité ou à l'intégrité physique ou psychique d'une personne et à mettre en péril son emploi ou à dégrader le*

[23] « *L'employeur prend les mesures nécessaires pour assurer la sécurité et protéger la santé physique et mentale des travailleurs. Ces mesures comprennent : 1° Des actions de prévention des risques professionnels, y compris ceux mentionnés à l'article L. 4161-1 ; 2° Des actions d'information et de formation ; 3° La mise en place d'une organisation et de moyens adaptés. L'employeur veille à l'adaptation de ces mesures pour tenir compte du changement des circonstances et tendre à l'amélioration des situations existantes.* »

[24] Paru en français sous le titre *Burn-out. Le syndrome d'épuisement professionnel*, Les Arènes, 2011

[25] C'est dans un livre écrit en 1998, *Le Harcèlement moral. La Violence perverse au quotidien*, que la psychologue Marie-France Hirigoyen utilise pour la première fois en France le terme de « harcèlement moral ».

climat de travail ». Son ouvrage principal, « *Mobbing. Psychoterror am Arbeitplatz une wie mann sich dagegen wehren kann* », est disponible en français sous le titre « La persécution au travail » (Seuil, 2002).

On retrouve dans les témoignages des signes de ce que Maslach et Leiter appellent des « discordances majeures », des conflits de valeurs, dans plusieurs témoignages de personnes à qui les tâches confiées contraires à leur éthique ou à leurs valeurs personnelles, et les conduit même à douter de l'utilité du travail accompli : « *Mon travail a-t-il un sens ?* », « *Mon univers s'est effondré… cette hypothèse était pour moi inconcevable* », « *Ce qui m'était demandé allait à l'encontre de ma déontologie* », « *Il aurait fallu que je sois un béni-oui-oui en permanence, mais cela m'était impossible. Certes, dans ce métier il faut savoir accepter une certaine dose de frustration, mais là, c'était trop* ». Le *burnout* touche souvent les personnes qui ont de fortes attentes envers leur travail : ce qui est déterminant pour elles, c'est le métier et le sens donné à leur mission. Elles croient à la plus-value qu'elles apportent à leur organisme. Ce sont de bons petits soldats, impliqués, enthousiastes et talentueux, mais qui n'ont pas vu, ou pas voulu voir, qu'ils en faisaient trop aux yeux de leur hiérarchie. Et plus l'émotion au travail est importante, plus la personne y met de l'affect, plus elle se sent stressée quand les choses ne vont pas comme elle le voudrait. En cela, les délégués à la protection des données sont particulièrement exposés au *burnout*.

Au final, les employeurs ont eu gain de cause

Remarquons également que le sujet même qui était à l'origine du conflit (la conformité de l'entreprise ou de l'organisme au RGPD) n'est (et ne devient) jamais un sujet pour l'employeur. Selon les témoins qui sont restés en contact avec leurs anciens collègues, ces responsables de traitement ont continué à ignorer superbement les règles en la matière, en l'absence de contrôle et de sanction de l'autorité compétente. Après le départ du témoin, un autre salarié à l'échine plus souple ou un DPO externe a été désigné auprès de la Commission Nationale de l'Informatique et des Libertés. Dans plusieurs cas, la personne licenciée reste officiellement désignée, son départ n'étant pas signalé à l'autorité.

Reste l'inconfortable impression que ces acteurs ont finalement eu raison… Jamais l'existence de la CNIL et l'utilisation de ses éventuels pouvoirs ne semblent avoir été pris en compte. Certaines déclarations laissent même penser le contraire (« *J'en n'ai rien à foutre de la CNIL... et de toute façon, le risque de contrôle est très faible* », « *De toute façon, je connais personnellement l'un des Commissaires de la CNIL…* », « *Je connais les membres des Prud'hommes et de la CNIL* ») ou le cas du superviseur qui retient surtout une publication de la CNIL qui dit en substance que l'Autorité se montrera magnanime durant les premières années suivant l'entrée en application du RGPD.

Pourtant les infractions au RGPD sont multiples. Par référence aux articles 37 à 39 du règlement européen, on relève une absence de désignation du délégué à la protection des données, l'incapacité à accomplir ses missions dans laquelle sont placés les témoins, le fait que le DPO ne soit pas « *associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel* », l'absence d'aide et des « *ressources nécessaires* » pour permettre au DPO d'exercer efficacement ses missions, le non-respect de l'indépendance du délégué (qui ne doit pas recevoir d'instruction qui « *est à l'abri d'influences guidées par des intérêts divergents, de nature à altérer la liberté de ses positionnements*[26] »), l'impossibilité pour le DPO de faire directement rapport au niveau le plus élevé de la direction[27], l'impossibilité pour le délégué de réellement vérifier le respect du RGPD et l'impossibilité pour lui de « *coopérer avec l'autorité de contrôle* » (*a minima*, d'interagir avec la CNIL).

Sur ce dernier point, on rappellera que les lignes directrices concernant les délégués à la protection des données du CEPD indiquent en leur page 18 que « *les DPD ne doivent pas recevoir d'instructions sur la façon de*

[26] Cf. *Guide pratique RGPD - Délégué à la Protection des Données* de la CNIL

[27] « *Le DPO doit également être en capacité de s'adresser directement au niveau le plus élevé sur une problématique spécifique s'il l'estime nécessaire* » - Source : *Guide pratique RGPD - Délégué à la Protection des Données* de la CNIL

traiter une affaire, par exemple, quel résultat devrait être obtenu, comment enquêter sur une plainte ou s'il y a lieu de consulter l'autorité de contrôle. ». Dans son *Guide pratique RGPD - Délégué à la Protection des Données*, la CNIL précise « *Par ailleurs, le DPO peut consulter la CNIL sur toutes questions ayant rapport avec la protection des données personnelles ou sa fonction. Il est interdit au responsable de traitement ou au sous-traitant de soumettre ces questions à sa validation ou de les prohiber* ».

Le cas où le délégué avait été soigneusement tenu à l'écart d'un incident de sécurité qui impactait des données personnelles amène à rappeler un passage du *Guide du DPO* de la CNIL : « *Il est essentiel que le délégué ou, le cas échéant, son équipe, soit associé le plus tôt possible à toutes les questions relatives à la protection des données. À titre d'exemple, l'organisme veille notamment à ce que le DPO soit immédiatement consulté lorsqu'une violation de données se produit* ».

Seuls quatre témoins ont pris contact avec la CNIL pour faire part de leurs difficultés. Le premier a envoyé à la Commission une description factuelle de sa situation : « *Par précaution, outre mes échanges avec mon avocat, j'ai pris la précaution de déposer une sorte de main-courante auprès de la CNIL* ». Les trois autres témoins, qui ont clairement informé l'autorité de leur situation intenable et des non-conformités constatées, se disent déçus de l'inaction de la Commission : « *Certes, on m'a prêté une oreille compatissante, mais il n'y a pas eu de suite et je n'ai pas connaissance d'actions concrètes* ». La mise en œuvre par la CNIL, en novembre 2022, d'un dispositif spécifique pour recueillir et traiter les signalements des lanceurs d'alerte[28], pourra-t-elle changer les choses ? Ce dispositif fait suite à la publication du décret du 3 octobre 2022 visant à améliorer la protection des lanceurs d'alerte. La CNIL y figurait, aux côtés de quarante autres autorités compétentes pour recueillir et traiter les signalements externes émanant de lanceurs d'alertes et relevant de leurs champs de compétences respectifs. Nous reviendrons *infra* sur cette nouveauté. Sans surprise, les témoins sont unanimes pour regretter que la CNIL ne soit pas davantage crainte par les entreprises : « *Dans le secteur bancaire, l'ACPR[29] va jusqu'à retirer l'accréditation de l'établissement. C'est autrement plus dissuasif que les sanctions pécuniaires de la CNIL* ».

Le sentiment d'impunité des responsables de traitement concernés se renforce quand on constate que seuls quatre des témoins ont saisi les prud'hommes. Trois des instances sont pendantes à ce jour. Le quatrième témoin a été débouté (mais a fait appel). Devant les prud'hommes, son avocat commence par indiquer qu'il ne connait pas bien la fonction de DPO… et se voit immédiatement couper la parole par le Président : « *Comment osez-vous vous présenter à moi si vous n'avez pas travaillé votre dossier ?* ». Le témoin se propose alors de présenter rapidement son métier. Le Président ne lui donne pas la parole et lève la séance. Au bout d'un délibéré de quelques minutes, le délégué est débouté. Notons que deux des témoins ont pris soin d'échanger très tôt avec leur avocat, ce qui leur a permis d'obtenir une rupture conventionnelle et qu'un autre témoin attend encore que la CNIL prenne action : « *Dès que la CNIL aura contrôlé et sanctionné mon ancien employeur, je pourrai alors porter mon cas devant la justice* ». Un dernier indique avoir souhaité porter le litige devant la justice, mais y a renoncé, faute d'avoir pris la précaution de conserver les écrits nécessaires.

Un retour difficile à la vie normale

Tous les témoins disent avoir eu (ou connaître encore) des difficultés pour rebondir professionnellement. Que faire figurer dans son *curriculum vitae* ? Que dire lors des entretiens d'embauche ? Quelle sera la réaction de l'ancien employeur en cas de prise de références ? Comment faire à nouveau confiance à un autre employeur ?

Dégoutés, deux témoins ont rayé de leur plan de carrière le métier de délégué à la protection des données. Cinq d'entre eux sont encore au chômage : l'un des témoins, encore traumatisé, indique « *se donner encore le temps avant de se sentir en état de reprendre un poste de DP*O ». Un autre a déjà refusé deux propositions : « *La*

[28] https://www.cnil.fr/fr/lanceurs-dalerte-adresser-une-alerte-la-cnil
[29] Autorité de contrôle prudentiel et de résolution, institution intégrée à la Banque de France, chargée de la surveillance de l'activité des banques et des assurances en France.

première fois, j'ai senti une réticence quand j'ai demandé à pouvoir échanger avec le DPO que j'aurai dû remplacer. La seconde fois, les moyens étaient franchement sous-dimensionnés. Bref, je me montre beaucoup plus exigeant désormais ». Deux témoins se sont mis à leur compte en tant que consultants RGPD et quatre autres ont rejoint des cabinets conseil. Un témoin est désormais assistant d'un délégué interne, dans une fonction de juriste, ce qu'il trouve moins exigeant : « *Aucun affect dans mon nouveau poste, ma mission étant focalisée sur les contrats. Aucun débat, plus rien de subjectif…* ». Seules trois personnes ont retrouvé un poste de DPO interne. L'un d'entre eux déclare « *J'ai pu intégrer une entreprise au sein de laquelle je peux enfin exercer mes missions de DPO interne dans de saines conditions. La société n'étant pas cotée en Bourse, elle n'est pas court-termiste et donne la priorité à la création de valeurs pérennes. À titre d'exemple, je peux enfin donner une réalité au concept de Privacy by Design !* ». Un autre ajoute « *Je bénéficie enfin d'un encadrement de qualité qui soutient mes actions* ».

Le fait d'avoir attaqué aux prud'hommes son ancien employeur constitue-t-il un handicap pour la suite de sa carrière ? De façon assez surprenante, l'un des témoins s'est entendu donner le conseil suivant, proféré par un consultant RGPD : « *Un DPO ne doit jamais porter plainte contre son responsable de traitement s'il veut continuer à travailler dans ce secteur* ».

Une décision qui a ému les DPO internes

Malgré ses démarches, l'auteur n'a malheureusement pas réussi à recueillir le témoignage de la déléguée à la protection des données qui, après avoir été licenciée, a interjeté une requête auprès du Conseil d'Etat pour obtenir l'annulation, pour excès de pouvoir, de la décision de la CNIL clôturant sa plainte dirigée contre son ancien employeur. La requête a été rejetée (Décision n° 459254 du 21 octobre 2022[30]). Il parait délicat de tirer des enseignements de ce cas sans avoir connaissance de l'ensemble des éléments, c'est-à-dire du contenu de la requête initiale, du mémoire complémentaire et des trois mémoires en réplique. Les rares informations contenues dans la décision du Conseil d'État ne sont en effet que le reflet de la position de l'employeur.

Celui-ci motivait le licenciement de son DPO interne sur *« l'absence de production d'une feuille de route demandée* », « *des alertes répétées de non-conformité* [de la part de la déléguée] *non motivées et non documentées* », « *une absence de réponse aux sollicitations des salariés de la société* », « *une absence de disponibilité délibérée* » et « *un non-respect de processus internes à la société, consistant notamment à s'affranchir des chaînes hiérarchiques en s'adressant directement aux collaborateurs d'une équipe sans l'aval du chef de celle-ci* ». Regrettant à nouveau de n'avoir pu obtenir auprès de la personne concernée sa version des faits, l'auteur ne peut que rapprocher ces griefs des situations observées dans les cas commentés *supra*.

Ainsi, on a vu qu'il est possible de surcharger de travail un DPO de façon à ce qu'il lui soit difficile de répondre rapidement aux sollicitations. De même, on peut exiger la production immédiate d'un document (comme une feuille de route) dont la conception demande normalement un certain délai. Et nous aurions été curieux de savoir à quoi ressemblait les « *alertes de non-conformité non motivées et non-documentées* » pour émettre une opinion.

Et que dire de la quasi-interdiction pour le DPO d'interagir directement avec les opérationnels ? Nous avons vu dans plusieurs des témoignages recueillis que l'objectif visé était bien de gêner le délégué dans ses missions. Aussi, il est étonnant de constater que la CNIL ne semble y a avoir vu là aucune atteinte à l'autonomie du délégué à la protection des données. Pourtant, les articles 38.3 du RGPD[31], le considérant 97 du Règlement (qui indique clairement que les DPO, « *qu'ils soient ou non des employés du responsable du*

[30] www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-10-21/459254

[31] « *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.* »

traitement, devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance ») et le chapitre 3.3 des lignes directrices du G29[32] (endossées par le CEPD) semblent assez clairs à ce sujet[33].

Et la DPO n'a-t-elle pas été acculée à essayer de collecter directement auprès des opérationnels des réponses qui lui étaient indispensables pour satisfaire sa direction ? Peut-être avait-elle essuyé plusieurs refus à ses demandes formulées auprès des directeurs Métiers concernés ? Il a été relevé dans les témoignages commentés *supra* des situations de ce type, dans lesquelles le délégué est mis dans une situation intenable et dont l'issue lui sera forcément préjudiciable. Cela vient en contradiction avec la recommandation que formule la CNIL dans son *Guide pratique RGPD - Délégué à la Protection des Données* : « *Il* [le DPO] *ne doit pas travailler en vase clos, mais être pleinement intégré aux activités opérationnelles de son organisme* ».

On apprend également que, d'après l'employeur, « *d'importantes ressources humaines et opérationnelles ont été octroyées à Mme C..., dont une équipe de trois collaborateurs et un budget d'intervention important dont elle décidait de l'affectation, qu'elle exerçait ses fonctions de délégué à temps complet et à titre exclusif, et animait un comité de pilotage de la protection des données à caractère personnel réunissant des cadres dirigeants.* ». Là encore, il est difficile d'en tirer des conclusions sans disposer de l'ensemble des éléments. Les ressources humaines et le budget dont il est question étaient-ils en adéquation avec les besoins réels ? Et un délégué à la protection des données peut très bien animer un comité sans qu'il n'en ressorte grand-chose.

Force est de constater que cette décision a fait grand bruit au sein de la communauté des DPO internes, qui se montrent critiques envers la CNIL : « *Il y a une dizaine d'années, la CNIL avait déjà mis la tête des Correspondants Informatique et Libertés sous l'eau quand elle avait infligé une sanction d'un euro à un responsable de traitement*[34]*. Son absence de soutien d'un DPO interne va laisser des traces...* », « *Si l'objectif était d'indiquer aux employeurs qu'ils peuvent facilement se débarrasser d'un DPO trop zélé, c'est réussi ! Et avec le soutien de la CNIL par-dessus le marché* », « *Avec cette décision, on vient de simplifier le process pour se débarrasser d'un DPO facilement alors même que cette fonction Compliance est souvent regardée d'un œil torve par des responsables de traitement qui sont obligés de s'en doter* », « *Je suis très inquiet pour la stabilité, la crédibilité et l'indépendance de notre fonction* ». Il aurait été utile que la Commission Nationale de l'Informatique et des Libertés apporte quelques lumières sur cette décision qui n'est pas de nature à conforter les DPO internes dans leur position déjà souvent délicate.

Partie III - Les causes sources

Essayons maintenant de lister les causes à l'origine de ces situations. Indubitablement, elles sont imputables aux responsables de traitement pour une très large part. La quasi-obligation qu'a imposée le RGPD de désigner un délégué à la protection des données (alors que la nomination de son prédécesseur, le Correspondant Informatique et Libertés, était facultative, c'est-à-dire volontaire) explique sans doute l'attitude des organismes qui ont mené la vie dure à leur DPO (mais ne l'excuse pas).

---

[32] WP 243, *Lignes directrices concernant les délégués à la protection des données*, adoptées le 13 décembre 2016 - Version révisée et adoptée le 5 avril 2017

[33] De plus, à la page 136 du document *The DPO Handbook* publié en juillet 2019, on trouve une liste de bonnes pratiques pouvant assurer l'indépendance du délégué. Parmi elles, on relève « *Des règles devraient être mises en place au sein de l'organisation pour garantir l'obligation de tous les membres du personnel de coopérer avec le DPD sans avoir à attendre un ordre ou une autorisation de leur supérieur* ». *The DPO Handbook*, rédigé par Douwe Korff et Marie Georges, a été financé par l'Union européenne et préparé dans le cadre du matériel de formation du programme de formation des formateurs *T4DATA*. https://azop.hr/wp-content/uploads/2021/01/the-dpo-_handbook_-t4data.pdf

[34] En janvier 2014, la formation restreinte de la CNIL avait, par sa délibération 2014-040 du 29 janvier 2014, infligé une sanction pécuniaire d'un euro à l'Association française des urbanistes, ce qui avait mis en difficulté plusieurs Correspondants Informatique et Libertés dont les recommandations devenaient inaudibles auprès de leurs directions (https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000028711033)

On constate que, souvent, c'est l'encadrement immédiat du DPO qui est défaillant : « *Les employés ne quittent pas l'entreprise, ils fuient leurs managers*[35] ». Il est vrai qu'un délégué à la protection des données interne est un salarié qui présente deux particularités qui nécessitent un style de management adapté : c'est un travailleur intellectuel et il bénéficie d'une indépendance par le fait du RGPD (sans être pour autant un salarié protégé). Il n'est donc pas rare de voir des cadres se trouvant devant un DPO qui leur a été confié comme une poule devant un couteau… et qui commettent envers eux toutes les erreurs possibles : Ils leur dénient toute autonomie, ne respectent pas le domaine, ce qui peut aller du désintérêt poli jusqu'au *« Le RGPD, je n'en n'ai rien à foutre !»* évoqué *supra*. De plus, n'ayant aucune idée de la complexité du sujet et des efforts à consentir, ils exigent des résultats très rapides de la part du DPO, mais sans lui apporter le moindre soutien, écoute ou moyen.

Il serait bon que ces *managers* relisent Peter Drucker. Par exemple, dans son livre intitulé *Management Challenges for the 21st Century – Knowledge Worker Productivity*, il donne le conseil suivant : « *Exigez des travailleurs intellectuels qu'ils définissent leur propre tâche et leurs résultats, car ils doivent être autonomes. Avec ses connaissances spécialisées et uniques, chaque travailleur intellectuel en sait plus sur son domaine spécifique que n'importe qui d'autre dans l'organisation. Cela signifie qu'une fois que chaque travailleur intellectuel a défini sa mission et que le travail a été envisagé de manière appropriée, on attend qu'il élabore son propre parcours et qu'il en assume la responsabilité.* ». Dans *Managing in the Next Society*, il va plus loin : « *Considérez les travailleurs intellectuels comme des volontaires et aidez-les dans leur définition de leurs objectifs, dans l'intérêt de l'organisation. Permettez-leur de prendre des décisions dans leur champ de compétences, respectez-les ainsi que leur expertise, assurez-vous qu'ils restent intellectuellement challengés* ».

Peter Drucker aborde aussi l'épineuse question de la définition des objectifs à atteindre : « *Définir quels devraient être les résultats des actions d'un travailleur intellectuel donne lieu à controverse. L'essentiel est d'aligner les objectifs définis par le travailleur intellectuel et désirés par la direction. Ce sujet est un défi permanent pour l'encadrement* ». Ce sujet est souvent un casse-tête pour les *managers* qui ne savent que gérer des travailleurs qu'ils contrôlent de A à Z et qui sont démunis face au travailleur intellectuel indépendant qu'est le DPO.

Les témoins pour partie responsables ?

Quand ils sont contactés par des DPO qui se disent en difficulté, les agents de la CNIL observent que, dans quelques cas, le délégué s'est probablement montré trop cassant ou maximaliste et surtout qu'il n'a pas compris qu'il appartient au responsable de traitement de prendre les décisions, et non pas au DPO. Il faut savoir l'accepter, le RGPD n'ayant jamais obligé un responsable de traitement de suivre à la lettre toutes les recommandations de son délégué.

La CNIL a clarifié ce point crucial dans son Guide pratique RGPD - Délégué à la Protection des Données : « *Le DPO est-il responsable de la conformité ? Ses recommandations sont-elles obligatoires ? – Réponse : Le DPO n'est pas personnellement responsable en cas de manquement aux obligations prévues par le RGPD. C'est l'organisme qui est responsable du respect du RGPD. Il est impossible de transférer au délégué, par délégation de pouvoir, la responsabilité incombant au responsable de traitement ou les obligations propres du sous-traitant. Si les recommandations du DPO ne sont pas suivies, le responsable de traitement ou le DPO peuvent utilement documenter les décisions qui ont été prises ainsi que, le cas échéant, les raisons pour lesquelles l'avis du DPO n'a pas été suivi* ».

Dans les témoignages recueillis, on observe fréquemment une absence de dialogue entre le DPO et le Responsable de traitement. Rares sont les témoins qui ont demandé à être reçus rapidement par la grande direction, encore plus rares sont ceux qui ont pris soin de formaliser un plan stratégique et de le présenter afin de vérifier que la vision est partagée quant aux objectifs et aux attentes en matière de protection des

[35] L'entreprise américaine Gallup avait mené en 2015 une étude sur les motifs de démission. Pour la moitié des personnes interrogées, le *manager* était le principal responsable d'un abandon de poste. Autrement dit, les salariés ne claquent pas la porte à l'entreprise, mais à une seule personne : leur supérieur.

données personnelles. Dans plusieurs cas, cela aurait permis d'éviter les malentendus, voire au DPO de disposer clairement de tous les éléments pour prendre la décision de quitter un environnement professionnel qui ne lui correspond pas.

L'absence de détermination d'objectifs à atteindre et de moyens pour la direction de mesurer concrètement les résultats obtenus est également à l'origine de plusieurs situations conflictuelles : il est possible que le DPO ait fait un travail remarquable, mais que personne n'en soit conscient ou qu'il soit difficile de l'apprécier. Il est également possible que les responsabilités du délégué ne soient pas clairement définies, ce qui peut causer des malentendus entre le DPO et l'entreprise. On rappellera qu'un seul des témoins bénéficiait d'une lettre de mission. Dans son Guide du DPO, la CNIL recommande « *de formaliser les missions confiées au DPO au travers d'un document spécifique. Ce document peut également être l'occasion de définir les modalités de travail du DPO (moyens alloués, interlocuteurs relais identifiés, fréquence des réunions avec la direction de l'organisme et les services traitant les données, circuit de communication, etc.) en décrivant comment les obligations de l'organisme désignant seront transposées en pratique* ». L'AFCDP met en libre disposition un modèle de lettre de mission de DPO[36]. C'est notamment dans ce document que peuvent être spécifiées les conditions dans lesquelles le délégué à la protection des données a accès aux données, informations et collaborateurs.

Le manque de formation ou de préparation de certains témoins mérite également d'être noté. L'un d'entre eux reconnait que la certification et les trente-cinq heures de formation préalable qu'il a suivies ne font pas un DPO[37]. Un membre de l'AFCDP a confié à l'auteur que toutes ses demandes de formation destinées à maintenir ses compétences lui étaient refusées, avec le commentaire suivant : « *Nous vous avons envoyé en formation pendant cinq jours, vous avez décroché la certification, vous êtes désormais un expert, cela est suffisant* » !

La question des ressources est plus épineuse. Il n'existe pas pour l'heure de méthode partagée pour évaluer leur adéquation avec les besoins. Dans son *Guide du DPO*, la Commission indique que « *Par exemple, l'analyse de projets complexes par le DPO nécessite du temps pour délivrer des conseils pertinents. L'estimation de la charge de travail doit être proportionnée aux priorités établies* ». Et il est difficile pour un délégué à la protection des données qui vient de prendre son poste d'estimer et de justifier ses demandes (de budget, d'aide, d'allègement de charge). On rappellera qu'aucun témoin ne produisait d'indicateur, les mettant ainsi en difficulté pour appuyer leur *desiderata*. Notons aussi que quasiment aucun témoin ne disposait d'un budget propre[38] (le seul dans ce cas s'est révélé dans l'impossibilité de l'utiliser).

Avant d'aller plus loin, penchons-nous quelques instants sur une profession également soumise à une forte pression, celle des Responsables de la Sécurité des Systèmes d'Information (les RSSI). Pouvons-nous distinguer des points communs avec le stress vécu par nos témoins ?

---

[36] https://afcdp.net/dpo-fiche-de-poste-et-lettre-de-mission

[37] L'auteur a l'habitude de dire qu'il refuserait d'être opéré par un chirurgien qui a suivi trente-cinq heures de formation, de même qu'il ne monterait pas dans un avion dont le pilote n'a que cinq jours d'entrainement. Telle qu'elle existe actuellement, la certification des DPO ne mesure qu'un niveau de connaissances, mais en aucun cas un savoir-faire ni un savoir être. Ne faudrait-il pas la renommer « certification des connaissances » ?

[38] Les professionnels de la Privacy interrogés dans le cadre du *IAPP-EY Annual Privacy Governance Report 2021* trouvaient à 63 % que les moyens mis à leur disposition étaient insuffisants. Pour autant, le montant du budget moyen dont ils disposaient alors peut faire rêver n'importe quel DPO français (le rapport indique une moyenne de 873.000 $, ventilée de la façon suivante : 57 % en masse salariale et frais de déplacement, 17 % pour des prestations de conseil externe, 11 % en acquisition d'outillage, 11 % en formation et 4 % pour d'autres dépenses). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4227244

Une comparaison avec la situation des RSSI

De nombreux DPO peuvent se reconnaître dans le témoignage d'un ancien RSSI d'une collectivité, publié en mars 2023 dans le magazine Cyberun sous le titre « Les RSSI face au Burn out[39] » : « *Ce qui rend un RSSI efficace, c'est aussi son plus gros point faible : l'acharnement à mener à bien sa mission. En effet, le RSSI doit savoir défendre son point de vue et aller à contre-courant (le fameux « On a toujours fait comme ça, pourquoi changer ? »). Cette lutte permanente est usante et peut conduire à une forme de résignation. Un premier signe ? Lorsque vous vous surprenez à dire « Vous voulez faire n'importe quoi malgré mes conseils ? Et bien, allez-y, faites ! ». Mais cet état d'esprit ne vient pas seul, une chaîne hiérarchique au mieux défaillante, au pire réfractaire, sera à coup sûr le facteur aggravant.* ». Quelques temps auparavant, le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique[40]) et la société Advens avaient publié les résultats d'une enquête sur le stress des RSSI français[41](l'illustration de Fix[42] en est extraite. Les DPO peuvent s'y reconnaitre facilement…). Sans grande surprise, ils ont établi que cette profession est éprouvante et soumise à un niveau élevé de stress. L'évaluation du niveau de tentions nerveuse des 330 répondants a été basée sur un modèle de mesure reconnu (la PSS, *Perceived Stress Scale*[43]) qui utilise une échelle allant de 0 à 40 : le stress est jugé positif ou stimulant si le niveau est inférieur à 16 (« zone verte »), entre 16 et 24, il existe des sentiments d'impuissance occasionnels et des perturbations émotionnelles (« zone orange ») et au-delà de 22, l'individu se situe en « zone rouge », accompagnée de risques accrus pour la santé physique et mentale, avec un sentiment de menace et d'impuissance. Il ressort de l'enquête que 33 % des répondants sont en zone orange et 28 % en zone rouge. Parmi celles-ci, vingt-deux personnes sont même dans une zone à risque de dépression clinique (risque de *burnout*), avec un score supérieur à 28 sur 40.

L'enquête s'est également intéressée aux causes de ce stress. On retrouve des points communs avec celles du stress des délégués : RSSI et DPO sont trop souvent, à tort, perçus par leur entourage professionnel comme des gêneurs, ils sont obligés tous les jours de sauter du coq à l'âne, ils ne savent pas tout et peuvent vite se retrouver dépassés, RSSI et DPO éprouvent quelques difficultés à formuler des réponses binaires et immédiates, ils peuvent avoir du mal à communiquer et convaincre sur des domaines pouvant paraître austères.

Il est intéressant de mener quelques réflexions par rapport à la situation des délégués à la protection des données. Pour les pilotes de l'enquête, les entreprises embauchent volontairement un RSSI, alors que la plupart d'entre elles sont contraintes par le RGPD de désigner un DPO, quelquefois en traînant les pieds. Par ailleurs, même en l'absence de dialogue, les directions et les RSSI partagent les mêmes objectifs (la protection des actifs de l'entreprise), ce qui est loin d'être le cas concernant les délégués à la protection des données (qui sont perçus comme motivés en premier lieu par la protection des personnes concernées).

---

[39] *Les RSSI face au Burn out*, Cyril Bras, Cyberun, n°28, mars 2023
[40] www.cesin.fr
[41] L'enquête est librement accessible sur la page https://www.cesin.fr/articles-slug/?slug=Le+CESIN+et+Advens+r%C3%A9v%C3%A8lent+les+r%C3%A9sultats+d%E2%80%99une+grande+enqu%C3%AAte+in%C3%A9dite+sur+le+stress+des+Responsables+Cyber
[42] www.fix-dessinateur.com
[43] Voir, par exemple, https://www.inrs.fr/media.html?refINRS=FRPS%204

En résumé, le RSSI stresse principalement car il a le sentiment de construire un château de sable sur une plage à marée montante, de se battre contre un ennemi externe et invisible, et de vivre en permanence avec une épée de Damoclès au-dessus de la tête (que constitue l'attaque au bon vouloir du pirate). À l'inverse, le DPO connaît parfaitement l'origine principale de son stress : son superviseur qui n'a pas su lui assurer l'environnement propice à un exercice serein et efficace de sa fonction, sa direction quand elle ne lui apporte aucun soutien.

Nous reviendrons *infra* sur cette étude menée par le CESIN et la société Advens quand seront étudiées les actions envisageables. Etudions maintenant une actualité qui entre en totale résonance avec notre sujet, l'action coordonnée que vont mener cette année plusieurs autorités de contrôle européennes.

Pour 2023, l'action coordonnée européenne est focalisée sur le DPO

En septembre 2022, le Comité Européen de la Protection des Données (CEPD) a choisi comme thème de son action coordonnée pour l'année 2023 les conditions d'exercice du DPO[44]. Ce choix montre l'importance du DPO pour les autorités chargées de la protection des données. Comme l'attestent les récents arrêts de la Cour de justice de l'Union européenne, son statut soulève encore des questions et mérite des éclaircissements. Espérons que l'action coordonnée prendra acte des dérives relevées par l'auteur et apportera les corrections indispensables.

Dans le cadre du *Coordinated Enforcement Framework* adopté en octobre 2020[45], les autorités de contrôle européennes qui le souhaitent vont donc mener des actions locales visant un même objectif. Les résultats de ces actions sont ensuite regroupés et analysés, ce qui permet de mieux comprendre le sujet et d'assurer un suivi ciblé au niveau national et européen. Si l'on se réfère au calendrier de l'action précédente (qui concernait l'utilisation de services basés sur le *Cloud* par le secteur public), on peut espérer une publication du rapport début 2024. Ce document comprendra notamment les recommandations formulées par chaque autorité et les points d'attention. La publication du rapport ne marquera pas automatiquement la fin des initiatives des autorités sur le sujet, certaines pouvant décider de maintenir l'effort.

Dans son communiqué, le CEPD indique que les autorités suivront une méthodologie commune afin de garantir la cohérence de l'action et le respect de ses objectifs. En fait, les autorités participantes[46] peuvent ajuster leurs actions à leurs propres besoins, ressources et priorités[47]. Ainsi, en réponse à une question qui

---

[44] *EDPB adopts statement on European Police Cooperation Code & picks topic for next coordinated action*, 14 septembre 2022, https://edpb.europa.eu/news/news/2022/edpb-adopts-statement-european-police-cooperation-code-picks-topic-next-coordinated_en

[45] https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-coordinated-enforcement-framework-under-regulation_en

[46] À date, outre la CNIL, voici les autorités qui ont confirmé leur participation à cette action commune : le *Bayerisches Landesamt für Datenschutzaufsicht* (Bavière), la *Croatian Personal Data Protection Agency*, la *Úřad pro ochranu osobních údajů* de la République Tchèque, l'*Office of the Data Protection Ombudsman* de Finlande, l'*Agencia de Proteccion de Datos* espagnole, le *Commissioner for Personal Data Protection* chypriote, la *Andmekaitse Inspektsioon* estonienne, La *Hungarian National Authority for Data Protection and Freedom of Information*, le *Garante per la protezione dei dati personali italien*, la *Integritetsskyddsmyndigheten* suédoise, la *Data State Inspectorate* de Lettonie, l'*Information Commissioner of the Republic of Slovenia* et la *Comissao Nacional de Protecçao de Dados* portugaise. Participent également la *Data Protection Authority* du Liechtenstein et l'EDPS (*European Data Protection Supervisor*). Pour sa part, l'Autorité de protection des données belge (APD) a décidé de procéder dans un premier temps à un sondage (Pour qu'ils puissent remplir le questionnaire en toute confiance et transparence, il n'y est pas demandé aux DPO de s'identifier ou d'indiquer l'organisation pour laquelle ils travaillent). L'autorité précise que « *Le questionnaire visera aussi à clarifier les attentes des DPO en termes de soutien de la part d'une autorité de protection de données* ».

[47] Les différences apparaissent dès la lecture des communiqués de presse publiés par les autorités participantes. L'Allemagne indique se focaliser sur les questions de qualifications et les ressources du DPO, ainsi que sur les éventuelles entraves à son indépendance. Elle veut aussi vérifier que les délégués peuvent avoir accès directement à l'échelon le plus élevé de la direction. Enfin elle compte examiner « *les rapports annuels des délégués à la protection des données* ». L'autorité tchèque se concentrera sur le statut des délégués à la protection des données dans l'administration

lui était posée par l'auteur lors de l'Université AFCDP des DPO du 9 février 2023, Mathias Moulin a indiqué que la CNIL procéderait probablement par des missions de contrôles sur place. Certaines d'entre elles pourraient, en toute hypothèse, déboucher sur des sanctions (« *Rien n'est exclu, nous avons aussi besoin de jurisprudence* »). Le Secrétaire général adjoint de la CNIL a évoqué le dialogue nécessaire avec les associations de DPO, afin que la campagne soit la plus pertinente : « *Nous en tirerons des enseignements au niveau national, mais aussi au niveau européen. Il sera intéressant de voir comment la France se situe par rapport à ses voisins. Les enseignements pourraient être valorisés dans des outils, dans du droit souple – c'est-à-dire de la doctrine-, mais aussi, si besoin, dans du répressif* ». Dans une interview disponible en ligne[48], Mathias Moulin avait insisté sur le nécessaire soutien au DPO : « *Le métier est encore plus essentiel qu'auparavant. Il faut lui donner les moyens, l'impliquer dans la gouvernance. À défaut, c'est jouer avec la réputation de son organisme et avec la sécurité des données personnelles de ses clients* ».

Lors d'une conférence organisée en mars 2023 par l'IAPP[49], Gwendal Le Grand, Secrétaire général adjoint du CEPD, a apporté quelques précisions : « *L'idée n'est pas de rendre la vie des DPD plus difficile, mais de s'assurer qu'ils ont bien les moyens de travailler correctement au sein de leur organisation* ». À cette même occasion, un représentant de l'autorité espagnole a indiqué qu'elle compte analyser « *les pratiques de plus de 30.000 entités des secteurs public et privé via un questionnaire qui comprendra, entre autres, des questions relatives à la désignation, aux connaissances et à l'expérience du DPD, à ses tâches, ses ressources et à son position* ». Concernant ce dernier point, Anu Talus, le commissaire finlandais à la protection des données a rappelé que « *le délégué à la protection des données doit avoir la possibilité de rendre compte directement à la direction générale* ». À la lecture du rapport annuel sur l'année 2021 de l'autorité de contrôle belge, nous ne sommes pas surpris d'apprendre qu'elle participe également à cette initiative : « *Il ressort d'un nombre croissant d'enquêtes qu'il existe encore une marge d'amélioration et de précision du fait que le DPO manque souvent de soutien, n'est pas impliqué ou trop tardivement et que ses avis ne sont pas (suffisamment) suivis. On constate souvent que le DPO (pour diverses raisons) ne répond pas aux exigences imposées par le RGPD.* ».

Le 15 mars 2023, le CEPD a donné le coup d'envoi de son action coordonnée sur « *la désignation et la position des délégués à la protection des données* ». Son communiqué précise « *En tant qu'intermédiaires entre les autorités de protection des données, les individus et les unités opérationnelles d'une organisation, les délégués à la protection des données jouent un rôle essentiel en contribuant au respect de la législation sur la protection des données et en promouvant une protection efficace des droits des personnes concernées* ». Sur son site, le Comité liste les autorités qui ont annoncé leur participation à cette action commune. Si le communiqué[50] du Comité Européen de Protection des Données n'évoque que la vérification du positionnement du Délégué et des ressources dont il dispose, quels peuvent être très concrètement les points de contrôle sur lesquels seront jugées les conditions d'exercice du DPO, en lien avec ce que prévoit le RGPD ? L'auteur s'est procuré les trente-six questions que la CNIL a adressé à un certain nombre de responsables de traitement dans le cadre d'un contrôle sur pièces (la Commission précise bien qu'elle attend des éléments de preuve pour chaque réponse apportée). Ces questions figurent en annexe n°4.

publique. L'autorité estonienne a sélectionné dix-neuf organisations des secteurs public et privé. La Hongrie, le Portugal et la Slovénie adresseront directement un questionnaire aux DPO, mais avec des variantes : les DPO portugais pourront y répondre sans avoir besoin de s'identifier ni de citer leur responsable de traitement. À l'inverse, l'autorité slovène précise que les réponses apportées par les DPO pourraient entraîner un contrôle du responsable du traitement...

[48] https://afcdp.ubicast.tv/permalink/v12663780c4c2qw165np/iframe/

[49] https://iapp.org/news/a/edpb-launches-coordinated-enforcement-on-role-of-dpos/

[50] https://edpb.europa.eu/news/news/2023/launch-coordinated-enforcement-role-data-protection-officers_en

À la connaissance de l'auteur, deux autorités au moins ont déjà mené par le passé des actions sur ce sujet[51] : celle du Luxembourg et celle d'Irlande[52]. Si cette dernière n'a pas souhaité publier le résultat de ses travaux, la CNPD luxembourgeoise a posté sur son site toutes les délibérations qui témoignent des vingt-cinq contrôles qu'elle a réalisés courant 2018[53] (donc immédiatement après l'entrée en application du RGPD) auprès d'un panel varié de responsables de traitement dont les identités n'ont pas été dévoilées. Ces délibérations s'ouvrent sur le passage suivant : « *Vu l'impact du rôle du délégué à la protection des données et l'importance de son intégration dans l'organisme, la Commission nationale pour la protection des données a décidé de lancer une campagne d'enquête thématique sur la fonction du DPD* ». À l'issue de cette campagne, treize responsables de traitement ont été invités à appliquer des mesures correctrices et huit d'entre eux ont écopé en sus d'une amende (la plus élevée de 27.100 €).

Commençons par lister les points de contrôle retenus par l'autorité de contrôle luxembourgeoise. Ses agents voulaient s'assurer :

- que l'organisme soumis à l'obligation de désigner un DPD l'a bien fait ;
- que l'organisme a publié les coordonnées de son DPD[54] ;
- que l'organisme a communiqué les coordonnées de son DPD à l'autorité ;
- que le DPD dispose d'une expertise et de compétences suffisantes pour s'acquitter efficacement de ses missions ;
- que les missions et les tâches du DPD n'entraînent pas de conflit d'intérêt ;
- que le DPD dispose de ressources suffisantes pour s'acquitter efficacement de ses missions ;
- que le DPD est en mesure d'exercer ses missions avec un degré suffisant d'autonomie au sein de son organisme ;
- que l'organisme a mis en place des mesures pour que le DPD soit associé à toutes les questions relatives à la protection des données ;
- que le DPD remplit sa mission d'information et de conseil auprès du responsable du traitement et des employés ;
- que le DPD exerce un contrôle adéquat du traitement des données au sein de son organisme ;
- que le DPD assiste le responsable du traitement dans la réalisation des analyses d'impact en cas de nouveaux traitements de données.

On constate d'emblée de la majorité des responsables de traitement impliqués dans les témoignages

[51] Notons également que, dans son Plan de Gestion 2022, l'Autorité de protection des données belge a, pour objectif stratégique et opérationnel, de « *Continuer à expliquer la désignation et la position du DPO sur la base des enquêtes quotidiennes, en analysant aussi – si c'est pertinent – le rôle du DPO (et ce parce que le DPO est et reste une figure clé dans le RGPD)* », et cela « *car Il ressort d'un nombre croissant d'enquêtes qu'il existe encore une marge d'amélioration et de précision du fait que le DPO manque souvent de soutien, n'est pas impliqué ou trop tardivement et que ses avis ne sont pas suivis. On constate souvent que le DPO (pour diverses raisons) ne répond pas aux exigences strictes imposées par le RGPD* ».
https://www.autoriteprotectiondonnees.be/publications/plan-de-gestion-2022.pdf

[52] Il convient de mentionner également l'initiative que la CNIL a menée courant 2022 auprès d'une cible spécifique, celle des collectivités dont certaines n'ont pas encore désigné de délégués à la protection des données alors qu'elles y sont contraintes.

[53] Il s'agit des délibérations n° 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 18, 19, 20, 23, 25, 29, 30, 36, 37, 38, 39, 40, 41, 42, et 43/FR/2021, publiées du 5 mars au 27 octobre 2021 (source https://cnpd.public.lu/fr/decisions-sanctions.html?r=f%2Faem_first_released%2F2021&)

[54] La CNIL publie en données ouvertes la liste des « Organismes ayant désigné un(e) délégué(e) à la protection des données (DPD/DPO) ». Dans la version consultée par l'auteur (mise à jour le 20 mars 2023), il est surprenant de noter la présence d'd'adresses électroniques permettant de joindre les DPO désignés qui comportent un nom de domaine en « cnil.fr ». Les tentatives d'envoi de courriels à ces adresses aboutissent sur un message d'erreur généré par le domaine Cnil.fr. Y aurait là pour l'autorité de contrôle matière à sanctionner puisque le DPO n'est pas joignable ?

affligeants évoqués dans la première partie de ce document est loin de répondre à ces exigences. Feront-ils partie du panel qui sera contrôlé prochainement par la CNIL ?

Si certains points sont binaires (comme la publication des coordonnées du délégué ou la communication de sa désignation à l'autorité), on perçoit bien la difficulté que devraient rencontrer les autorités qui vont participer à l'action commune afin de déterminer des règles pour juger si le délégué à la protection des données dispose de ressources suffisantes, si son indépendance est réelle ou s'il dispose d'une expertise et de compétences suffisantes pour s'acquitter efficacement de ses missions. À cet égard, la lecture de certaines délibérations de la CNPD nous apporte quelques premiers éléments.

Concernant l'expertise et les compétences du DPO

Quatre responsables de traitement ont été mis sur la sellette : avaient-ils respecté l'article 37.5 du RGPD ? Ont-ils bien désigné leur délégué « *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* » ? Dans leur cas, l'ampleur et la sensibilité des données traitées faisait que le chef d'enquête s'attendait à ce que le DPD ait au minimum trois ans d'expérience professionnelle en matière de protection des données[55].

Une fondation a été sanctionnée après que la CNPD a constaté que le délégué disposait de moins de trois ans d'expérience professionnelle en matière de protection des données et qu'il ne possédait pas lui-même d'expertise juridique[56]. Certes, il avait accès à un cabinet d'avocats en cas de besoin, mais cet accès était conditionné à l'approbation de sa hiérarchie. Le chef d'enquête en conclut qu'il « *existe dès lors un risque que le DPD ne puisse pas accéder à l'expertise juridique dont il a pourtant besoin* ». Le contrôlé a depuis pris la décision d'engager « *un nouveau DPD disposant de compétences élargies (compétences juridiques et techniques) ainsi qu'une expérience confirmée et un cursus professionnel plus en ligne avec le rôle de DPD* ».

Une administration s'est vue enjoindre la mise en œuvre de mesures correctrices sur ce même sujet[57]. Le chef d'enquête avait constaté que « *le DPD n'a pas de formation initiale en matière juridique ou protection des données, ni ne justifie d'une pratique en la matière. Le fait que le DPD ait participé à deux formations spécifiques protection des données et suivi des ateliers participatifs ne suffit pas à établir l'existence d'une expertise adaptée aux besoins du responsable de traitement* ». L'administration contrôlée a mis en avant la collaboration étroite mise en place entre son délégué et le service juridique. Néanmoins, la formation restreinte a considéré que cela ne permet pas d'établir que le délégué disposait d'une expertise adaptée aux besoins du contrôlé, notamment au vu de la sensibilité, de la complexité et du volume des données traitées. La formation restreinte note d'ailleurs que, à la suite de son premier contrôle, le responsable de traitement a décidé le recrutement d'un DPO disposant d'un niveau d'expertise adapté.

Dans les deux autres cas[58], la formation restreinte de la CNPD a abandonné ce grief (mais a prononcé des sanctions pour d'autres motifs), après avoir constaté que, si les délégués à la protection des données ne

[55] Cette référence à une expérience de « trois ans au moins » provient-elle du *Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001* ? En effet, en page 4 de ce document, on relève le passage suivant : « *Toutefois, le réseau des DPD des institutions et organes de l'Union recommande que ces délégués aient l'expérience/maturité suivante : au moins 3 ans d'expérience pertinente pour exercer les fonctions de DPD dans un organisme où la protection des données n'est pas liée à l'activité principale (et donc les activités de traitement des données à caractère personnel sont principalement administratives) ; et au moins 7 ans d'expérience pertinente pour exercer les fonctions de DPD dans une institution de l'UE ou dans les organes de l'UE où la protection des données est liée à l'activité principale ou qui ont un volume important d'opérations de traitement de données à caractère personnel.* ».

[56] Délibération CNPD n° 29FR/2021 du 4 août 2021

[57] Délibération CNPD n° 23FR/2021 du 29 juin 2021

[58] Délibération CNPD N° 38FR/2021 du 15 octobre 2021 et Délibération CNPD N° 36FR/du 13 octobre 2021

disposaient pas des connaissances requises, ils pouvaient librement s'appuyer sur des personnes qui possédaient toutes les compétences requises en matière juridique et en matière de protection des données.

Concernant l'absence de conflit d'intérêt

Deux responsables de traitement ont été concernés par le respect de l'article 38.6 du RGPD. L'un d'entre eux[59] avait désigné une personne qui était également responsable du service informatique. Pour la formation restreinte, « *Le DPD pourrait donc être amené à se prononcer sur des traitements qu'il a lui-même mis en place en tant que responsable du service IT*. ». Cet acteur a désigné un nouveau délégué, totalement dédié à sa mission. Dans le second cas, un établissement public placé sous la tutelle d'un Ministère qui avait désigné un avocat en tant que DPO externe, le grief a été abandonné après que la fiche de fonction a été modifiée pour clarifier l'absence de conflit d'intérêt.

Dans ses délibérations, la CNPD liste quelques bonnes pratiques permettant de respecter l'article 38.6 : « *recenser les fonctions qui seraient incompatibles avec celle de DPD ; établir des règles internes à cet effet, afin d'éviter les conflits d'intérêts ; inclure une explication plus générale concernant les conflits d'intérêts ; déclarer que le DPD n'a pas de conflit d'intérêts en ce qui concerne sa fonction de DPD, dans le but de mieux faire connaître cette exigence ; prévoir des garanties dans le règlement intérieur de l'organisme, et de veiller à ce que l'avis de vacance pour la fonction de DPD ou le contrat de service soit suffisamment précis et détaillé pour éviter tout conflit d'intérêts* ». Il convient aussi de noter que la CNPD dissocie clairement le sujet des conflits d'intérêt de celui de l'autonomie du DPO, comme l'avait d'ailleurs fait le G29 dans ses lignes directrices sur le délégué à la protection des données (WP243).

Concernant les ressources du DPO

Le respect de l'article 38.2 du RGPD est traité dans six délibérations. Sur ce point, la formation restreinte de la CNPD prend comme référence les lignes directrices du G29 relatives au DPO (WP243[60]) : « *Il convient de prévoir un temps suffisant pour que les DPD puissent accomplir leurs tâches. Cet aspect est particulièrement important lorsqu'un DPD interne est désigné à temps partiel ou lorsque le DPD externe est chargé de la protection des données en plus d'autres tâches. Autrement, des conflits de priorités pourraient conduire à ce que les tâches du DPD soient négligées. Il est primordial que le DPD puisse consacrer suffisamment de temps à ses missions. Il est de bonne pratique de fixer un pourcentage de temps consacré à la fonction de DPD lorsque cette fonction n'est pas occupée à temps plein. Il est également de bonne pratique de déterminer le temps nécessaire à l'exécution de la fonction et le niveau de priorité approprié pour les tâches du DPD, et que le DPD (ou l'organisme) établisse un plan de travail ; accès nécessaire à d'autres services, tels que les ressources humaines, le service juridique, l'informatique, la sécurité, etc., de manière à ce que les DPD puissent recevoir le soutien, les contributions et les informations essentiels de ces autres services* ».

Concernant un premier établissement public sous la tutelle d'un Ministère, et compte-tenu de l'importance des traitements, le contrôleur s'attendait à ce que le contrôlé assure au minimum un équivalent temps plein pour l'équipe en charge de la protection des données[61]. Le chef d'enquête s'attendait également à ce que le DPD ait la possibilité de s'appuyer sur d'autres services, tels que le service juridique, l'informatique, ou la sécurité. Or, malgré l'existence d'un budget alloué au délégué, les constatations concernant le temps consacré à la fonction de DPD « *sont de nature à mettre en évidence une inadéquation entre les ressources et moyens mis à disposition du DPD et les besoins du responsable du traitement* ». Il en est quasiment de même pour un second établissement public[62]. Bien que celui-ci fasse remarquer que, si son délégué « *bénéficiait de l'appui d'un consultant externe* », la

[59] Délibération CNPD n° 29FR/2021 du 4 août 2021
[60] https://ec.europa.eu/newsroom/article29/items/612048
[61] Délibération CNPD N° 38FR/2021 du 15 octobre 2021
[62] Délibération CNPD n° 30FR/2021 du 4 août 2021

formation restreinte ne l'a pas entendu de cette oreille : « *Même en prenant en considération le fait que le DPD consacre plus de temps à ses missions de DPD que les 50 % initialement prévus ainsi que le support fourni par l'intervention temporaire, jusqu'en mars 2019, d'un consultant externe, la formation restreinte estime que le DPD ne disposait pas du temps suffisant pour accomplir ses tâches, ceci notamment au regard de la sensibilité, de la complexité et du volume des données traitées par le contrôlé.* ». Le jugement est similaire pour la fondation évoquée *supra*[63] : « *Il a été constaté que le DPD ne consacrait que 50 % de son temps de travail à l'exercice de ses missions. L'indication selon laquelle le DPD disposait du support d'un prestataire externe ne constitue pas un élément suffisant pour démontrer que le DPD disposait des ressources suffisantes pour s'acquitter de ses missions* ».

Au sein d'une administration[64], il est constaté que « *le DPD est affecté à 25 % (environ 10h par semaine) et exerce seul ses missions. Le fait que le DPD bénéficie du support informel du service juridique et du service informatique et le fait qu'un prestataire externe soit intervenu à raison de 60 jours homme sur une période de 12 mois (soit environ 5 jours par mois), ne sauraient suffire à fournir un temps suffisant pour que le DPD accomplisse ses missions.* ». Le contrôlé a indiqué recruter un délégué à la protection des données à temps plein, qui « *disposera du support en interne du service juridique, du service informatique et de la personne qui assure actuellement la fonction et d'une enveloppe budgétaire pour un support externe* ».

La délibération n° 18FR/2021 du 31 mai 2021 traite d'une situation spécifique : celle d'un DPO mutualisé interne positionné en dehors du Luxembourg (un DPD « Groupe »). Malgré la présence d'un interlocuteur local et d'une équipe qui épaule le DPD groupe, le chef d'enquête relève *« le risque que le DPD groupe n'ait pas suffisamment de ressources au niveau local à Luxembourg, les ressources étant concentrées au niveau du groupe, mais ne semblant pas suffisamment déployées au niveau local* » ainsi que « *le risque qu'en cas de fort pic d'activité concernant les affaires juridiques à traiter au sein de l'entité luxembourgeoise, le point de contact local ne puisse pas avoir les moyens de s'acquitter efficacement de ses missions relatives à la protection des données, ce qui engendrerait le risque que le DPD ne puisse pas exercer efficacement ses missions de DPD pour le Luxembourg* ». La formation restreinte estime qu'une telle organisation requiert que l'organisme détermine et documente le temps nécessaire au point de contact local pour exercer ses missions relatives à la protection des données afin de pouvoir lui attribuer les ressources nécessaires. Or, il ressort du dossier que le contrôlé n'a pas procédé à une quelconque formalisation ou documentation permettant de démontrer qu'il a fourni à la fonction de délégué groupe les ressources nécessaires à l'exercice de ses missions.

En revanche, dans sa délibération N° 36FR/2021 du 13 octobre 2021, la formation restreinte abandonne son grief (mais le responsable de traitement – en l'occurrence une société d'assurance – écope tout de même d'une amende de 13.200 € pour d'autres infractions au RGPD relatives aux conditions d'exercice de son DPD). Après avoir constaté que « *les ressources dédiées à l'équipe en charge de la protection des données étaient d'environ 0.7 ETP, (0.3 pour le vice-DPD et 0.2 pour chacune des deux juristes en charge des demandes des personnes concernées)* », elle semble avoir été sensible au passage en temps plein du délégué.

Concernant le respect de l'indépendance du DPO

Cinq responsables de traitement se sont vu reprocher de ne pas placer leur délégué en mesure d'exercer ses missions avec un degré suffisant d'autonomie au sein de son organisme (infraction à l'article 38.3 du RGPD). Le chef d'enquête s'attend à ce que le délégué à la protection des données soit notamment « *rattaché au plus haut niveau de la direction afin de garantir au maximum son autonomie* ».

[63] Délibération CNPD n° 29FR/2021 du 4 août 2021
[64] Délibération CNPD n° 23FR/2021 du 29 juin 2021

Au sein d'une banque, le délégué était à quatre degrés de la direction générale. Outre le fait que le DPD n'était pas rattaché au plus haut niveau de la direction et bien que le délégué puisse intervenir au Comité exécutif et au Comité de contrôle interne à sa demande et à tout moment, « *Il n'a pas été démontré par le contrôlé que la reddition de compte directe auprès du plus haut niveau de la direction était formalisée. […] Le rattachement hiérarchique à la Direction et donc l'accès à cette dernière ne sont pas directs et permanents* ». Dans sa délibération[65], la formation restreinte évoque, parmi les mesures à prendre, la création d'un « *mécanisme d'escalade d'urgence à la direction permettant de contourner le(s) niveau(x) hiérarchique(s) intermédiaire(s).* ». Une société de transports (sanctionnée à hauteur de 15.400 €) se voit reprocher un rattachement de qualité insuffisante[66] : « *Bien que le DPD soit fonctionnellement rattaché à la Direction et qu'il participe au Comité de Direction en fonction de l'ordre du jour, le rattachement hiérarchique à la Direction et donc l'accès direct et permanent à cette dernière n'est pas formellement garanti.* ». En mesure de correction, le délégué a été rattaché directement au Secrétariat général.

La fondation déjà évoquée se voit reprocher le « filtre » que représente un directeur placé entre le délégué et la grande direction[67] : « *Il ressort de l'enquête que le DPD est rattaché au Directeur [...]. Bien que formellement, dans la déclaration de nomination, il soit prévu que le DPD rende compte directement au comité de direction une fois par trimestre, dans les faits, la remontée d'information se fait uniquement par l'intermédiaire du Directeur de rattachement*. ». La formation restreinte demande à ce que le DPD puisse intervenir personnellement au plus haut niveau de la hiérarchie. Une administration se voit reprocher le manque de formalisme concernant la reddition du délégué auprès de la grande direction[68] : « *Compte tenu du caractère informel des contacts du DPD avec la direction, ces éléments ne tendent pas à démontrer l'existence d'un rapport direct au niveau le plus élevé de la direction. Par ailleurs, le responsable de traitement n'a pas été en mesure de démontrer que le DPD pouvait agir sans recevoir d'instruction en ce qui concerne l'exercice de ses missions* ».

Dans la délibération n° 20FR/2021 du 11 juin 2021, la formation restreinte formule trois reproches : a) un rattachement hiérarchique du délégué qualifié d'incertain (« *La Société n'a pas été en mesure de démontrer l'existence d'un rapport direct au niveau le plus élevé de la direction, par exemple, par le biais d'un rapport d'activité. S'agissant du rattachement hiérarchique, le DPD était initialement rattaché au directeur juridique, lui-même rattaché au directeur administratif et financier* ») ; b) le fait que les rapports rédigés par le délégué à destination du directeur général étaient d'abord discutés avec le Directeur administratif et financier ; et enfin c) qu'il était prévu que le DPD puisse accéder au plus haut niveau de la direction seulement en cas de « problème significatif ». Pour la formation restreinte, « *Outre la question de savoir quels sont les critères qui permettent de déterminer, en pratique, l'existence d'un tel problème, la formation restreinte émet des réserves quant à cette condition qui pourrait constituer un obstacle à l'accès direct du DPD au plus haut niveau de la direction, en ce que le DPD pourrait se trouver dans la position de devoir justifier l'existence d'un tel « problème significatif » avant d'intervenir auprès du plus haut niveau de la direction. Or, la formation restreinte considère que le DPD devrait pouvoir contourner les niveaux hiérarchiques intermédiaires dès qu'il l'estime nécessaire* ». La société a modifié sa politique générale de gestion des données à caractère personnel pour y spécifier que « *le DPO s'il estime nécessaire peut directement prendre contact avec le Directeur Général de la Société afin de lui remonter toute problématique* ».

[65] Délibération CNPD N° 41FR/2021 du 27 octobre 2021
[66] Délibération CNPD N° 40FR/2021 du 27 octobre 2021
[67] Délibération CNPD n° 29FR/2021 du 4 août 2021
[68] Délibération CNPD n° 23FR/2021 du 29 juin 2021

Concernant l'association du DPD à toutes les questions relatives à la protection des données

Plusieurs responsables de traitement se voient reprocher une infraction à l'article 38.1 du RGPD. Concernant la banque déjà évoquée *supra*[69], « *le fait que le DPD ait participé à deux Comités de Contrôle Interne, à une réunion du Management Board, qu'il soit invité permanent du Comité de Sécurité et qu'il soit impliqué si un aspect Data Protection concerne un nouveau produit ne suffit pas à démontrer le caractère formel, permanent et régulier de son implication* ». Pour la formation restreinte, « *Une des possibilités pourrait être d'analyser, avec le DPD, tous les comités/groupes de travail pertinents au regard de la protection des données et de formaliser les modalités de son intervention (information antérieure avec l'agenda des réunions, invitation, fréquence, statut de membre permanent, etc.* ». Pour l'une des sociétés de transports contrôlées[70], « *Aucune règle ou fréquence n'a été définie de façon formelle quant à la participation du DPD à ces comités ou réunion* » et « *Le contrôlé n'a pas apporté la preuve quant à la présentation du rapport d'activités du DPD au Comité de Direction sur une fréquence trimestrielle* ». Concernant l'autre société de transports[71], la formation restreinte prend note du fait que, en cours d'enquête, le contrôlé a indiqué qu'il avait décidé de « *formaliser des réunions mensuelles entre le DPD et les chefs de service qui traitent le plus de données personnelles (principalement informatique, ressources humaines) ... ainsi que des réunions biannuelles avec les autres chefs de services »* et d'ajouter *« en annexe à la politique générale de gestion de données, une fiche permettant à chaque personne en charge d'un projet de traiter avec le DPO la question de la protection des données* ».

La délibération n° 18FR/2021 du 31 mai 2021 qui concerne la société luxembourgeoise dont le DPO est mutualisé et au niveau du groupe (à laquelle avait déjà été reproché un manque de ressources pour le délégué), aborde également ce critère : « *[Certes] le DPD participe à de nombreuses réunions au niveau Groupe et [...] organise régulièrement des réunions avec ses points de contacts locaux. Mais ces éléments ne suffisent pas à démontrer le caractère direct, formel et permanent de l'implication du DPD à Luxembourg [...] Le DPD Groupe reçoit un rapport mensuel de la part du point de contact local. [...] Le fait de transmettre les procès-verbaux du [Comité GDPR] au DPD Groupe ne permet pas d'établir son association appropriée et en temps utile. Ces éléments ne sauraient compenser l'absence d'une implication directe du DPD Groupe au sein de la Société contrôlée, ce qui pourrait engendrer le risque que le DPD ne soit pas suffisamment impliqué au niveau opérationnel à Luxembourg.* ». Le chef d'enquête fait valoir qu'il « *n'a pas eu connaissance d'éléments permettant d'adresser ce risque, comme par exemple la mise en place formelle de visites sur base d'une fréquence définie du DPD Groupe (ou d'un membre de son équipe Data Protection) à Luxembourg. Ces visites permettraient notamment au DPD de pouvoir discuter directement avec l'encadrement supérieur de la Société contrôlée des problématiques liées à la protection des données et de pouvoir évaluer directement les problématiques* ». La formation restreinte demande à ce que soient définies clairement les modalités de collaboration entre le DPD et les « points de contact locaux » ainsi que la répartition des tâches et responsabilités.

Un cas avec DPO externe est également traité[72] : « *Le DPD externe [a] un rôle qualifié d'essentiellement « réactif », [Son] implication était donc relativement limitée. Il [intervient] principalement sur demande explicite du responsable du traitement et non de manière spontanée* ». Le rapport de contrôle précise que l'implication limitée du DPD externe se caractérisait plus particulièrement par une « *participation faible aux réunions récurrentes, uniquement sur invitation quand le besoin a été estimé* ». Pour la formation restreinte, « *Le contrôlé n'a pas démontré avec suffisance l'association du DPD externe d'une manière appropriée et en temps utile à toutes les questions relatives à la protection des données* ».

[69] Délibération CNPD N° 41FR/2021 du 27 octobre 2021
[70] Délibération CNPD N° 40FR/2021 du 27 octobre 2021
[71] Délibération CNPD n° 20FR/2021 du 11 juin 2021
[72] Délibération CNPD N° 38FR/2021 du 15 octobre 2021

Concernant la mission d'information et de conseil auprès du responsable du traitement

Pour plus de clarté, nous avons préféré scinder l'exigence de l'article 39.1 a) du RGPD : nous commençons par aborder l'information du responsable de traitement pour traiter ensuite de celle des salariés.

Plusieurs responsables de traitement se sont vus reprocher l'absence de formalisme de la reddition du DPO vers l'encadrement supérieur : « *Il ressort de l'enquête que l'organisme n'a pas de reporting d'activité spécifique sur la protection des données destiné à l'encadrement supérieur (Comité de Direction, Conseil d'Administration). Absence de reporting formel des activités du DPD vers le Comité de Direction sur base d'une fréquence définie*[73] », « *Il est attendu que les missions d'information et de conseil à l'égard du responsable de traitement soient mieux formalisées, par exemple avec un rapport d'activité*[74] », « *Il n'existe pas d'outil tel qu'un rapport d'activité qui aurait pu permettre au DPD d'adresser des conseils formels au responsable de traitement* », *« Compte tenu du degré de sensibilité relativement élevé [...] la formation restreinte considère dès lors qu'un reporting formel des activités du DPD auprès de la direction, sur la base d'une fréquence définie, constitue une mesure proportionnée afin de démontrer que le DPD exerce ses missions d'information et de conseil à l'égard du responsable du traitement* ». Dans les résultats d'un sondage mené en 2020 par l'autorité danoise auprès des DPO désignés auprès d'elle, 65 % des répondants avaient indiqué ne formaliser aucun reporting vers leur direction. Datatilsynet formulait alors le conseil de mettre en place des routines formelles qui garantissent un dialogue direct et régulier entre le Délégué à la Protection Des données et la direction. Concernant le rapport du DPO, l'auteur rappelle son article « *Collègues DPO : Le bilan annuel est un outil précieux – Faisons-en une bonne pratique*[75] ».

Concernant la mission d'information et de conseil auprès des employés

Pour un acteur du secteur Santé, la formation restreinte note qu'il ressort de l'enquête « *que le responsable du traitement n'a pas été en mesure de démontrer que le DPD exerce ses missions d'information du personnel en contact direct avec les données de patients alors que le plan de formation du personnel salarié inclut un e-learning GDPR obligatoire* » et ordonne « *la mise en place de mesures assurant que l'intégralité des personnes agissant sous la responsabilité exclusive ou partielle du responsable du traitement en ce qui concerne le traitement de données personnelles suivent des formations régulières, au moins annuelles, en la matière*[76] ».

Le personnel d'une administration reçoit des séances de sensibilisation relatives à la sécurité informatique, mais pas de sensibilisation sur la protection des données en général. En conséquence, la formation restreinte constate que « *le personnel du contrôlé n'était pas spécifiquement sensibilisé à la protection des données personnelles* » et demande la mise en place d'un dispositif de formation adéquat.

Concernant le « contrôle adéquat » que doit exercer le DPO sur les traitements des données au sein de son organisme

Là où le Correspondant Informatique et Libertés pouvait se contenter du déclaratif, son successeur, le délégué à la protection des données, doit « *contrôler le respect* » du règlement (article 39.1 b) du RGPD).

Sept responsables de traitement se voient reprocher une infraction à cette exigence, dans des termes proches : « *Il ressort de l'enquête que l'organisme ne dispose pas de plan de contrôle* », « *Il ressort de l'enquête que l'organisme ne dispose pas de plan de contrôle formalisé, spécifique à la protection des données* », « *Il ressort de l'enquête que l'organisme ne dispose pas d'un plan de contrôle formalisé mais d'une liste de tâches, comprenant des points de contrôle* ». L'une des

[73] Délibération CNPD N° 40FR/2021 du 27 octobre 2021
[74] Délibération CNPD n° 20FR/2021 du 11 juin 2021
[75] B. Rasle, 29 mars 2020, https://www.anaxia-conseil.fr/le-bilan-annuel-est-un-outil-precieux-faisons-en-une-bonne-pratique.html
[76] Délibération CNPD N° 39FR/2021 du 15 octobre 2021

délibérations[77] apporte une précision intéressante : « *Le chef d'enquête s'attend à ce que l'organisme dispose d'un plan de contrôle formalisé en matière de protection des données, même s'il n'est pas encore exécuté* ». Quelques-uns des organismes incriminés ont tenté d'expliquer que c'est la tenue du registre des traitements, opéré par le Délégué, qui faisait office de mesure de contrôle. La formation restreinte ne l'a pas entendu ainsi : « *La formation restreinte relève que cet élément [le fait que le DPD soit impliqué dans l'établissement du registre des activités de traitement] pris isolément ne suffit pas à démontrer que le DPD effectue sa mission de contrôle du respect du RGPD de manière adéquate* ».

En réaction, tous les acteurs concernés se sont engagés à mettre en place une stratégie d'audit et de contrôle formelle par l'élaboration d'un plan de contrôle maîtrisé par le DPD. L'un d'entre eux précise que « *le plan de contrôle sera fourni par le [DPD] à la fin de chaque année pour l'année suivante* ». Certains ont enrichi la lettre de mission de leur délégué en y ajoutant ou précisant sa mission de contrôle.

Il est prudent de se préparer à un éventuel contrôle de la CNIL

À partir de l'analyse des délibérations de la CNPD, on voit donc qu'il est prudent de se préparer à l'éventualité d'une visite des agents de la CNIL dans le cadre d'une mission de contrôle sur place. Sur la base de la démarche utilisée par l'autorité luxembourgeoise, les DPO peuvent déjà préparer les documents et éléments de preuve qui seront probablement demandés, comme la description de leur poste, leur contrat de travail, leur lettre de mission, les comptes-rendus de leurs entretiens annuels, l'organigramme de l'organisme qui montre leur positionnement, les comptes-rendus des réunions qu'ils ont tenues avec leur superviseur et avec le responsable de traitement, les traces des comités de direction ou exécutifs auxquels ils ont participé, les preuves des formations qu'ils ont suivies, le nombre d'heures qu'ils consacrent à leur fonction, leur budget et son utilisation, leur plan de contrôle, les preuves de leurs actions de sensibilisation des personnels, etc.

Il est sage également d'examiner honnêtement chacun des points de contrôle utilisés par la CNPD et de préparer, pour chacun d'entre eux, les éléments de preuve. Les lignes directrices concernant les délégués à la protection des données (DPD) du G29 (WP243) rappellent que « *Le responsable du traitement ou le sous-traitant reste responsable du respect de la législation sur la protection des données et doit être en mesure de démontrer ce respect* » au titre de l'article 5.2 du RGPD. Les réponses apportées à la CNIL et la fourniture des éléments de preuve engagent donc le responsable de traitement. Naturellement, si des écarts sont constatés, la logique voudrait qu'ils soient comblés rapidement sans attendre une éventuelle sanction.

Les contrôles de l'autorité luxembourgeoise ayant été réalisés peu de temps après l'entrée en application du RGPD, aucune des délibérations analysées ne signale un manquement à l'article 39.1.C) : « *[Les missions du délégué à la protection des données sont au moins les suivantes […] 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* » (que la CNPD synthétique en « *Le DPD assiste le responsable du traitement dans la réalisation des analyses d'impact en cas de nouveaux traitements de données* »). Il convient donc de se préparer également à être en mesure de prouver le respect de cette disposition.

Deux analogies intéressantes

Avant d'aborder les actions qui peuvent être envisagées pour que le sort des DPO s'améliore, essayons d'identifier des fonctions qui présentent des similitudes avec celle de délégué et dont l'étude pourrait être utile. Nous évoquerons le cas des « responsables de la conformité » désignés au titre du code de l'énergie

[77] Délibération CNPD n° 23FR/2021 du 29 juin 2021

puis celui des « responsables de la conformité et du contrôle interne », désignés par les établissements financiers au titre du Règlement délégué (UE) n° 231/2013 de la Commission du 19 décembre 2012[78].

En application de l'article L.111-62 du code de l'énergie[79], toute société de gestion d'un réseau de distribution ou de gaz naturel desservant plus de 100.000 clients a l'obligation de désigner auprès du régulateur un « Responsable de la conformité » chargé de veiller au respect des engagements fixés par le code de bonne conduite dont doit se doter chacun de ces acteurs.

Ce responsable peut être un salarié ou un prestataire. Il a accès aux réunions utiles à l'accomplissement de ses missions ainsi qu'à toutes les informations détenues par la gestion de réseau et ses sous-traitants. Il établit chaque année un rapport qu'il présente à la CRE (Commission de Régulation de l'Energie), et ce rapport est rendu public[80]. Son indépendance doit être garantie et son aptitude professionnelle vérifiée.

La nomination de ces responsables de la conformité est soumise à l'approbation de la Commission de Régulation de l'Energie. À l'occasion d'une audience, un jury vérifie les compétences du candidat et les conditions qui doivent assurer son indépendance. Doivent être fournis à cette occasion un *curriculum vitae* précisant notamment le parcours professionnel et la formation de la personne pressentie, le projet de lettre de mission qui récapitule les missions qui lui seront confiées ainsi que les moyens qui seront mis à sa disposition, le projet de fiche de poste décrivant précisément l'emploi, une déclaration établissant l'absence de conflit d'intérêts, le projet du contrat de travail montrant que la promotion du candidat et ses augmentations salariales à venir ne sont pas liées à l'atteinte de quelconque objectif. Si l'entreprise compte faire appel à un prestataire, elle doit y ajouter le projet de contrat ou de convention.

Après avoir effectué une demande au titre du CRPA[81] auprès de la PRADA[82] de la CRE, l'auteur a obtenu une délibération par laquelle le régulateur a rejeté en 2017 une demande d'approbation de la nomination d'un responsable de la conformité. Dans ce cas, le distributeur d'énergie prévoyait de faire appel à un prestataire, via une convention. Le distributeur d'énergie s'y engageait formellement « *à mettre tous les moyens en œuvre afin de protéger de toute situation mettant en cause son indépendance en tant que responsable de conformité* ». Le projet prévoyait également que le responsable de la conformité puisse, à son initiative et tant que de besoin, signaler à la CRE les difficultés qu'il pourrait rencontrer dans la conduite de ses fonctions.

La commission a considéré que les conditions dans lesquelles il est proposé que le candidat exerce la fonction de responsable de la conformité ne permettaient pas de satisfaire aux conditions d'indépendance nécessaires à l'exercice de cette fonction. En effet, d'après les documents présentés par le distributeur d'énergie, il était prévu que le responsable de la conformité effectue ses missions pour l'équivalent de 20 % de son temps de travail, « *soit une durée de 7 heures de travail par semaine en moyenne, à organiser à sa convenance* ». Le régulateur a considéré qu'une telle disposition pourrait être insuffisante pour assurer les missions de responsable de la conformité. Par ailleurs, la convention était prévue pour une durée d'un an, renouvelable par périodes ne pouvant excéder une année. Pour la commission, la nomination d'un responsable de la conformité pour une durée trop brève « *n'est pas de nature à apporter les garanties d'indépendance suffisantes pour l'exercice de ses fonctions* ».

Projetons-nous maintenant dans le secteur financier. La fonction règlementaire de RCCI (Responsable de la Conformité et du Contrôle Interne) a été créée en septembre 2006. Chaque société de gestion doit confier

[78] Une autre situation est inspirante : celle du médecin qui, selon l'article R4127-5 du code de la santé publique « *ne peut aliéner son indépendance professionnelle sous quelque forme que ce soit* ».
[79] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000023985404
[80] Dans quelques rapports dont l'auteur a pris connaissance, on trouve quelques apports des DPO des sociétés concernées, relatifs à la conformité au RGPD (le « responsable de la conformité » désigné au titre du code de l'énergie n'étant pas chargé de cette thématique et n'étant en aucune façon le responsable hiérarchique du DPO).
[81] Code des Relations entre le Public et l'Administration, qui codifie les dispositions de la loi CADA
[82] Personne Responsable de l'Accès aux Documents Administratifs

la fonction de conformité à un RCCI, internalisé (ou externalisé pour les « petites » structures). Le RCCI doit disposer d'une carte professionnelle délivrée par l'Autorité des Marchés Financiers (AMF), l'autorité de tutelle et de contrôle. La carte professionnelle s'obtient à la suite d'une formation d'une semaine dispensée par l'AMF et d'un examen sous forme d'entretien devant un jury. Ce dernier juge de l'honorabilité du candidat au poste de RCCI, de sa connaissance des obligations professionnelles et de son aptitude à exercer les fonctions. Le jury vérifie également que la fonction Conformité mise en place par la société de gestion dispose de l'autorité et des ressources humaines et techniques suffisantes pour s'acquitter de ses missions de manière appropriée et indépendante. Le RCCI doit par ailleurs avoir accès, au sein de son entreprise, à toutes les informations nécessaires à l'exercice de ses missions.

Le RCCI est associé en amont à la conception des projets, conseille, forme, exerce une veille règlementaire, formule des propositions afin de remédier aux dysfonctionnements qu'il a pu constater lors de l'exercice de sa mission de contrôle. De plus, au moins une fois par an, il remet un rapport sur la conformité aux dirigeants, document également transmis à l'AMF.

En dépit de ses obligations importantes et de l'engagement potentiel de sa responsabilité, le RRCI ne bénéficie pourtant pas d'un statut particulièrement protégé. En effet, sa responsabilité peut être engagée et il peut faire l'objet d'un avertissement, d'un blâme, d'un retrait temporaire ou définitif de sa carte professionnelle, voire d'une interdiction à titre temporaire ou définitif de l'exercice de tout ou partie de ses activités (si l'Autorité délivre la carte professionnelle, elle est donc compétente pour la retirer). Même si le RCCI est le correspondant principal de l'AMF, il est néanmoins bon de rappeler que la conformité de la société de gestion est de la responsabilité finale de son organe de direction, le RCCI intervenant en conseil et en alerte vis-à-vis de lui. C'est seulement en cas de constat de dysfonctionnement grave au sein de l'entreprise vis-à-vis des règles de conformité que le RCCI doit signaler la situation à l'AMF.

Partie IV - Quelles pistes d'actions ?

C'est peu dire que les DPO attendent beaucoup de l'initiative conjointe européenne pilotée par le CEPD. Dans l'attente de ses résultats, nous allons tenter de lister les actions qui pourraient être étudiées afin que les délégués à la protection des données disposent de conditions d'exercice nominales. Certaines d'entre elles pourraient nourrir des travaux menés au sein de la principale association qui regroupe et représente les DPO en France, l'AFCDP.

La question du stress des DPO ne peut pas être occultée et une prise de conscience est nécessaire[83]. Pour commencer, il serait utile de mesurer le stress des professionnels et de mieux le caractériser. Le présent document ne porte que sur un nombre réduit de cas et n'est qu'un examen narratif. Son auteur espère qu'il peut inciter notamment à la réalisation d'une évaluation quantitative et représentative : les témoignages recueillis sont-ils marginaux ou bien cachent-ils une réalité encore plus affligeante ? Une enquête s'inspirant de la démarche du CESIN, mais adaptée au délégué à la protection des données, serait également très utile. L'utilisation de la même méthode pour mesurer le niveau de stress (Cf. Annexe 1) permettrait des comparaisons entre les niveaux de stress des RSSI et des DPO. En revanche, il serait nécessaire d'adapter le questionnaire visant à identifier les sources de stress aux spécificités du métier de DPO : l'AFCDP semble le lieu idéal pour initier de tels travaux. Ces réflexions devraient permettre d'envisager des pistes de modification des causes du stress, soit d'atténuation de ses conséquences. Leur étude peut s'inscrire dans le cadre de communautés de DPO, à travers notamment d'ateliers de « résilience face au stress ». L'enjeu est

[83] Selon l'enquête en ligne et les interviews de DPO réalisées de février à avril 2019 par l'AFPA, 42,7 % des DPO internes se disaient stressés ou très stressés, et près de 40 % des DPO indiquaient rencontrer de temps à autre des situations de tension ou de conflit personnel avec la direction. Source Étude Ministère du travail/DGEFP, réalisée avec l'appui de l'AFPA, en partenariat avec l'AFCDP et la CNIL https://travail-emploi.gouv.fr/IMG/pdf/resultats-enquete-dpd-dpo.2.pdf

important, pour rendre la filière plus apaisée et plus attractive. Pour paraphraser l'une des conclusions de l'étude menée par le CESIN et la société Advens, en travaillant sur les causes du stress du délégué, la conformité au RGPD et à la loi Informatique et Libertés progresseront. Enfin l'étude annuelle menée par l'AFPA (à laquelle participe l'AFCDP depuis sa première édition) pourrait être enrichie d'un volet dédié au stress du DPO et à ses causes, ce qui permettrait de suivre son évolution dans le temps.

Des échanges avec les associations qui représentent les délégués à la protection des données au sein de chaque état membre devraient également être pleins d'enseignements. Observent-elles les mêmes symptômes (et si oui, comment les problèmes sont-ils traités ?) L'AFCDP prévoit d'aborder le sujet avec les autres membres de CEDPO[84] (*Confederation of European Data Protection Organisations* - Confédération des organisations européennes de protection des données), entité qu'elle a fondée en 2011 avec ses homologues néerlandais, allemands et espagnols : ont-ils connaissance de cas similaires à ceux observés en France ? Comment mesurent-ils l'adéquation des moyens dont disposent leurs délégués ? Quelle est leur définition concrète de l'indépendance[85] du DPO ? C'est du côté de l'Allemagne que sont espérés les apports les plus nombreux, la fonction de DSB (pour *datenschutzbeauftragter*) ayant été créé en 1977 pour le secteur privé et en 2001 pour le secteur public à l'occasion de la transposition de la Directive 94/46/CE[86]. Sans attendre ces échanges, des travaux ont été initiés au sein de l'AFCDP pour recueillir auprès de ses milliers de membres la conception concrète de l'autonomie du délégué et des exemples concrets d'atteintes à cette indépendance (Cf. Annexe 2).

Sur sa page « *Désigner un délégué à la protection des données (DPO) ou modifier une désignation*[87] », la CNIL recommande aux responsables de traitement qui s'apprêtent à désigner leur Délégué « *Assurez-vous en particulier que ces 3 conditions sont réunies : le DPO détient les compétences requises, le DPO dispose de moyens suffisants, le DPO a la capacité d'agir en toute indépendance* ». Très franchement, combien de dirigeants ont pris connaissance de ces recommandations ? Visiblement aucun de ceux évoqués dans les témoignages recueillis. Ne faudrait-il pas en sus que la CNIL adresse à chaque responsable de traitement qui vient de désigner son DPO interne un courrier « mettant les points sur les i » et lui rappelant ses obligations concernant son délégué à la protection des données ? Ce courrier pourrait être rédigé pour pouvoir également être utile aux « superviseurs » des DPO, afin qu'ils leurs assurent un « cocon » favorable à la bonne réalisation de leurs missions plutôt que de les corseter. L'idéal serait que le message amène l'organisation à prendre conscience du stress potentiel vécu par son délégué et à avoir un mouvement naturel de soutien, de reconnaissance et d'empathie envers lui. À titre d'exemple, la Commission pourrait expliquer au responsable de traitement que le DPO ne peut pas faire tout seul et qu'il a besoin d'interagir avec les opérationnels (dès l'inventaire des traitements en vue de constituer le registre). L'analogie évoquée par Lucy Savary – DPO interne mutualisée - lors de l'Université AFCDP des DPO de février 2023, est excellente pour cela[88] : elle a comparé le délégué à la protection des données à un moniteur d'auto-école, qui apprend aux autres à conduire mais qui ne tiendra pas le volant pour eux plus tard. Un DPO ne fait pas : il explique là où il faut arriver et ne peut pas porter toute la misère du monde sur ses frêles épaules. Un autre membre de l'AFCDP, Alexandre Eloy, regrette que des directions, auprès desquelles on compare le DPO à un chef d'orchestre, le perçoivent plutôt

[84] www.cedpo.eu
[85] Le mot indépendance provient du latin *in* (privé de) et *dependere* (être suspendu à).
[86] À titre d'exemple, en 2011, la cour fédérale allemande du travail a statué qu'un responsable de traitement ne pouvait mettre fin au mandat d'un DSB interne afin d'en désigner un externe. Il s'agissait d'une entreprise qui, après avoir fusionné avec d'autres entreprises pour former un groupe, souhaitait confier à un délégué externe la conformité des traitements mis en œuvre par l'ensemble du groupe. Or la loi fédérale révisée en septembre 2010 déjà exigeait une « bonne raison » pour que soit mis fin à la mission d'un délégué à la protection des données allemand. Le juge a estimé que la stratégie du chef d'entreprise ne répondait pas à ce critère. Le licenciement de l'ancien délégué interne à la protection des données (qui n'avait pas démérité) a été jugé nul et non avenu (jugement du 23 mars 2011 sous le numéro de dossier 10 AZR 562/09. https://www.bundesarbeitsgericht.de/entscheidung/10-azr-562-09/).
[87] https://www.cnil.fr/fr/designation-dpo
[88] Voir son interview réalisée le 9 février 2023 : https://afcdp.ubicast.tv/permalink/v12663c07ae557lxiiyv/iframe/

à tort comme un homme-orchestre… Parallèlement, la Commission pourrait adresser aux délégués à la protection des données nouvellement désignés un courrier destiné à les aider, à les mettre sur les bons rails.

La CNIL aurait-elle les moyens de s'intéresser aux cas de « rotations » rapides de DPO ? Que cachent-t-elles ? N'est-il pas inquiétant de voir un organisme changer de Délégué à un rythme élevé ? La Commission ne pourrait-elle pas, dans certains cas, adresser un questionnaire à chaque départ de DPO pour en connaître la raison. En effet, actuellement, il suffit au responsable de traitement qui met fin à la mission de son délégué d'envoyer un simple courriel au service des délégués à l'adresse électronique indiquée dans l'accusé réception de la désignation. N'y aurait-il pas moyen de créer un téléservice qui serait le pendant de celui utilisé pour les désignations, obligeant à indiquer les raisons et le contexte de la fin de mission ? Il est intéressant de noter que l'une des questions (la n°26) que la CNIL adresse aux responsables de traitement qu'elle contrôle actuellement dans le cadre de l'action conjointe européenne 2023 (Cf. Annexe n°4) porte sur ce sujet : « *Dans quel contexte la désignation du précédent délégué à la protection des données a-t-elle pris fin (changement de poste, démission, licenciement) ?* ».

L'autorité de contrôle pourrait également, sur la base d'informations qu'elle est seule à détenir, s'intéresser à « l'espérance de vie » d'un délégué à la protection des données. Selon certaines études[89], les RSSI ne resteraient en moyenne que vingt-six mois à leur poste à cause du stress. Qu'en est-il des délégués à la protection des données ? Dans le même ordre d'idée, combien de temps dans sa carrière une personne peut-elle espérer être DPO ?

Il conviendrait également d'essayer d'objectiver l'évaluation de l'adéquation des ressources dont bénéficie le DPO. On a vu *supra* que la CNPD luxembourgeoise s'est principalement focalisée sur le temps dont dispose le délégué pour exercer ses missions et les moyens humains sur lesquels il peut s'appuyer. Sur son site Web, la CNIL donne les exemples complémentaires suivants : « *Cela implique en particulier que le DPO bénéficie de moyens matériels adéquats, puisse accéder aux informations utiles, soit associé en amont des projets impliquant des données personnelles et soit facilement joignable par les personnes concernées* ». Dans son guide DPO, la CNIL y ajoute l'association du DPO à toutes les questions relatives à la protection des données, le fait de lui permettre d'entretenir ses connaissances spécialisées ou la constitution d'une équipe à son service.

Malgré les publications existantes, comment juger objectivement avant un éventuel contrôle de la CNIL si les moyens matériels (notamment le budget) sont « adéquats » ? Il en est de même pour l'appréciation du temps suffisant dont doit disposer le DPO pour qu'il puisse accomplir ses tâches. Quelle méthode suivre ? Sur ce chantier, comme sur le précédent, l'AFCDP pourrait s'investir.

Ne serait-il pas judicieux de renforcer la procédure de désignation d'un délégué à la protection des données en s'inspirant de ce que font la CRE (Commission de Régulation de l'Energie) concernant les « Responsables de la conformité » et l'AMF (Autorité des Marchés Financiers) concernant les RCCI ? Sans aller jusqu'à un passage devant un jury, ne faudrait-il pas prévoir une vérification par la CNIL des critères principaux sur la base d'un dossier que fournirait le responsable de traitement (comprenant le *curriculum vitae* du DPO, la lettre de mission qui récapitule les missions qui lui sont confiées, la description des moyens mis à sa disposition, la fiche de poste décrivant précisément l'emploi, une déclaration établissant l'absence de conflit d'intérêts, etc.) ? Dans un premier temps, le téléservice qui permet de désigner en ligne un délégué à la protection des données auprès de la Commission pourrait être enrichi. Pour mémoire, avant l'entrée en application du RGPD, il convenait de communiquer bien plus de précisions lors de la désignation d'un Correspondant Informatique et Libertés. Le responsable de traitement devait notamment décrire les moyens qu'il comptait mettre à disposition de son CIL afin que celui-ci assure pleinement ses missions.

[89] *CISO Stress Report*, Nominet, 2020, https://media.nominetcyber.com/wp-content/uploads/2020/02/Nominet_The-CISO-Stress-Report_2020_V10.pdf

On peut aussi regretter l'abandon de l'obligation qu'avaient les responsables des traitements lors de la désignation d'un Correspondant Informatique et Libertés d'informer les instances représentatives du personnel. Cela pourrait notamment donner la possibilité au CSE (Comite Social et Economique) d'émettre un avis sur la réelle indépendance du DPO.

Il serait utile également de concevoir des messages à l'attention des directions des ressources humaines dont certaines méritent peu leur appellation. Concernant les DPO, la prise en compte du stress ne devrait-elle pas en priorité être faite par l'employeur et se traduire dès l'élaboration de la fiche de poste ?

Enfin, ne faudrait-il pas revoir les lignes directrices WP243 (relatives au DPO), rédigées par le G29 avant l'entrée en application du RGPD ? Il est probable que ce soit l'une des propositions qu'on peut s'attendre à trouver dans le rapport final de l'action conjointe européenne de 2023 qui sera publié début 2024. Le document pourrait également être enrichi de larges passages du « Guide du DPO » de la CNIL.

Plusieurs des pistes qui viennent d'être évoquées l'ont déjà été il y a plus de quatorze ans. Dans le cadre du Mastère spécialisé « Management et Protection des Données Personnelles » de l'ISEP, une thèse professionnelle avait été soutenue en 2009 sur la question suivante : « *Donne-t-on les moyens au Correspondant informatique et libertés d'être efficace ?* » (Op.cit.). Son auteur, Aurélie Goyer, faisait déjà le constat suivant : « *Les conditions de travail des Correspondants Informatique et Libertés restent très hétérogènes : « Globalement très (trop) peu de CIL n'ont le temps ni l'aide humaine et/ou matérielle pour exercer leurs missions.../... on déplore un réel manque de moyens compte tenu des besoins exigés par les missions à remplir.* ». Aurélie avait mené un sondage auprès des professionnels concernés avec l'aide de l'AFCDP et de la CNIL. À la question « *Comment le CIL peut-il obtenir plus de moyens ?* », trois leviers avaient été cités en priorité : 1) Un formulaire de désignation bien plus exigeant et précis, des actions de la CNIL vis-à-vis des responsables de traitement dès la réception de la désignation (opération de communication, étude des bilans, sondage auprès des Responsables de traitement, etc.), et quelques contrôles de responsables de traitement pour vérifier les conditions d'exercice du CIL ; 2) L'établissement de benchmarking entre CIL afin de connaître les moyens dont disposent d'autres correspondants désignés pour des entités similaires ; 3) Des textes plus clairs et incitatifs sur ce point, comme ils l'étaient en Allemagne, par exemple. En effet, concernant la question des moyens alloués au *Beauftragter für Datenschutz*, le paragraphe 4f (5) de la loi allemande précisait à l'époque que : « *Les organismes publics et non publics sont tenus d'apporter leur soutien au délégué à la protection des données dans l'exécution de sa mission et, dans la mesure où cela est nécessaire à l'exécution de sa mission, de mettre à sa disposition du personnel auxiliaire, des locaux, des installations, des appareils et des moyens* ».

Pour une exigence accrue des DPO internes envers leur employeur

Etudions maintenant les actions qui peuvent être envisagées au niveau des DPO eux-mêmes, sur la base de l'analyse des témoignages recueillis.

Il serait souhaitable que les futurs délégués à la protection des données se montrent plus incisifs lors de leur parcours d'embauche afin d'être plus sélectifs dans le choix de leur employeur. Peu d'entre eux ont posé les quelques « bonnes questions » ou su détecter les signaux qui auraient dû leur mettre la puce à l'oreille. N'est-il pas inquiétant qu'on cherche à dissuader le candidat d'échanger avec le délégué qui quitte son poste ? Il est vrai que, souvent, une part importante du parcours se fait auprès d'un cabinet de recrutement et non auprès du futur éventuel employeur. D'après les témoins qui en sont passés par là, non seulement le cabinet n'avait aucune idée du métier de délégué, mais il se montrait incapable d'apporter la moindre réponse à des questions aussi basiques que « *Quelles sont les raisons du départ du DPO actuel ?* », « *Qui sera mon superviseur ?* », « *Disposerai-je d'un budget ?* » ou « *Comment, très concrètement, sera assurée mon indépendance ?* ». À l'occasion d'un sondage réalisé par l'AFCDP auprès de ses membres, le *verbatim* suivant avait été collecté : « *Lors de mon entretien d'embauche, j'aurai dû mieux questionner mon employeur sur ses véritables intentions de mise en conformité avec le RGPD. Entre les promesses du début et la réalité du terrain, l'écart a été impressionnant* ».

L'auteur a également noté que quasiment aucun témoin n'avait pris soin de formaliser un plan stratégique (et, surtout, de le partager avec la grande direction). Pourtant, c'est un exercice obligé lors de toute prise de poste. Un plan stratégique classique comprend un diagnostic, la description de l'environnement, l'écoute clients - à commencer par le responsable de traitement et les directions Métiers-, l'offre de service, les ambitions, les leviers, les moyens, les feuilles de route - une par membre de l'équipe du DPO-, les indicateurs et les objectifs - à court et moyen terme). La présentation par le nouveau délégué à la protection des données au responsable de traitement du plan stratégique permet de vérifier l'alignement avec les attentes de la direction. Dans plusieurs cas décrits au début du présent document, le *clash* a mis en évidence un écart considérable entre ce que le DPO s'était fixé comme objectifs, méthode et priorités, et ceux de sa direction. On rappellera utilement l'un des griefs sur lequel une déléguée à la protection des données a été licenciée[90] : y était mentionné, parmi les défaillances dans l'exercice de ses fonctions « *l'absence de production d'une feuille de route* ». L'absence d'indicateurs est également problématique : pour une grande direction, une fonction qui n'en produit pas n'existe tout simplement pas.

Dans les cas (de plus en plus nombreux) de remplacement d'un DPO, il est indispensable de bien comprendre ce qui est attendu par la direction : une continuité ? Une inflexion ? Un repositionnement ? Et, dans le dernier cas, de quelle ampleur et dans quelle nature ? Et où sont les priorités de la grande direction ? À quelle fréquence et sous quelle forme souhaite-t-elle disposer d'un *reporting* ? Un nouveau délégué à la protection des données doit donc s'intéresser à son prédécesseur (quelle était sa « doctrine », son « style » ?), pour s'assurer que le responsable de traitement ne va pas être déboussolé par une nouvelle façon de faire. Lors de l'Assemblée générale de l'AFCDP qui s'est tenue le 22 juin 2022, un chercheur de la chaire *Good In Tech*[91] (Sciences Po), Alexis Louvion, a fait part de ses travaux sur « *Le rôle d'une association dans la construction d'un groupe professionnel : un regard sociologique* ». Lors de son intervention, il a insisté sur la nécessité « *de détecter les conflits possibles de rôles entre la perception qu'a le DPO de sa mission et celle qu'en a le responsable de traitement. Le DPO doit absolument cartographier le « Là où l'on m'attend » versus le « Là où je veux être ». Si aucune surface commune n'existe, on court à la catastrophe. Et s'il existe des différences, il faut les clarifier et en discuter avec qui de droit de toute urgence* ».

Dans le même ordre d'idée, chaque délégué à la protection des données devrait faire l'effort de soumettre à la signature du responsable de traitement la Charte de déontologie du DPO[92], afin de s'assurer de son réel soutien[93]. Cette charte, dans son chapitre 4 (« Éthique du Délégué à la protection des données »), comprend un passage dédié à l'indépendance du DPO : « *Le Responsable de traitement/sous-traitant doit définir et faire connaitre les mesures garantissant l'indépendance du Délégué à la protection des données. Il doit s'abstenir de toute ingérence et met le Délégué à la protection des données dans une situation qui lui permet de fait d'assurer cette indépendance, ce qui inclut la mise à disposition de moyens […] Il n'a, dans son rôle de Délégué à la protection des données, aucun compte à rendre à un supérieur hiérarchique. Il dispose d'une liberté organisationnelle et décisionnelle dans le cadre de sa mission. Il agit de manière indépendante, ne reçoit aucune instruction dans l'exercice de sa fonction et arrête seul les décisions s'y rapportant. Il est libre de consulter la CNIL ou tout sachant, dans la limite du cadre de sa fonction et de l'exercice de ses missions* ».

Ce même passage aborde également le cas des délégués à la protection des données qui œuvrent à temps partiel : « *Le Responsable de traitement/sous-traitant veille : à limiter les tâches qui incomberaient au Délégué à la protection des données au titre d'autres missions ; à s'assurer que le Délégué à la protection des données ne subisse pas de préjudices du fait de sa mission lors de l'étude annuelle de ses performances (gestion des ressources humaines) au titre de ses autres*

[90] Conseil d'Etat, Décision n° 459254 du 21 octobre 2022
[91] www.sciencespo.fr/nous-soutenir/fr/nos_projets/chaire-good-in-tech/
[92] https://afcdp.net/charte-de-deontologie-du-dpo/
[93] Il est intéressant de noter que certains DPO externes le font afin de « qualifier » la réelle volonté de leur futur client de se conformer au RGPD.

responsabilités ; à faire en sorte qu'une fois sa mission terminée, le Délégué à la protection des données poursuive, au sein de l'organisme, au moins la carrière qu'il aurait eue s'il n'avait pas occupé la fonction de Délégué à la protection des données ».

Lors d'un sondage que l'AFCDP avait mené auprès de ses membres en 2020 sur la place et les moyens du DPO, ces *verbatim* illustrent l'intérêt de la démarche : « *La charte de déontologie du DPO permet de clarifier les choses, de « qualifier » son responsable de traitement. Son absence entraîne des pressions souvent subtiles mais pourtant réelles : isolement progressif, manque d'accès aux ressources, travail dans l'urgence, tentative pour noyer le DPO sous des dossiers peu importants afin qu'il ne puisse pas se focaliser sur les dossiers stratégiques* ». Si d'emblée le responsable de traitement refuse de signer cette charte (qui, pour l'essentiel, ne fait que reprendre le RGPD), la personne qui occupe le poste de délégué à la protection des données peut se considérer comme avertie. À elle de savoir si elle compte rester au sein de l'organisme.

La présentation au responsable de traitement du plan stratégique ou la soumission de la charte de déontologie doivent également être utilisées par le nouveau DPO pour lui poser les questions suivantes : « *Aujourd'hui tout va bien. Vous me réservez un accueil chaleureux et m'assurez de votre soutien. Qu'en sera-t-il quand je vous signalerai une non-conformité manifeste et que je formulerai un conseil qui peut gêner le « business » ? Qu'en sera-t-il si je suis soumis à des pressions de la part de directions Métier qui n'accepteraient pas mes analyses ?* ». Peut-être sera-t-il surpris, mais mieux vaut prévenir que guérir. Mais encore faut-il que le délégué rencontre le responsable de traitement. L'AFCDP a mené en novembre 2019 un sondage auprès de ses membres pour essayer de décrire les caractéristiques d'une désignation « idéale » d'un DPO. Les professionnels étaient d'abord invités à indiquer les mesures qui, d'après eux, semblent indispensables avant ou lors d'une désignation de DPO. Avec surprise, la nécessité d'avoir un entretien en tête à tête avec le Responsable de traitement n'était jugée indispensable que pour 43 % des répondants (et 25 % des répondants avouaient n'avoir tout simplement pas essayé). Pourtant, l'implication réelle et directe de la direction dès les premiers moments de la désignation est impérative. Comme l'indique l'un des répondants, « *Trop souvent les DPO sont nommés par des dirigeants seulement pour faire bonne figure devant la CNIL. Une sensibilisation des dirigeants en amont de la désignation du DPO serait un plus pour éviter le rejet de recommandations élémentaires sous le seul prétexte que « Le RGPD ne vise que les GAFA, la CNIL ne s'intéressera jamais à nous ». Le DPO aura beau faire tout son possible pour être le « chef d'orchestre » de la conformité au sein de l'entreprise, si la Direction ne le soutient pas clairement, il sera le chef d'orchestre de chaises vides* ».

Enfin rappelons aux DPO qui viennent de rejoindre un nouvel organisme que la période d'essai a deux finalités : si elle sert à l'employeur pour apprécier la valeur professionnelle du salarié et le confirmer dans son poste, elle sert aussi au salarié à vérifier qu'il se trouve bien dans l'entreprise et dans le poste pour lequel il a été engagé. À son approche, les nouveaux embauchés devraient se livrer à une analyse la plus honnête possible pour leur éviter de perdre un temps précieux. Plusieurs des témoins ont laissé passer ce moment crucial et l'ont regretté. Pour faire le lien avec l'un des sujets précédents, la finalisation du plan stratégique et sa présentation au responsable de traitement doivent impérativement se faire avant la fin de la période d'essai (ce qui est cohérent avec une prise de poste qui est généralement jugée au bout de 90 jours).

La question de la formation des délégués à la protection des données doit également être abordée. Certains des témoins évoqués en première partie de ce document disposaient-ils réellement de l'expertise et de l'expérience requises ? En aparté, les services de la CNIL se disent souvent déçus du niveau de formation des délégués. À ce sujet, il est pertinent de rappeler l'un des enseignements de la plus récente des études réalisées par l'AFPA sur les DPO désignés auprès de la CNIL (1.811 répondants[94]) : ils sont nombreux à être peu ou pas assez formés. En effet, 33 % d'entre eux avouent n'avoir suivi aucune formation depuis 2016 et 24 % des répondants indiquent n'avoir suivi dans la même période qu'une ou deux journées de

[94] *Observation de la fonction de Délégué à la Protection des Données (DPO) - Les besoins de formation des DPO 2022*, Etude réalisée par l'AFPA, en partenariat avec le Ministère du Travail, la CNIL, l'AFCDP et l'ISEP https://travail-emploi.gouv.fr/actualites/l-actualite-du-ministere/article/le-delegue-a-la-protection-des-donnees-dpo-un-metier-en-forte-evolution

formation. Les délégués à la protection des données peuvent s'orienter vers des formations longues proposées par des universités ou des écoles (voir, entre autres, la liste des formations DPO réalisée par l'AFCDP[95] et la page dédiée sur le site de SupDPO[96]). On notera que, parmi les questions soulevées par la CNIL dans le cadre des contrôles qu'elle réalise au titre de sa participation à l'action conjointe européenne pour 2023, figure celle-ci : « *De combien d'heures de formation annuelle le délégué à la protection des données dispose-t-il/elle pour développer et maintenir son expertise professionnelle en matière de protection des données à caractère personnel ? Qui valide ses demandes de formation et sur quels critères ? Fournir la liste des formations suivies lors des années précédentes par le délégué à la protection des données, ainsi que les formations prévues pour l'année en cours* ».

Les formations devraient également aborder la question de l'assertivité du DPO. Il y a quelques années déjà, le comité scientifique du Mastère Spécialisé de l'ISEP « Management et Protection des Données Personnel[97] » a enrichi le cursus d'un module dispensé par Raffaella Bottino, consultante au sein de Miaconsulting, dans lequel elle enseigne cette qualité. En effet, dans la négociation, c'est la posture assertive qui se démontre la plus efficace (davantage que le « marketing de la peur[98] »). Elle consiste à être capable d'affirmer les limites que les autres doivent respecter tout en s'exprimant et en protégeant son estime personnelle sans agressivité ni passivité. Elle est indispensable dans toutes les situations demandant une réponse claire et précise, jusqu'aux situations de dérive ou de conflit. Elle permet aussi de maintenir une relation viable et de poursuivre le dialogue. Comme l'indique Raffaella Bottino, « *L'assertivité, c'est défendre son droit en respectant l'autre. Un négociateur assertif est clair sur ses besoins et les formule explicitement sans agressivité. C'est une posture indispensable pour tout Délégué à la Protection des Données* ». Elle ajoute que l'assertivité s'apprend comme tout comportement. La maîtrise de l'assertivité tire sa source de la confiance en soi (en tant que personne et professionnel et expert) et d'une bonne utilisation des techniques de communication (qualité du contact sécurisante pour l'interlocuteur, écoute, questionnement, formulation précise sans atténuation langagière du problème, maîtrise émotionnelle). Un auto-quiz est proposé en annexe n°5 afin d'évaluer son assertivité.

À certains égards, il serait aussi utile de rappeler qu'il revient au responsable de traitement de prendre les décisions, de façon éclairée sur la base des conseils qu'ils ont formulés auprès de lui. Le DPO a un rôle d'accompagnement (et non pas de décision), il apporte son expertise auprès de la direction afin que celle-ci puisse assurer la conformité des traitements. L'auteur a relevé dans quelques témoignages un sentiment de grande frustration chez des délégués à la protection des données qui s'attendaient à ce que l'intégralité de leurs recommandations soient transposées et qui constatent que certaines d'entre elles restent ignorées. Les services de la CNIL semblent faire le même constat : il leur arrive de constater que des délégués, mécontents de leur sort, ont en fait mal interprété leur rôle et s'indignent à chaque fois que leur direction, après avoir étudié leurs conseils, ne les suivent pas. Dans de tels cas, le délégué concerné devrait commencer par questionner sa pratique : son analyse était-elle pertinente ? A-t-il su la présenter de la « bonne » façon, avec les bons arguments et auprès des bons interlocuteurs ? Sa recommandation était-elle suffisamment fondée, claire, pragmatique, opérationnelle ? On rappellera l'un des griefs sur lequel une déléguée à la protection des données a été licenciée[99] : y était mentionné, parmi les défaillances dans l'exercice de ses fonctions, « *des alertes répétées de non-conformité non motivées et non documentées* ». Tout DPO doit donc s'attendre, qu'un jour où l'autre, l'un de ses conseils ne soit pas suivi. Il doit alors en conserver une trace écrite (et en faire état dans son rapport annuel, s'il suit cette bonne pratique). Dans l'idéal, il appartient au responsable de traitement de consigner les raisons pour lesquels il n'a pas suivi la recommandation de son Délégué… mais cela est

[95] https://afcdp.net/la-formation-des-dpo/
[96] https://supdpo.fr/formations/
[97] https://formation-continue.isep.fr/offres-de-formation/formations-diplomantes/mastere-specialise-management-et-protection-des-donnees-a-caractere-personnel/
[98] B.Rasle, *Le marketing de la peur est-il le plus productif ?* », septembre 2017 https://www.anaxia-conseil.fr/le-marketing-de-la-peur-est-il-le-plus-productif.html
[99] Conseil d'Etat, Décision n° 459254 du 21 octobre 2022

excessivement rare. Sur ce sujet, on notera, parmi les questions soulevées par la CNIL dans le cadre de ses contrôles (Cf. Annexe n°4), celle-ci : « *Dans le cas où l'avis du délégué à la protection des données n'est pas suivi par l'organisme, les raisons en sont-elles documentées ?* ».

Ne faudrait-il par également inciter les DPO à définir, établir, faire connaitre et défendre leur indépendance[100] ? Le respect de cette autonomie est essentiel pour que le délégué soit en mesure d'agir conformément aux intentions de la loi. Bien que la fonction de DPO a été créée en Norvège dès 2001, l'autorité de contrôle Datatilsynet reconnaissait avoir une connaissance insuffisante de leurs conditions d'exercice. Elle a donc mené un sondage auprès de 1.341 Délégués en fin d'année 2020[101]. On y découvre que, à la question « *Dans quelle mesure pensez-vous que la direction et vous-même avez à peu près la même compréhension de votre indépendance en tant que DPO ?* », 39 % des répondants avaient indiqué que leur direction avait une interprétation assez éloignée de leur propre conception de leur indépendance. Cela rejoint l'un des *verbatim* qui avait été recueilli par l'AFCDP sur ce même sujet en septembre 2020, « *Il est difficile de faire comprendre aux dirigeants la notion d'indépendance du DPO. Une fois cette difficulté aplanie, il est plus facile d'aborder la question du budget et des moyens* », « *Dès les premiers contacts, certains chercheront à vous tester, à piétiner votre indépendance. Il faut vous y préparer et y résister car cela est difficile à rattraper* ». Il est intéressant de noter, parmi les points soulevés par la CNIL dans le cadre de ses contrôles, l'absence de question directement liée à l'indépendance du DPO. La Commission semble avoir préféré traiter ce sujet par des questions indirectes (Cf. Annexe n°4) : « *Les analyses ou recommandations du délégué à la protection des données peuvent-elles être orientées, amendées ou soumises à validation par un supérieur hiérarchique ou par un autre service ?* », « *Le délégué bénéficie-t-il de garanties lui assurant qu'il n'est pas pénalisé (par exemple, sur l'obtention d'avantages professionnels ou l'avancement de carrière) pour l'exercice de ses fonctions ?* » et la question sur l'existence d'un budget et d'une autonomie budgétaire.

On se rappelle que lors de la transposition de la directive de 95/46/CE, en 2004, certains parlementaires se montraient réservés quant à la formule du délégué à la protection des données[102] : « *Le système des correspondants à la protection des données offre-t-il des garanties d'indépendance suffisantes ?* », « *Nous restons très réservés sur ce système des correspondants, même si le rapporteur assure que l'exercice de leur mission se fera en toute indépendance* » déclarait à l'époque le député Frédéric Dutoit (député des Bouches-du-Rhône de 2002 à 2007, parti communiste) tandis que le sénateur Robert Bret (sénateur des Bouches-du-Rhône de 1998 à 2008, parti communiste) craignait que, « *au mieux, il [le CIL] exercera un travail de vérification routinière largement superficielle, au pire, il laissera passer des fichiers un peu problématiques par crainte de voir surgir des difficultés dans l'entreprise* ».

---

[100] Dans le document *Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001*, on trouve le passage suivant : « *Dans la pratique, il peut être difficile pour le DPD d'exercer ses fonctions en toute indépendance. Il va sans dire que la situation et la personnalité du DPD joueront un rôle, mais on peut généralement supposer que certains éléments tendront à affaiblir la position d'un DPD : délégué à temps partiel, délégué avec un contrat à durée limitée, délégué placé sous un superviseur, délégué dépourvu de son propre budget.* » et « *La bonne exécution des tâches du délégué à la protection des données exige souvent que celui-ci adopte une attitude ferme et insistante, y compris avec les responsables qui occupent une position élevée dans l'organisation. Ainsi, il peut être perçu, au mieux, comme un acteur de la bureaucratie ou, au pire, comme un trouble-fête. Le DPD doit donc être capable de résister aux pressions et aux difficultés qui accompagnent ce poste important.* ». Le document *Professional Standards for Data Protection Officers* a été formalisé par le réseau des DPO des institutions européennes et publié le 14 octobre 2010. https://edps.europa.eu/sites/edp/files/publication/10-10-14_dpo_standards_en.pdf. Pour sa part, l'auteur qualifie souvent le DPO « *d'élément d'inconfort utile* ».

[101] *Data Protection Officer survey On working conditions for Data Protection Officers and compliance with data protection legislation in Norwegian enterprises*, Septembre 2021, https://www.datatilsynet.no/contentassets/e9a029532bf14a69adf4515922245e8f/data-protection-officer-survey-2020-21.pdf

[102] B. Rasle*, Collègues DPO : Le bilan annuel est un outil précieux – Faisons-en une bonne pratique*, 29 mars 2020, www.linkedin.com/pulse/coll%C3%A8gues-dpo-le-bilan-annuel-est-un-outil-pr%C3%A9cieux-faisons-en-rasle/

En première lecture au Sénat, Charles Gautier† (sénateur socialiste de Loire-Atlantique) s'était inquiété du manque d'indépendance des correspondants de la CNIL en entreprise[103] : « *...la nomination de correspondants à la protection des données nous semble dangereuse. Sous prétexte de simplifier la procédure, de nombreux fichiers privés ne seront plus soumis à la CNIL. En outre, ces correspondants ne disposeront d'aucune garantie d'indépendance.* ». En réponse, M. Alex Türk, à l'époque Commissaire de la CNIL et rapporteur des travaux de la commission du Sénat, avait indiqué que les CIL demeureraient intégrés dans la hiérarchie de l'entreprise ou de la collectivité, mais que les expériences étrangères [allemande et néerlandaise] avaient montré qu'ils pouvaient exercer un véritable pouvoir d'influence. Il a en outre précisé que certaines protections étaient prévues pour ces correspondants vis-à-vis de leur employeur.

Ce point avait été de nouveau abordé en seconde lecture à l'Assemblée : on relève, parmi les propositions de la commission des lois, le passage suivant[104] : « *Conforter le statut du « correspondant à la protection des données » en prévoyant que celui-ci doit exercer sa mission en toute indépendance et bénéficier, à cet effet, des qualités requises. La garantie de l'indépendance est donc décisive puisqu'elle conditionne l'efficacité et la pertinence du dispositif des correspondants. A cet égard, les lois en vigueur en Allemagne et aux Pays bas précisent que le correspondant ne reçoit dans le cadre de ses fonctions aucune instruction de la part du responsable du traitement ou de l'organisation qui l'a désigné, ou encore que le correspondant ne doit subir aucune discrimination ou « inconvénient » du fait de l'exercice de ses fonctions. Ainsi, le correspondant allemand est-il directement placé sous l'autorité du directeur afin de ne pas subir de pression de la part de l'encadrement intermédiaire de son organisation. C'est pourquoi, après avoir adopté un amendement rédactionnel du rapporteur, la Commission a adopté un amendement du même auteur précisant que le correspondant devait agir « de manière indépendante » et posséder « les qualifications requises ». En revanche, elle a rejeté un amendement de M. Patrick Bloche prévoyant que la CNIL doit « agréer » la désignation du correspondant, le rapporteur ayant indiqué que ce dispositif aurait pour conséquence d'alourdir inutilement la charge de travail de la CNIL* ».

Dans une interview accordée à l'IAPP, Cathal Ryan, *Assistant Commissioner* de l'autorité de contrôle irlandaise DPC, avait déclaré en janvier 2020[105] : « *Le délégué à la protection des données doit être indépendant et doit pouvoir soulever les questions relatives à la protection de la vie privée au plus haut niveau de la direction. Il est vivement conseillé aux entreprises de prendre au sérieux l'apport du DPD et d'éviter de se contenter de pourvoir le poste avec une personne insuffisamment qualifiée pour satisfaire aux exigences du RGPD. Trop souvent, ils n'ont souvent pas le soutien de l'organisation dans le cadre de leurs missions. C'est pourquoi un DPD doit être dotée d'une personnalité forte, il ne doit pas lâcher prise, quelle que soit la réaction de l'organisation aux questions qu'il soulève. La fonction n'étant pas particulièrement facile, les organisations devraient proposer des salaires élevés afin d'attirer des personnes ayant les connaissances et l'expérience nécessaires pour réussir* ».

L'auteur a bénéficié du témoignage de Yann-Hervé Beulze. Au cours de sa carrière, il a été RCCI (Responsable de la Conformité et du Contrôle Interne), Correspondant risques, RSSI et DPO. Yann-Hervé formule trois conseils concernant le délégué à la protection des données : à l'identique des autres fonctions de conformité, ne pas être le « gêneur permanent » et s'évertuer à montrer les bénéfices de l'effort de toutes et tous, savoir hiérarchiser les sujets pour être pertinent vis-à-vis du patron (« *Je traite seuls les petits bobos mais je n'hésite pas à aller le voir sur les sujets importants* »), ne pas se laisser prendre par « *l'ardeur du néophyte* », au risque de saturer tout le monde avec les données personnelles – à commencer par le patron. Il faut savoir doser, savoir cadencer, savoir quand il est judicieux de parler du RGPD… mais aussi quand il est judicieux de savoir se taire afin de rendre le sujet « digérable » par l'organisme. Pour lui, le profil psychologique et

[103] Cf. les discussions en deuxième lecture au Sénat du projet de loi
http://www.senat.fr/cra/s20040715/s20040715H1.html
[104] Cf. Rapport n° 1537 de M. Francis Delattre, fait au nom de la commission des lois, déposé le 13 avril 2004
https://www.assemblee-nationale.fr/12/rapports/r1537.asp
[105] *Seeking clarity on the role of the DPO*, par Chelsea Marcous, 28 janvier 2020, IAPP, https://iapp.org/news/a/seeking-clarity-on-the-role-of-the-data-protection-officer/

comportemental du DPO est important. Quel est son « caractère », son tempérament[106] ? Certes, il faut être analytique (comme pour un RCCI ou un Directeur des Risques), mais il faut aussi être un bon communiquant et pédagogue pour ne pas rester paralysé durant les moments cruciaux (il doit échapper au syndrome du « lapin pris dans les phares de la voiture »). Enfin il estime que le délégué devrait se former sur des sujets tels que « *Savoir gérer son patron et comment s'adresser à lui* », « *Savoir gérer son stress et les conflits* » et « *Savoir communiquer* ».

Les DPO pourront utilement rester à l'écoute du vieux serpent de mer du statut de l'avocat en entreprise, inspiré du modèle allemand. Chez nos voisins, on estime à environ 40.000 le nombre d'avocats salariés qui exercent leur métier en entreprise (et non pas dans un cabinet). Par une loi adoptée le 17 décembre 2015, le législateur allemand a consolidé ce statut en posant les conditions d'un exercice indépendant du métier : l'avocat d'entreprise ne doit pas recevoir d'instructions hiérarchiques qui empêcheraient une analyse indépendante du dossier qu'il traite. Pour éviter toute ambiguïté, la loi exige que cette indépendance soit garantie contractuellement et dans les faits. En France, à l'occasion des débats sur le budget 2021 de la Justice, le garde des Sceaux avait réactivé la polémique, car si l'idée est soutenue par les associations représentant les intérêts des juristes d'entreprises et directeurs juridiques, elle est accueillie avec plus de réserve par les institutions représentatives des avocats qui dénoncent l'absence d'indépendance des juristes d'entreprise en raison du lien de subordination les unissant à leur employeur[107].

Abordons maintenant la question du budget du DPO, qui est un facteur d'autonomie. Il faut constater que la situation actuelle est loin d'être satisfaisante : dans le cadre d'un sondage mené en 2019 auprès de ses membres, l'AFCDP révélait qu'un quart des répondants n'avait même pas essayé d'obtenir un budget spécifique, tandis que 34 % indiquaient avoir tenté d'en obtenir un, mais sans succès. Cela est regrettable, car outre le fait de participer concrètement à son indépendance, l'existence d'un budget aide le DPO à mener à bien ses missions et lui donne une sorte de « reconnaissance » (dans de nombreuses entreprises, une fonction qui n'a pas de budget… n'existe pas aux yeux de la direction). D'après la dernière étude en date réalisée par l'Afpa sur la fonction de DPO[108], 60 % d'entre eux n'ont toujours pas de budget[109]. Parmi les questions soulevées par la CNIL dans le cadre de sa campagne de contrôle (Cf. Annexe n°4) on relève celle-ci : « *L'organisme a-t-il alloué un budget spécifique aux activités du délégué à la protection des données ? Le cas échéant, le délégué à la protection des données peut-il gérer ce budget de manière indépendante ?* ».

Regrettons également que les délégués à la protection des données ne fassent pas plus d'efforts au sein de leur organisme pour mieux faire connaître leurs apports et la plus-value de leurs actions. Il faut constater que, comme maints RSSI, les DPO sont trop timides et ne savent pas se « vendre ». Aussi n'est-il pas surprenant qu'ils soient trop souvent perçus uniquement comme des freins et des contraintes.

Poursuivons avec la nécessité pour les DPO de maintenir eux-mêmes leur motivation, de « s'auto-encourager », puisque personne ne le fait pour eux. Il arrive que, découvrant le peu d'écho de ses efforts, le délégué sente son moral flancher. Dans ces situations, il faut prendre du champ et ne pas se focaliser sur le

---

[106] Comme l'indique le document *CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations* publié le 30 mai 2016, « *Être DPO nécessite une certaine forme de "gravité" et du leadership* ». https://cedpo.eu/wp-content/uploads/CEDPO-Minimum_Qualifications_DPO_20160530.pdf

[107] Voir la question écrite n° 20626 de M. Bernard Fournier (Loire - Les Républicains) publiée dans le JO Sénat du 11/02/2021 - https://www.senat.fr/questions/base/2021/qSEQ210220626.html

[108] *Évolution de la fonction de Délégué à la Protection des Données - Etude 2022*, réalisée par l'Afpa avec l'aide de la CNIL, de l'AFCDP et de l'ISEP, commanditée par le Ministère du Travail

[109] Parmi les bonnes pratiques pouvant assurer l'indépendance du délégué citées dans *The DPO Handbook* (Op. cit.), on relève « *Le DPO devrait disposer de son propre budget* ».

recul ponctuel mais constater les progrès accomplis sur une échelle de temps plus longue[110]. La persévérance est sans conteste l'une des qualités requises pour être délégué à la protection des données : « *Ténacité est le maître mot ! Combien de fois ai-je dû encaisser des rebuffades ou voir mes analyses et conseils balayés d'un revers de la main… Mais, au final et avec un peu de recul, notre entreprise est sur le bon chemin. Les réflexes commencent à s'implanter et les zones de résistance ont tendance à se réduire. Ne rien lâcher et garder le cap. C'est dans la durée que l'on pourra juger de l'efficacité de mes actions en tant que DPO* », « *Faire preuve de patience et de diplomatie… mais en prenant soin de bien marquer la ligne jaune à ne pas franchir. Une main de fer dans un gant de velours, et toujours avec sourire et conviction* », « *Avancer progressivement et sans craindre les compromis qui nous mettent parfois en marge d'une conformité idéale* » sont quelques-uns des *verbatim* recueillis auprès de membres de l'AFCDP.

Nous avons vu que plusieurs des témoins se sont retrouvés en situation de *burnout*. C'est malheureusement un état dont ne sont pas toujours conscients ceux qui en souffrent. Ils vont s'impliquer dans leur fonction jusqu'au point de non-retour. Il est donc important de faire attention aux signes annonciateurs, car s'il est pris à temps, le *burnout* peut être contré. En revanche, le temps de récupération d'un épuisement professionnel avéré peut être long. Constatant que la plupart des témoins n'ont pas perçu suffisamment rapidement l'état de stress dans lequel ils se trouvaient, il est suggéré aux DPO de l'évaluer. En annexe 1, et sur la base de l'étude réalisée par le CESIN et la société Advens, l'auteur propose une méthode pour ce faire[111].

Plusieurs DPO en grande souffrance qui ont été interviewés ont reconnu s'être isolés : ils n'ont pas cherché à consulter leur médecin, à consulter un avocat ou l'inspecteur du travail, à en parler avec leur entourage ou à un confrère, à contacter la CNIL. Tous ont reconnu que c'était là une erreur et les conseils qu'ils prodiguent désormais vont tous dans ce sens : « *Même quand tout va bien, je garde désormais toujours un œil à la fenêtre* », « *Si jamais cela se reproduisait, je n'hésiterai pas une seconde à en parler autour de moi* », « *J'ai mal placé ma fierté. Aller voir son médecin pour parler de son mal être dans son travail n'a rien d'honteux* ». Un membre AFCDP avait témoigné sur ce même sujet : « *Ne surtout pas rester seul et rejoindre au plus tôt une association. Non seulement on gagne du temps mais on y trouve du réconfort moral aux moments les plus durs* ». Depuis plusieurs mois, sur une proposition de son Secrétaire général Philippe Salaün (par ailleurs DPO de CNP Assurances), l'AFCDP travaille sur une initiative visant à mettre à disposition des délégués à la protection des données un service d'écoute faisant intervenir des psychologues du travail.

On ne rappellera jamais assez le conseil donné aux DPO de tout consigner par écrit. Même si l'autre partie (responsable de traitement, superviseur, directeur de service, etc.) refuse de laisser une trace de ses dires, tout délégué devrait prendre l'initiative de lui adresser un simple message dans lequel est synthétisée la position exprimée (refus d'entendre ou de suivre la recommandation du DPO, tentative d'atteinte à l'indépendance du DPO voire menace voilée), avec une formulation qui peut être « *Je me permets de transcrire les propos que vous avez tenus lors de notre échange du [date]. Merci de me signaler toute incompréhension de ma part* ». Notons que les lignes directrices du CEPD sur le calcul des sanctions administratives (adoptées le 12 mai 2022) indiquent que la gravité de la non-conformité serait augmentée si l'infraction a été sciemment été commise par la grande direction en dépit des conseils formulés par le délégué à la protection des données. La violation du RGPD est alors considérée comme intentionnelle[112]. Constatant que plusieurs des DPO qui ont été licenciés et qui n'ont pas osé porter l'affaire devant les Prud'hommes, on soulignera que ce n'est que

[110] Voici une astuce pour penser « temps long » : imaginez le discours qui serait prononcé lors de votre pot de départ et dressant le constat du chemin que vous aurez fait parcourir à votre organisme... Les petites contrariétés n'y seront pas évoquées et n'apparaitront que les grandes avancées que vous aurez obtenues.

[111] L'auteur a relevé sur Internet plusieurs listes de métiers présentés comme faiblement stressants. De façon surprenante, on y trouve la fonction de « Chargé de conformité – déontologue » !

[112] « *The seriousness of the infringement was increased, however, by the fact that the infringement was committed in contrary to an advice from the data protection officer and, thus, considered intentional* » https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf

lorsqu'ils sont strictement nécessaires à l'exercice de ses droits de la défense dans le litige l'opposant à son employeur qu'un salarié peut en conserver une copie[113] (et c'est au salarié d'établir que cette copie était strictement nécessaire à l'exercice des droits de sa défense). Si les relations entre la direction et le DPO empirent au point que ce dernier soit convoqué pour un entretien préalable à un éventuel licenciement, l'auteur recommande l'écoute de l'enregistrement de « *Didier Bille, le sniper des RH* », diffusée pour la première fois le 11 avril 2018 sur France Culture[114]. Dans cette interview, un ancien DRH qui a licencié plus de mille salariés au sein de grandes entreprises raconte tout ce qu'il a fait par le menu. Un récit sans honte ni tabou dans lequel Didier Bille indique comment il utilisait à son profit le fait que rares sont les salariés qui prennent soin de conserver une copie privée de documents qui pourraient lui être utiles par la suite en cas de contentieux : « *Si tu choisis la voie conflictuelle, tu seras de toute façon licencié... et comme tu pars dans 5 minutes... en effet, à la fin de cet entretien tu sors de mon bureau et tu es dehors dans 5 minutes, tu n'auras aucun élément pour prouver ce qui a été dit ou pour te défendre, alors que nous, on pourra choisir tranquillement tous les éléments en notre faveur...* ». L'ancien DRH indiquait également pourquoi les personnes mises en cause n'ont pas toujours intérêt à essayer de se défendre pendant l'échange : « *Durant l'entretien préalable, Je vais devoir lui reprocher quelque chose. La plupart du temps, le dossier est très (très) maigre. Le salarié ne se retrouve pas en face de moi car on lui reproche quelque chose, il a juste le malheur de figurer dans une liste de personnes qu'on nous demande d'éjecter. Quand la personne choisissait la voie conflictuelle, nous cherchions, avec son manager, une broutille, que j'allais ensuite pouvoir monter en épingle. Et, lors de l'entretien préalable, je vais lui exposer cette broutille. On a la victime devant nous. Cette personne va tenter de se défendre. Elle est en train de nous fournir les arguments qu'éventuellement son avocat utilisera plus tard. Ça va nous aider à bâtir sa lettre de licenciement, en répondant déjà à des contre-arguments de son avocat et en évitant d'écrire certaines choses qui iraient nourrir son système de défense. Il nous aide en fait à torpiller par avance sa défense.* ».

Il serait aussi utile de mieux faire connaître aux DPO la possibilité nouvelle qu'ils ont de lancer une alerte auprès de la CNIL[115]. L'article 22.III de la loi Informatique et Libertés dans sa version de 2004 le prévoyait expressément[116] : « *Il [le Correspondant Informatique et Libertés] peut saisir la Commission nationale de l'informatique et des libertés des difficultés qu'il rencontre dans l'exercice de ses missions* ». Cette disposition ne figurait plus dans le RGPD. Mais grâce au député Sylvain Waserman, le statut protecteur de lanceur d'alerte instauré par la loi dite « Sapin 2 » du 9 décembre 2016 a récemment été amélioré par la loi du 21 mars 2022 (Loi 2022-401 du 21-3-2022). Le texte renforce la protection des personnes qui signalent des violations du droit de l'Union – dont le RGPD. La CNIL figure dans le Décret n° 2022-1284 du 3 octobre 2022[117] parmi les « autorités externes » devant se saisir et traiter les alertes dans leur champ de compétences (c'est-à-dire celui de la « Protection de la vie privée et des données personnelles »). Ce canal pourrait donc éventuellement être envisagé pour protéger le délégué à la protection des données[118] après avoir épuisé toutes les voies d'ordre

---

[113] Cf. Cour de cassation Chambre sociale 31 mars 2015, pourvoi n° 13-24.410, Bull. 2015, V, n° 68 https://www.legifrance.gouv.fr/juri/id/JURITEXT000030446037/

[114] Reportage de Leila Djitli, Podcast : www.radiofrance.fr/franceculture/podcasts/les-pieds-sur-terre/didier-bille-le-sniper-des-rh-2918023

[115] Emmanuel Cauvin (ancien Group DPO d'Arcelor Mital puis d'Orpea), dans son article *Premier bilan du RGPD : pauvre DPO...* publié fin 2018 dans MagSecurs n°59, s'exprimait à ce propos : « *Pour faire bonne mesure, le RGPD prévoit que le DPO ne reçoit aucune instruction, ne peut être relevé de ses fonctions ou pénalisé, et fait directement rapport au niveau le plus élevé de la direction. Ces dispositions protectrices et valorisantes sont d'un maigre secours face à la réalité quotidienne du DPO.../... Dénoncer tel ou tel service auprès de la CNIL ? Les volontaires pour le suicide professionnel risquent de ne pas se bousculer au portillon* ».

[116] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000441676

[117] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046357368

[118] La loi n° 2022-401 du 21 mars 2022 dispose que « *Les [lanceurs d'alerte] .../... pour avoir signalé ou divulgué des informations dans les conditions prévues aux articles 6 et 8 de la présente loi.../...ne peuvent faire l'objet de mesures de représailles, ni de menaces ou de tentatives de recourir à ces mesures, notamment sous les formes suivantes : Suspension, mise à pied, licenciement ou mesures équivalentes ; Rétrogradation ou refus de promotion ; Transfert de fonctions, changement de lieu de travail, réduction de salaire, modification des horaires de travail ; Suspension de la formation ; Evaluation de performance ou attestation de travail négative ; Mesures disciplinaires imposées ou administrées, réprimande ou autre sanction, y compris une sanction financière ; Coercition, intimidation, harcèlement ou ostracisme ; Discrimination, traitement désavantageux ou injuste, etc.* ». Peut-on imaginer qu'un DPO se place volontairement sous cette forme de protection s'il s'attend à faire l'objet très prochainement d'un licenciement ?

inférieur (discussions avec le superviseur et le responsable de traitement). Sur une page spécifique de son site Web (« *Lanceurs d'alerte : adresser une alerte à la CNIL*[119] »), la Commission décrit qui est concerné et comment s'y prendre. Elle précise que « *Les signalements des lanceurs d'alerte doivent concerner un manquement relevant de la règlementation en matière de protection des données personnelles (RGPD, loi Informatique et Libertés, etc.), y compris en matière de cybersécurité. L'alerte doit porter sur des faits qui se sont produits ou pour lesquels il existe une forte probabilité qu'ils se produisent* ». Naturellement, la CNIL peut effectuer des contrôles, voire prononcer des sanctions, si elle considère que ce qui lui a été signalé le justifie. Certes, elle s'engage à protéger l'identité de l'auteur du signalement, mais un responsable de traitement contrôlé pour savoir s'il a doté son DPO des conditions d'exercice exigées par le RGPD ne devrait pas avoir beaucoup de difficulté à imaginer d'où cela provient…

L'auteur s'est entretenu avec une représentante de la MLA (Maison des Lanceurs d'Alerte[120]), association loi 1901 créée en 2018 afin d'accompagner les lanceurs d'alerte et d'améliorer leur protection. À tout moment, les personnes qui contactent la Maison des Lanceurs d'Alerte, que ce soit avant ou après avoir lancé l'alerte, peuvent bénéficier d'un accompagnement juridique, technique, psychologique, médiatique, financier et social, notamment lorsqu'ils font l'objet de représailles. C'est elle qui a soutenu le lanceur d'alerte qui a révélé en 2020 des failles de sécurité dans des logiciels vendus aux laboratoires d'analyse et autres établissements de santé par l'entreprise Dedalus France. Le lanceur d'alerte avait été licencié à la suite de ses signalements. Le 15 avril 2022, la formation restreinte a sanctionné le responsable de traitement d'une amende de 1,5 million d'euros, notamment pour des défauts de sécurité ayant conduit à la fuite de données médicales de près de 500.000 personnes[121].

C'est encore la MLA qui a saisi la CNIL en février 2021[122]. Une *data scientist* employée auprès d'un Groupement d'Intérêt Public en charge de la collecte et du traitement des données de santé des établissements médicaux et sociaux de la région Provence-Alpes-Côtes d'Azur avait en effet constaté des faits susceptibles de porter atteinte au droit à la protection des données à caractère personnel protégé par le RGPD[123]. Sollicitée pour constituer un dossier d'autorisation CNIL pour organiser la sous-traitance des données recueillies par la société Mondobrain, une société de droit américain, cette lanceuse d'alerte a signalé ces faits à ses supérieurs à partir d'août 2019. Quelques mois plus tard, cette lanceuse d'alerte a saisi la CNIL. Licenciée, elle a bénéficié de l'aide de la Maison des Lanceurs d'Alerte.

Enfin, c'est aussi cette association qui est venue en aide au lanceur d'alerte qui avait révélé un programme d'écoute et de transcription d'enregistrements à leur insu des utilisateurs de Siri, l'assistant vocal « intelligent » d'Apple[124]. On apprenait alors que Siri collectait bien plus que les simples requêtes qui lui étaient formulées, mais aussi disputes, bruits de fond et autres conversations, notamment au sujet de maladies, de religion, de sexualité ou encore de politique[125].

---

119 https://www.cnil.fr/fr/lanceurs-dalerte-adresser-une-alerte-la-cnil

120 https://mlalerte.org/

121 Délibération SAN-2022-009 du 15 avril 2022

122 https://mlalerte.org/traitement-des-donnees-de-sante-en-region-paca-la-maison-des-lanceurs-dalerte-saisit-la-cnil/

123 Voir *ARS Paca : alerte aux fuites de données*, par Sébastien Boistel, le Ravi, juin 2021 - https://www.leravi.org/medias/lanceurs-dalerte/alerte-sur-un-risque-de-fuite-de-donnees-a-lars-paca-via-mondobrain-une-start-up-americaine/

124 https://mlalerte.org/le-lanceur-dalerte-sur-les-ecoutes-dapple-adresse-une-lettre-ouverte-aux-autorites-europeennes/

125 L'article « *Exercer son droit d'accès : un parcours semé d'embûches* » (B. Rasle, 18 janvier 2023) relate un constat identique relevé par un étudiant du *Mastère Spécialisé Management et Protection des Données Personnelles* de l'ISEP : « *Lors de l'exercice 2021, un GAFA qui propose un assistant domestique avait renvoyé à un étudiant plusieurs centaines de fichiers audio, correspondant chacun à un enregistrement vocal. Problème : plusieurs d'entre eux ne correspondaient pas à un ordre destiné à l'assistant, mais à des échanges privés, dont certains d'ordre intime.* ». https://www.anaxia-conseil.fr/la-securite-des-donnees-personnelles-enfin-prise-au-serieux.html

Serait-il souhaitable que le DPO devienne un salarié protégé[126] ? Compte tenu donc de la spécificité des fonctions de délégué à la protection des données, de l'indépendance qu'elles supposent vis-à-vis de la direction de l'entreprise, il aurait été légitime de se demander si, à l'instar des représentants du personnel, des membres du comité d'entreprise ou des délégués syndicaux, le DPO interne n'aurait pas dû devenir un salarié protégé dont la résiliation du contrat de travail (à l'amiable ou non) devrait être soumise à autorisation de la CNIL. La lecture du compte rendu des discussions de l'Assemblée autour de la loi Informatique et Libertés de 2004[127] montre que cette approche a été écartée dès l'origine en ce qui concerne le Correspondant Informatique et Libertés. En voici quelques extraits choisis :

- M. Christophe Caresche (Député de Paris, parti socialiste) : « *Le sous-amendement n° 54 vise, en accroissant leur protection [celle des CIL], à garantir plus encore les correspondants des pressions qui ne manqueront pas de s'exercer sur eux. M. le ministre dit qu'ils diffuseront la culture de la CNIL. Fort bien... Mais ils pourraient aussi diffuser la culture de l'entreprise, s'ils ont des tentations, voire subissent des pressions les incitant à constituer des fichiers ayant des caractéristiques contraires à la déontologie. Il faut donc protéger et mettre à l'abri ces salariés. Nous pensons comme M. Dutoit que la qualité de salarié protégé, telle que prévue par le code du travail, serait une garantie d'indépendance. Pourquoi ne pas la leur appliquer ?* ».
- M. Frédéric Dutoit (Député des Bouches-du-Rhône, parti communiste) : « *Un autre point nous inquiète : le statut de ce correspondant. Nous souhaiterions qu'il bénéficie d'un statut de salarié protégé et, surtout, que ce soit inscrit dans la loi. Nous vous demandons, monsieur le rapporteur, de réfléchir à cette proposition afin de modifier votre amendement et d'offrir au système des correspondants le minimum de garanties nécessaires à la protection des données à caractère personnel* ».
- M. Dominique Perben (garde des Sceaux, ministre de la justice) : « *Quant au sous-amendement n° 54, le dispositif protecteur déjà prévu apporte les garanties indispensables. Je ne pense pas qu'il soit nécessaire d'aller plus loin* ».
- M. Francis Delattre (Rapporteur du projet de loi, député du Val-d'Oise, UMP) : « *Il est vrai que la commission et le Gouvernement n'ont pas été jusqu'à faire du correspondant un salarié protégé, mais la CNIL lui garantit indépendance et capacité d'action. [c'est le travail de la CNIL] de se rendre sur place pour vérifier s'ils [les correspondants] travaillent en toute indépendance et assurent leur mission à la fois dans l'intérêt de la CNIL et de l'entreprise. De toute façon, il faut expérimenter. Ça ne sert à rien de placer dès le départ les personnes concernées dans un dispositif statufié, sans changement possible. Ce sera une expérimentation utile. On verra bien par la suite si l'octroi de garanties supplémentaires se justifie* ».
- M. Frédéric Dutoit : « *Monsieur le ministre, mais plus encore monsieur le rapporteur, je tiens à vous dire à quel point je regrette que votre angélisme nous empêche de garantir aux correspondants le statut de salarié protégé. C'est mal connaître les entreprises et la pression que peuvent exercer des patrons - j'ose dire le mot - que de créer un contexte qui leur permettra de soumettre les correspondants à une pression si forte qu'ils ne pourront rester réellement indépendants* ».

Plus récemment, c'est un sénateur, M. Claude Raynal (représentant de la Haute-Garonne), qui a en 2018 attiré l'attention de la ministre du travail sur le statut en droit français des délégués à la protection des données lors d'une question écrite[128]. Remarquant que « *la protection de l'indépendance et de la fonction de ces salariés face aux possibles pressions de leurs employeurs, qu'ils soient publics ou privés, étaient des conditions nécessaires à l'effectivité de leurs missions* », il souhaitait « *connaître les dispositifs mis en place afin de protéger au mieux ces salariés et de permettre à la France de respecter ses engagements européens* ». Dans sa réponse, la ministre s'était bornée à rappeler le paragraphe 3 de l'article 38 du RGPD et les lignes directrices adoptées par le G29 concernant le DPO, en précisant que « *Si le législateur n'a pas entendu conférer au délégué à la protection des données, le statut de salarié protégé au*

[126] Cf. Article L2411-1 du Code du travail
[127] http://www.assemblee-nationale.fr/12/cri/2003-2004/20040205.asp#P158_8086
[128] Question écrite n° 02896 de M. Claude Raynal (Haute-Garonne - SOCR) publiée dans le JO Sénat du 25/01/2018 - page 285 - https://www.senat.fr/questions/base/2018/qSEQ180102896.html

sens du droit du travail, il bénéficie néanmoins d'une large protection dans l'exercice de ses missions depuis le 25 mai 2018, date d'entrée en vigueur du RGPD ».

Sans aller jusqu'au statut de salarié protégé[129], ne serait-il pas possible de s'inspirer de l'Allemagne en ménageant pour le DPO une protection supérieure à ce que le RGPD prévoit ? L'article 6 du *Bundesdatenschutzgesetz* (loi fédérale sur la protection des données) du 20 décembre 1990 (dans sa version en application du 25 novembre 2019), dispose à son article 4 que « *Là où le DPD ne peut être relevé de ses fonctions que dans le cadre d'une application par analogie de l'article 626 du Bûrgerliches Gesetzbuch [Code civil], dans sa version publiée le 2 janvier 2002. Le licenciement d'une DPD est illégal, à moins que les faits n'autorisent l'organisme public à procéder à son licenciement pour motif grave sans respecter le délai de préavis* ».

La Cour de justice de l'Union Européenne a d'ailleurs récemment rappelé qu'il est possible aux États membres de prévoir une protection plus importante en faveur des DPO, en limitant par exemple les possibilités de licenciement d'un délégué à la protection des données salarié à la commission d'une faute grave. Cela constitue un encouragement qui sera peut-être entendu par le législateur afin de renforcer le statut du DPO interne dans notre législation nationale[130]. Malheureusement, ce sujet n'a pas été abordé lors de la première revue du RGPD, courant 2020[131].

Ainsi on peut regretter l'abrogation des dispositions que contenait le décret d'application n°2005-1309 du 20 octobre 2005[132] relatives à la fin de mission du Correspondant Informatique et Libertés :

- Article 53 : *Lorsqu'il envisage de mettre fin aux fonctions du correspondant pour un motif tenant à un manquement aux devoirs de sa mission, le responsable des traitements saisit la Commission nationale de l'informatique et des libertés pour avis par lettre remise contre signature, comportant toutes précisions relatives aux faits dont il est fait grief. Le responsable des traitements notifie cette saisine au correspondant dans les mêmes formes en l'informant qu'il peut adresser ses observations à la Commission nationale de l'informatique et des libertés. La Commission nationale de l'informatique et des libertés fait connaître son avis au responsable des traitements dans un délai d'un mois à compter de la réception de sa saisine. Ce délai peut être renouvelé une fois sur décision motivée de son président. Aucune décision mettant fin aux fonctions du correspondant ne peut intervenir avant l'expiration du délai prévu à l'alinéa précédent.*
- Article 54 : *Lorsque le correspondant est démissionnaire ou déchargé de ses fonctions, le responsable des traitements en informe la Commission nationale de l'informatique et des libertés. La notification de cette décision mentionne en*

[129] Le cas néerlandais est très intéressant et mériterait d'être étudié. Avant l'entrée en application du RGPD, le *Functionaris voor de gegevensbescherming* (délégué à la protection des données) avait le statut de salarié protégé. Ce statut est défini aux articles 670 et suivants du livre 7 du code civil (https://wetten.overheid.nl/BWBR0005290/2023-02-18/0#Boek7_Titeldeel10_Afdeling9_Artikel670). L'article 670a.d disposait que le DPO ne pouvait être licencié qu'avec l'autorisation préalable du « tribunal d'instance ». Cette disposition a été abrogée en 2015 et le DPO n'est plus listé dans les catégories de salariés protégés. La plupart des dispositions relatives au DPO et présentes dans la loi sur la protection des données (*Wet bescherming persoonsgegevens*) avant l'entrée en vigueur du RGPD ont également été abrogées.

[130] Voir *Les spécificités du DPO salarié*, par Marion Narran-Finkelstein, avocate, 22 septembre 2022, Village de la Justice, https://www.village-justice.com/articles/plateforme-protection-dpo-salarie,43255.html

[131] Le 24 juin 2020, un peu plus de deux ans depuis le début de la mise en œuvre du RGPD, la Commission européenne a publié un rapport d'examen et d'évaluation des résultats de son application. (Cf. *Deux ans de RGPD : Questions et réponses* https://ec.europa.eu/commission/presscorner/detail/fr/qanda_20_1166). L'AFCDP avait réagi à cette publication : « ... *l'AFCDP remarque avec étonnement que le bilan établi par la Commission ne fait à aucun moment mention du délégué à la protection des données, dont la création et les missions sont pourtant parmi les points les plus notables du RGPD* ». Le RGPD prévoit l'élaboration du premier rapport deux ans après le début de son application et ensuite, tous les quatre ans : la Commission européenne mettra-t-elle à profit l'évaluation de 2024 pour s'intéresser à la cheville ouvrière du règlement ?

[132] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000241445

outre le motif de la démission ou de la décharge. Il y est annexé, en lieu et place de l'accord prévu au huitième alinéa de l'article 43, le justificatif de la notification de la décision au correspondant.

Ces dispositions protectrices pour le DPO ne pourraient-ils pas être réintroduites à l'occasion d'une prochaine modification de la loi Informatique et Libertés[133] ?

Une ode aux DPO

Comme son prédécesseur le Correspondant Informatique et Libertés, le délégué à la protection des données est le levier le plus efficace pour que les règles soient respectées. Comme l'a rappelé Mathias Moulin, Secrétaire général adjoint de la CNIL, lors de son allocution prononcée le 9 février 2023 à la 17ème Université AFCDP des DPO, « *la fonction de DPO est essentielle* ». Il a ajouté « *Les responsables qui ne reconnaissent pas à sa juste valeur son apport manquent de vision ou jouent à la roulette russe* ». Souhaitons que chacun y mette du sien pour que cet élément d'autorégulation bénéficie d'un environnement qui lui permette de remplir ses missions pleinement et sereinement : les responsables de traitements en lui assurant support, écoute et ressources, les autorités de contrôle, en faisant utilement faire passer quelques messages par quelques décisions de sanctions proportionnées et les délégués à la protection des données eux-mêmes, en poursuivant leur professionnalisation, notamment en préparant mieux leur prise de poste. Tous ensemble, sauvons le soldat DPO !

Remerciements

À nouveau, l'auteur tient à remercier chaleureusement les consœurs et confrères qui ont accepté de témoigner. Merci également à Patrick Blum, ancien CIL puis délégué à la protection des données de l'Essec, délégué général de l'AFCDP, avec qui chaque échange est un bonheur. Les discussions avec Jean-François Louapre, du CESIN, et Benjamin Leroux, de la société Advens, ont été d'une grande aide au sujet de l'étude très intéressante qu'ils ont pilotée sur le stress des RSSI. Le présent travail a également bénéficié de l'écoute de la CNIL. Un grand merci à Albine Vincent, Cheffe du service des DPO, et à son adjointe, Marjorie Menapace, pour les fructueux échanges qui ont nourri la réflexion. Il faut saluer les actions qu'a menées, et que continue de mener, la Commission pour accompagner les CIL puis les DPO depuis bientôt vingt ans. Merci également à Maison des Lanceurs d'Alerte, qui va sans doute voir son activité fortement augmenter (pour faire un don : https://soutenir.mlalerte.org/). Je salue le dessinateur de talent Luc Tesson[134], qui a déjà réalisé plusieurs dessins humoristiques pour illustrer quelques moments clés de la vie du DPO et qui s'est à nouveau prêté au jeu pour égayer le présent texte. Bravo Luc pour tes dessins qui font toujours mouche ! Yann-Hervé Beulze, ancien RCCI, Correspondant risques et DPO d'un acteur du secteur financier, nous a fait vivre la fonction Responsable de la Conformité et du Contrôle Interne. Merci à Régis Brun, équipier du DPO de Groupama, d'avoir signalé à mon attention le statut de juriste d'entreprise tel que considéré chez nos voisins allemands. Enfin l'auteur tient à remercier les membres de l'AFCDP qui l'ont encouragé dans sa démarche. Un salut particulier à tous ceux qui ont répondu au très long questionnaire qui leur était proposé sur le sujet crucial de l'indépendance du DPO !

[133] En 2018, l'AFCDP avait formulé des suggestions dans le cadre de la rédaction du décret d'application de la loi Informatique et Libertés modifiée pour tenir compte du RGPD. Dans l'exposé des positions, on trouvait « *Conserver l'information des instances représentatives du personnel de la nomination d'un délégué à la protection des données* », « *Avis de la CNIL pour les cas où le responsable de traitement souhaiterait mettre fin aux fonctions du délégué à la protection des données* », « *Obligation pour le responsable de traitement de documenter les raisons de son éventuel refus de suivre les conseils de son délégué à la protection des données* ». Aucune de ces propositions n'a malheureusement été retenue par le législateur.

[134] www.dessinateurdepresse.com

L'auteur

Bruno Rasle se définit comme un « monomaniaque » de la conformité au RGPD et pratique cet art martial sous trois formes : à titre professionnel, il a été délégué à la protection des données mutualisé pour l'une des branches de la Sécurité sociale ; à titre bénévole, il est l'un des tous premiers membres de l'AFCDP et a été son délégué général pendant une douzaine d'années ; en tant qu'enseignant enfin, en tant que chargé de cours au sein de la formation la plus ancienne et du niveau le plus élevé en Europe (il forme les professionnels de la *Privacy* depuis 2007). Il a également pris une part active dans la création du métier de Correspondant Informatique et Libertés (puis de délégué à la protection des données). Il est coauteur des ouvrages suivants : *Halte au Spam* (Eyrolles, 2003) ; *Correspondant Informatique et Libertés : bien plus qu'un* métier (AFCDP, 2015) ; *Droit à l'oubli* (Larcier, 2015) ; *Se préparer au RGPD* (Éditions législatives, 2017). Il a créé l'Université AFCDP des DPO (et a été son organisateur jusqu'en 2020), l'Index AFCDP du droit d'accès et le *Job board* des DPO (AFCDP). Bruno Rasle est le co-auteur du code de déontologie du DPO et de la version annotée, commentée et indexée du RGPD mise à disposition par l'association. Il a participé à la création de CEDPO (Confédération européenne des associations de professionnels de la protection de la vie privée) dont il a été *Board Member*.

Ses publications sont nombreuses (« *La purge des données – Un effort qui en vaut la peine* », « *Pour une désignation idéale du DPO* », « *Courteline rend le sourire aux DPO* », « *Collègues DPO : le bilan annuel est un outil précieux ; faisons-en une bonne pratique* », « *PSSI : contrainte ou opportunité ?* »), de même que ses interventions en conférence (« *Cookie et Widget : peut-on vraiment surfer tranquille ?* », Université AFCDP 2011, « *Synergie entre RSSI et CIL* » , Cesin 2012 ; « *Mise en conformité des Zones de Libre Commentaire* », Université AFCDP 2013 ; « *Privacy by Design : le rôle clé des développeurs* », AtoutFox 2013 ; « *CPO & CSO : Bridging the gap* », IAPP Bruxelles 2013 ; « *Les méthodes agiles sont-elles Privacy-compatibles ?* », Cloud Week Paris 2015 « *La Blockchain est-elle soluble dans le RGPD ?* », AG AFCDP 2017 ; « *Le RGPD, évolution ou révolution ?* », Journées JCAS 2017 ; « *Que sommes-nous ? Responsable de traitement ? Responsable conjoint ? Sous-traitant ?* », AG AFCDP 2019 ; « *Comment auditer sa gestion des droits d'accès ?* », Université AFCDP 2021 ; « *Créer et animer un réseau de RIL* », Université AFCDP 2022).

Outre son enseignement au sein du Mastère Spécialisé « *Management et Protection des Données Personnelles* » de l'ISEP, il propose des formations courtes pour le compte d'Anaxia Conseil[135] (« *L'informatique appliquée au RGPD* », « *Réaliser une Analyse d'Impact – De la théorie à la pratique* », « *Violations de données : pour ne pas subir* », « *Contrôle de la CNIL – S'y préparer, le gérer, y survivre* », « *Être un DPO efficace dès les premiers jours* »).

Commons

[135] www.anaxia-conseil.fr

Annexes

Annexe n°1 – Méthode permettant à un DPO d'évaluer son niveau de stress et d'identifier ses causes

Constatant que la plupart des témoins n'ont pas perçu suffisamment rapidement l'état de stress dans lequel ils se trouvaient, il est suggéré aux DPO de l'évaluer. La présente proposition de méthode est basée sur celle utilisée dans l'étude réalisée par le CESIN et la société Advens sur le stress des RSSI. L'auteur s'est contenté d'adapter au métier de DPO certaines questions de la partie consacrée aux causes du stress.

L'enquête du CESIN et la société Advens est librement accessible sur la page https://www.advens.fr/wp-content/uploads/2022/06/advenscesin-etudecyberstress-septembre2021-0-comprime-4.pdf

Le questionnaire comporte deux parties. La première (dix questions) vise à évaluer le niveau de stress, la seconde tente d'identifier les facteurs propres aux métiers de DPO et susceptibles de contribuer au stress.

L'auteur suggère de reprendre sans aucune modification le premier questionnaire (notamment pour permettre des comparaisons entre le niveau de stress des délégués à la protection des données et celui des RSSI).

L'évaluation du niveau de stress se base sur un modèle reconnu (la PSS, *Perceived Stress Scale*), dont l'objet est la détermination du niveau de stress ressenti. Voici les dix questions destinées à évaluer le niveau de stress. À chaque question, il peut être répondu *Jamais*, *Presque Jamais*, *Parfois*, *Assez Souvent* et *Souvent* :

1. Au cours du dernier mois vous êtes-vous senti contrarié ou énervé par des événements non prévus ?
2. Au cours du dernier mois vous êtes-vous senti incapable de contrôler les « fondamentaux » de votre métier/fonction/rôle ?
3. Au cours du dernier mois vous êtes-vous senti(e) nerveux(se) ou stressé(e) ?
4. Au cours du dernier mois vous êtes-vous senti(e) pleinement capable de gérer vos problèmes professionnels ?
5. Au cours du dernier mois avez-vous senti que les choses allaient comme vous le vouliez ?
6. Au cours du dernier mois avez-vous pensé que vous ne pouviez pas assumer toutes les choses que vous deviez faire ?
7. Au cours du dernier mois avez-vous été capable de maîtriser (intérieurement et extérieurement) votre agacement ?
8. Au cours du dernier mois avez-vous senti que vous « maîtrisiez la situation » ?
9. Au cours du dernier mois vous êtes-vous senti(e) irrité(e) parce que les événements échappaient à vôtre contrôle ?
10. Au cours du dernier mois avez-vous trouvé que les difficultés s'accumulaient à tel point que vous ne pouviez plus les contrôler ?

Afin de calculer le score, il faut utiliser deux notations différentes. La première concerne les question 1, 2, 3, 6, 9 et 10 : *Jamais* = 0 ; *Presque Jamais* = 1 ; *Parfois* = 2 ; *Assez Souvent* = 3 et *Souvent* = 4. La seconde concerne donc les questions restantes 4, 5, 7 et 8 : *Jamais* = 4 ; *Presque Jamais* = 3 ; *Parfois* = 2 ; *Assez Souvent* = 1 et *Souvent* = 0. Avec l'échelle PSS utilisée, donnant une évaluation allant de 0 à 40, le stress est jugé positif ou stimulant si le niveau est inférieur à 16. Si le score obtenu se situe entre 16 et 24, il existe des sentiments d'impuissance occasionnels et des perturbations émotionnelles. Au-delà de 22, l'individu se situe en « zone rouge », accompagnée de risques accrus pour la santé physique et mentale, et un sentiment de menace et d'impuissance.

En revanche, l'auteur propose de ne pas reprendre les questions qui ont été proposées aux RSSI afin d'identifier et de classer par ordre d'importance les causes du stress (à titre d'exemples, les deux questions

suivantes sont adaptées au métier de RSSI mais aucunement à celui de DPO : *Trouvez-vous votre métier singulier, dans la mesure où il fait face à des adversaires, souvent « invisibles » et malveillants, ce qui est peu usuel, car peu de professions connaissent ce contexte d'adversité ?*). Il en propose quelques-unes ci-dessous comme base de réflexion au sein de l'AFCDP (les réponses peuvent être *Jamais ou presque jamais*, *Parfois* ou *Assez souvent ou souvent*) :

1. Souffrez-vous de l'image et des *a priori* parfois négatifs autour de votre fonction de DPO ?
2. Est-ce que la gestion de la conformité au RGPD vous parait un exercice intellectuellement difficile ?
3. Estimez-vous difficile de devoir adapter en permanence vos analyses devant un contexte complexe et évolutif, de devoir apprendre et vous réinventer sans cesse ?
4. Appréciez-vous les imprévus et les aléas, nombreux dans le métier ?
5. Ressentez-vous un manque d'expertise, de connaissances, de savoir-faire, de vécu ?
6. Etes-vous à l'aise avec l'étendue que doit couvrir le métier de DPO (juridique, technique, procédures, sociétal, humain) ?
7. Redoutez-vous les situations où votre métier de DPO vous place dans des contextes humainement délicats (confrontations avec la direction, par exemple) ?
8. Avez-vous une difficulté à exprimer une analyse de conformité dont vous savez qu'elle risque d'être mal reçue ?
9. Avez-vous le sentiment d'être incompris ou d'être jugé « excessif » lorsque vous faites des recommandations ?
10. Vous sentez-vous a minima soutenu par la direction ?
11. Avez-vous le sentiment d'être isolé par les autres, voire de ne pas vraiment faire partie de l'entreprise ?
12. Avez-vous le sentiment de dépasser une partie de votre énergie à vous « battre » contre des adversités internes ?
13. Comment ressentez-vous l'exercice de la communication ? Arrivez-vous à convaincre vos interlocuteurs ?
14. Avez-vous le sentiment de devoir vous justifier auprès des autres, voire auprès de vous-même, de l'utilité de vos actions ?
15. Au cours du dernier mois, avez-vous trouvé que votre charge de travail atteignait un niveau qui vous perturbe ?
16. Considérez-vous que votre situation professionnelle est incertaine, et qu'une crise majeure pourrait vous coûter votre poste ?
17. Considérez-vous que vous bénéficiez d'un encadrement aidant (qui vous place dans de bonnes dispositions pour réaliser vos missions) ?

Ces questions pourraient être regroupées en familles de critères : l'image qu'ont les autres du DPO (Les DPO sont, à tort, perçu par leur entourage professionnel comme un gêneur, un *big brother*, un juge, etc.) ; Complexité, évolutivité, incertitude, inconnu (Le DPO saute du coq à l'âne, ne sait pas tout, peut vite se retrouver dépassé, doit rester en veille permanente, éprouve quelques difficultés à formuler des réponses binaires et immédiates) ; Transversalité (La conformité s'insère de façon transverse à l'entreprise et à tous les niveaux, dans tous les projets, dans tous les métiers, en intégrant bien sûr les facteurs humain et organisationnel) ; Adversité face à des adversaires internes (Le DPO n'est pas écouté, pas pris au sérieux, pas soutenu, dénigré, isolé, menacé, agressé, laissé sans moyens suffisants, etc.) ; Gestion de crise (Pour un délégué à la protection des données, cela peut correspondre à un contrôle de la CNIL, à une saisine, à une violation de données, etc.), Communication (Le DPO peut avoir du mal à communiquer et convaincre sur un domaine pouvant paraître austère) ; Sens du travail (Le délégué à la protection des données peut avoir le sentiment d'une érosion de ses valeurs, de ne pas en avoir fait assez, de ne servir à rien) ; Charge de travail.

Pour le RSSI, les familles de critères les plus contributifs au stress sont la relation à la culpabilité (malgré les actions du RSSI, l'entreprise ne peut être totalement à l'abri d'une crise ayant un impact majeur), le contexte de combat (face aux cyberattaquants), la part importante d'incertitude et d'inconnu (le RSSI est confronté à une incertitude permanente sur le moment et la forme du prochain incident), et enfin la complexité de la fonction (Le RSSI se questionne sans cesse sur les stratégies de protection à adopter). Quelles seront-elles pour le DPO ?

Annexe n°2 – Sondage réalisé en mars 2023 auprès des DPO membres de l'AFCDP sur le sujet de l'indépendance du délégué à la protection des données

Sur proposition de l'auteur, un sondage a été mené du 29 mars au 7 avril 2023 auprès des membres de l'AFCDP. Intitulé « *Pour vous, c'est quoi l'indépendance du DPO ?* », ce sondage était ainsi présenté :

> « *Chers Membres, L'article 38.3 RGPD dispose que « 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 » tandis que le considérant 97 précise que « [Les] 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 ».*
>
> *Les lignes directrices concernant les délégués à la protection des données (DPD) du G29 (WP243) rappellent que le DPO doivent être « en mesure d'exercer leurs missions avec un degré suffisant d'autonomie au sein de leur organisme » et apportent quelques précisions.*
>
> *Le même article 38.3 dispose que « 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 » tandis que le considérant précise que « 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 ».*
>
> *Pour le G29, « Cette exigence renforce l'autonomie des DPD et contribue à garantir que ceux-ci agissent en toute indépendance et bénéficient d'une protection suffisante dans l'exercice de leurs missions relatives à la protection des données ».*
>
> *Nous vous invitons à répondre à un questionnaire focalisé sur ces questions. En tant que DPO, comment traduisez-vous dans votre quotidien les concepts d'indépendance et d'autonomie ? Qu'êtes-vous prêts à accepter… et surtout à ne pas accepter ? En bref, pour vous, que veut dire très concrètement l'indépendance du DPO ?* ».

Cent quarante DPO y ont répondu. Voici la valorisation de cette démarche :

Une première série de questions permettait de savoir si l'indépendance du DPO est connue des personnes censées la respecter.

1. **D'après vous, votre responsable de traitement a-t-il connaissance de votre indépendance entant que DPO ?**

32,14 % Oui, j'en ai la certitude
44,29 % Euh...probablement
18,57 % Je suis sûr que non
5 % Je ne sais pas

2. **D'après vous, les Directeurs des différents services avec lesquels vous interagissez ont-ils connaissance de votre indépendance en tant que DPO ?**

13,57 % Oui, tous. J'en ai la certitude
31,43 % Euh... probablement
26,43 % Uniquement ceux auxquels j'ai dû mettre « les points sur les i »
24,29 % Je suis sûr que non
4,29 % Je ne sais pas

3. **Mais les en avez-vous informés ?**

8,57 % Non, j'ai pensé qu'ils en étaient conscients
15 % Non, je ne les ai pas informés

9,29 % J'ai essayé, notamment en proposant au dirigeant de signer la Charte de déontologie du DPO (mais il a refusé)
35 % Certains d'entre eux uniquement
32,14 % Oui, je les ai tous clairement informés (ou ils ont tous été informés)

4. **Lors de vos actions de sensibilisation (auprès de la direction, de l'encadrement, ses salariés), faites-vous état de votre indépendance ?**

42,86 % Oui, systématiquement ou très souvent
46,43 % Rarement
10,71 % Jamais

5. **Avez-vous proposé à votre responsable de traitement de signer la Charte de déontologie du DPO, qui comprend un chapitre dédié à l'indépendance du Délégué ?**

10,71 % Oui, et il l'a signée
10,71 % Oui, mais il ne l'a pas signée (pas voulu ou pas encore)
62,86 % Non, je n'ai pas essayé
15,71 % Il existe une Charte de déontologie du DPO ?

6. **Votre indépendance en tant que DPO est-elle « officialisée » ?**

37,01 % Oui, elle apparait clairement dans ma lettre de mission
3,25 % Oui, grâce à la signature par mon responsable de traitement de la Charte de déontologie du DPO
12,34 % Oui, elle a été affirmée par la direction lors de ma désignation
40,26 % Non, elle n'apparait nulle part
7,14 % Je ne sais pas

Les répondants avaient la possibilité d'ajouter un commentaire. En voici une sélection. Quelques répondants avouent ne jamais évoquer leur indépendance : « *Je n'en parle pas* », *« Je pense ne pas être suffisamment clair sur le sujet...* », « *Je n'insiste pas sur ce point actuellement* », « *Je ne le fais pas et c'est là mon erreur* », « *Je n'ose pas parler d'indépendance* ». L'un d'entre eux préfère délayer le terme : « *Le terme indépendance est parfois mal perçu par les responsables de traitement, j'ajoute donc l'obligation de reporting et le devoir d'alerte* », tandis qu'un autre préfère utiliser un autre mot : « *Je parle plus de neutralité que d'indépendance* ».

Certaines contributions traduisent un malaise certain : « *Il m'a été indiqué qu'il ne fallait pas confondre indépendance et autonomie. Sous-entendu : il n'est pas question d'indépendance dans votre mission de DPO* », « *Il m'est difficile de faire état de ma supposée indépendance, étant en conflit d'intérêt du fait de mes multiples missions* », « *Mon rattachement actuel empêche fonctionnellement mon indépendance : lorsque j'aborde ce sujet avec ma hiérarchie, la proposition de me rendre indépendant est systématiquement refusée* » et « *C'est compliqué en tant que DPO d'une collectivité territoriale de faire passer la notion d'indépendance d'un agent rattaché à un Directeur général adjoint* ». Notons également cet apport pertinent : « *Le DPO est un peu comme un médecin ou un avocat : sa mission n'est pas de faire plaisir à celui qui le consulte, mais de lui donner un diagnostic sur la situation et de le conseiller sur la meilleure marche à suivre* ».

18,57 % des responsables de traitement et 24,29 % des directeurs de service n'ont pas connaissance de l'indépendance du DPO. Cela n'a rien d'étonnant alors que 23,57 % des répondants indiquent n'avoir rien fait pour que cela se sache, que 10,71 % n'en parlent jamais et que, pour 40,26 % des DPO, leur indépendance n'est formalisée nulle part.

Par référence à la partie IV du présent document, les actions suivantes sont susceptibles de corriger la donne :

- Action CNIL : Que la Commission adresse à chaque responsable de traitement qui vient de désigner son DPO interne un courrier « mettant les points sur les i » et lui rappelant ses obligations concernant son Délégué à la Protection des Données (et faisant clairement état de son indépendance)
- Action DPO : Inciter les DPO à définir, établir, faire connaitre et défendre leur indépendance
- Action DPO : Tout DPO devrait faire l'effort de soumettre à la signature du responsable de traitement la Charte de déontologie du DPO

Avec la série suivante de questions, l'objectif était de tenter de définir ce qu'est l'indépendance du DPO et l'idée que s'en font les personnes qui en bénéficient (ou qui devraient en bénéficier).

7. Avez-vous une idée claire de ce qu'est exactement votre indépendance en tant que DPO ?

45 % Oui, et je peux facilement en donner une définition et des exemples. Je sais parfaitement où elle commence et jusqu'où elle va

47,14 % J'en ai une certaine idée, mais sans avoir l'assurance de sa pertinence

7,86 % Non, j'aurai quelques difficultés à l'objectiver

8. En tant que DPO, avez-vous quelques difficultés à formuler un avis dont vous savez pertinemment qu'il risque de ne pas être apprécié de la direction/du responsable de traitement ?

59,29 % Non, aucune difficulté. Mes avis sont motivés et j'essaie quand c'est possible de suggérer des pistes d'amélioration

35 % Oui, j'avoue que cela peut être difficile du fait des réactions possibles

5,71 % Oui, j'avoue que cela m'est souvent difficile

9. D'après vous, l'indépendance dont il est ici question…

20,71 % C'est principalement inné, ça ne s'apprend pas, cela fait partie du caractère, de la personnalité, c'est une posture

79,29 % C'est principalement acquis, ça s'apprend et c'est un état

10. Etes-vous d'accord avec l'affirmation suivante ? : « La capacité à établir et défendre son indépendance devrait faire partie des *soft skills* indispensables à la fonction de DPO »

56,43 % Oui, tout à fait d'accord

40 % Plutôt d'accord

3,57 % Pas d'accord

11. Avez-vous connaissance d'une méthode (ou d'une formation) pour apprendre à assoir et défendre son indépendance ?

4,29 % Oui, et je peux en témoigner car je l'ai suivie/je m'en suis inspiré

4,29 % Oui, mais je n'en n'ai pas bénéficié

87,14 % Pas à ma connaissance, mais je suis intéressé à en connaître

4,29 % Pas à ma connaissance, et je pense que c'est peine perdue, l'indépendance ne s'apprend pas (c'est un état d'esprit)

La difficulté qu'ont les DPO pour définir concrètement leur indépendance se retrouve dans les réponses apportées à une série de questions de type « scenario » (« *D'après vous, en tant que DPO, considéreriez-vous la situation suivante comme une atteinte à votre indépendance ?* »). Cinq situations (parmi celles proposées)

constituent clairement une atteinte à l'indépendance des DPO (pour plus des trois quarts des répondants) :

12. Vous avez demandé à plusieurs reprises à rencontrer les opérationnels pour obtenir des éléments indispensables à vos missions, sans succès. On en vient à vous interdire même d'essayer…

0,71 % Non. En aucun cas
10 % Il est probable que cela constitue une atteinte à mon indépendance
88,57 % Oui, c'est clairement une atteinte à mon indépendance
0,71 % Je ne sais pas

13. On vous interdit de travailler sur la conformité d'un projet dont vous venez d'apprendre le lancement devant la machine à café

2,14 % Non. En aucun cas
13,57 % Il est probable que cela constitue une atteinte à mon indépendance
82,86 % Oui, c'est clairement une atteinte à mon indépendance
1,43 % Je ne sais pas

14. Vous envisagez de contacter l'un de vos sous-traitants pour vérifier un point précis auprès de leur DPO. La direction, qui en a eu vent, vous l'interdit

1,43 % Non. En aucun cas
17,86 % Il est probable que cela constitue une atteinte à mon indépendance
79,29 % Oui, c'est clairement une atteinte à mon indépendance
1,43 % Je ne sais pas

15. Un nouveau responsable légal vient d'arriver. Vous souhaitez le rencontrer afin de vous présenter. Votre « superviseur », qui en a eu vent, vous l'interdit

4,29 % Non. En aucun cas
19,29 % Il est probable que cela constitue une atteinte à mon indépendance
75 % Oui, c'est clairement une atteinte à mon indépendance
1,43 % Je ne sais pas

16. Vous envisagez d'adresser une demande de conseil à la CNIL. La direction, qui en a eu vent, vous l'interdit

2,86 % Non. En aucun cas
21,43 % Il est probable que cela constitue une atteinte à mon indépendance
73,57 % Oui, c'est clairement une atteinte à mon indépendance
2,14 % Je ne sais pas

En revanche, les situations suivantes sont appréciées avec moins de consensus :

17. Vous venez de prendre votre poste et vous prévoyez de commencer par vous présenter aux différentes directions et de les sensibiliser. Votre « superviseur » vous oblige à commencer par un audit

14,29 % Non. En aucun cas
35 % Il est probable que cela constitue une atteinte à mon indépendance
45,71 % Oui, c'est clairement une atteinte à mon indépendance
5 % Je ne sais pas

18. Vous êtes le DPO d'une filiale d'un groupe. Le DPO de l'entité tête de réseau vous ordonne de partager l'une des analyses avec laquelle vous êtes en total désaccord

10,71 % Non. En aucun cas
36,43 % Il est probable que cela constitue une atteinte à mon indépendance
42,14 % Oui, c'est clairement une atteinte à mon indépendance
10,71 % Je ne sais pas

19. Vous étiez dans un bureau qui permettait à tout salarié de venir vous voir, sans aucun filtrage, pour parler de la conformité au RGPD des traitements mis en œuvre par votre organisme. On veut vous déménager dans un bureau qui est situé dans une zone à accès très restreint…

21,43 % Non. En aucun cas
38,57 % Il est probable que cela constitue une atteinte à mon indépendance
30 % Oui, c'est clairement une atteinte à mon indépendance
10 % Je ne sais pas

20. Vous disposiez d'un budget propre, mais on vous demande de le diviser par quatre (alors qu'on demande un effort moindre aux autres directions…)

10,71 % Non. En aucun cas
54,29 % Il est probable que cela constitue une atteinte à mon indépendance
29,29 % Oui, c'est clairement une atteinte à mon indépendance
5,71 % Je ne sais pas

Deux nouvelles questions faisaient appel à l'imagination des répondants : « *En tant que DPO, comment réagiriez-vous en face de la situation suivante ?* » :

21. Durant vos congés, l'avis négatif que vous aviez formulé dans une analyse d'impact est devenu positif (mais toujours sous votre signature)

0,55 % Je serre les dents et je fais celui qui n'a rien vu
14,21 % J'informe mon superviseur oralement
67,76 % J'informe le responsable de traitement (par écrit)
11,48 % J'envisage de quitter l'organisme si ce fait n'est pas corrigé
4,92 % Correction ou pas, je me prépare à quitter l'entreprise
1,09 % Je ne sais pas

22. À la suite d'une violation de données, vous avez conseillé au responsable de traitement de communiquer auprès des personnes. Vous découvrez que votre superviseur a modifié radicalement votre note avant de la transmettre à la grande direction, sans vous en informer

1,85 % Je serre les dents et je fais celui qui n'a rien vu
79,63 % J'informe le responsable de traitement (par écrit)
10,49 % J'envisage de quitter l'organisme si ce fait n'est pas corrigé
5,56 % Correction ou pas, je me prépare à quitter l'entreprise
1,09 % Je ne sais pas

On voit bien ici la nécessité de mieux définir ce que recouvre très concrètement l'indépendance dont doit bénéficier le DPO au titre du RGPD.

Etaient ensuite proposées aux membres de l'association qui regroupe les DPO des questions sur leur situation, en lien avec le thème de l'indépendance :

23. En tant que DPO, pouvez-vous facilement et librement contacter votre responsable de traitement (ou son représentant, en cas de délégation de pouvoirs) ?

52,35 % Oui, sans aucun filtre ni limite
26,85 % Uniquement en cas de grande difficulté ou en cas d'urgence
18,12 % Après être passé par un supérieur, qui peut me refuser cette prise de contact
2,68 % Jamais

24. En tant que DPO, pouvez-vous/pourriez-vous contacter les services de la CNIL ?

74,29 % Oui, sans aucun filtre ni limite
19,29 % Uniquement en cas de grande difficulté ou en cas d'urgence
6,43 % Après être passé par un supérieur, qui peut me refuser cette prise de contact

25. En tant que DPO, avez-vous la possibilité d'indiquer clairement votre avis divergent au niveau le plus élevé de la direction et aux décideurs en matière de protection des données personnelles ?

61,43 % Oui, sans aucun problème
27,14 % Oui, mais à mes risques et périls
11,43 % Cela m'est très difficile

26. En tant que DPO, avez-vous la possibilité d'adresser une note d'analyse à votre responsable de traitement (faisant état, par exemple, d'une non-conformité) ?

58,57 % Oui, directement, sans aucun problème
30,71 % Oui, mais après l'avoir soumis à un superviseur (qui peut exiger qu'elle soit modifiée)
9,29 % Non, une telle note doit être adressée à mon superviseur, qui décide de son sort
1,43 % Non, on m'a interdit de telles initiatives

27. En tant que DPO interne, disposez-vous d'un budget ?

20, 71 % Oui, et il est non modifiable en cours d'exercice
20 % Oui, mais il peut être modifié en cours d'exercice
59,29 % Non

28. Si vous avez un budget, disposez-vous d'une autonomie budgétaire ?

22,45 % Oui, j'utilise mon budget librement
77,55 % Non, je dois soumettre mes projets pour décision par la direction

Si les répondants avaient déjà essuyé un refus, il leur était demandé de préciser la nature de la dépense qu'ils souhaitent engager. Viennent en premier les refus de formation, d'achat de documentation, d'adhésion à une association de DPO et de participation à une conférence (ce qui correspond à une infraction à l'exigence visant à permettre au délégué à la protection des données d'entretenir ses connaissances spécialisées). Suivent des refus d'acquisition d'outils facilitant la tenue des registres, de prestations d'accompagnement, de lancement d'une campagne de sensibilisation des salariés au RGPD et de déplacement du délégué dans un autre site que possède la société.

Plus de 20 % des répondants n'ont pas de réelle possibilité de porter conseil au responsable de traitement, comme le prévoit l'article 39.1.a du RGPD, et presque 60 % ne disposent d'aucun budget, ce qui limite

leur liberté d'action. Par référence à la partie IV du présent document, les actions suivantes sont susceptibles de corriger la donne :

- Action CNIL : Que la Commission adresse à chaque responsable de traitement qui vient de désigner son DPO interne un courrier lui rappelant ses obligations concernant son Délégué à la Protection des Données
- Action DPO : Inciter les DPO à demander un budget

L'ambition était ensuite de savoir si les répondants avaient déjà vécu des situations dans lesquelles leur indépendance avait été attaquée :

29. De votre perception, la direction de votre organisme a-t-elle déjà tenté de porter atteinte à votre indépendance en tant que DPO ?

51,43 % Non, jamais
29,29 % Oui, à de très rares exceptions
14,29 % Oui, à plusieurs occasions
5 % Oui, fréquemment

Une saisie libre permettait aux répondants d'apporter plus de précisions. Deux commentaires témoignent d'une surcharge du délégué afin qu'il consacre moins de temps à ses tâches liées à la protection des données personnelles : « *On me bombarde de travail en tant que juriste, et ma fonction de DPO passe à la trappe* » et « *On m'a obligé à passer d'un temps plein sur la fonction de DPO à un tiers temps* ». Une supervision trop pesante se retrouve dans plusieurs témoignages : « *Il ne m'est pas possible d'adresser directement à la direction mes notes visant à faire arbitrer un risque fort de non-conformité au RGPD. Je dois obligatoirement les soumettre à mon supérieur* », « *Mon responsable vérifie tout ce que j'écris. Systématiquement, sans connaitre les tenants et les aboutissants, il modifie mes documents et procédures. Où est l'indépendance du DPO dans ce cas ?* », « *Je suis sous la responsabilité d'une personne à qui je dois tout soumettre. Ce n'est qu'une fois validé ou non que mon avis est transmis à la direction. En quelque sorte, il s'agit d'un filtre. Cette personne n'a, par ailleurs, aucune connaissance RGPD.* ». Plus inquiétants sont les commentaires qui reflètent des situations dans lesquelles on a « tordu le bras » du DPO : « *Au sein de notre entreprise, c'est la DSI qui fait la loi. Je dois obéir à ses volontés* », « *On insiste pour obtenir mon approbation, jusqu'à temps que je cède. Usant* », « *On a déjà modifié mes avis documentés, sans que j'en sois informé* », « *On m'a dicté la réponse à fournir dans un cas de non-conformité* », « *Sur un projet pour lequel je considérais la minimisation insuffisante et le risque élevé, il m'a été demandé de réduire mon évaluation dans l'analyse d'impact pour le rendre acceptable* » et « *Après avoir formulé un avis négatif sur un projet, j'ai été convoqué à la direction et mis sous pression* ».

La question suivante était en rapport avec celles portant sur le « faire savoir » abordé au début du questionnaire :

30. Si votre direction a déjà tenté de porter atteinte à votre indépendance, d'après-vous, était-ce…

20,51 % Involontaire de sa part, car elle n'avait pas connaissance de mon indépendance en tant que DPO
19,23 % Volontaire, car elle a parfaitement connaissance de mon indépendance en tant que DPO
44,87 % Cela dépend des cas
15,38 % Je ne sais pas

31. En tant que DPO, avez-vous déjà reçu de la part de la direction de votre organisme des « instructions » sur la façon de traiter une affaire (et les résultats auxquels on vous demande d'aboutir) ?

50,71 % Non, jamais
32,86 % Oui, à de très rares occasions
13,57 % Oui, à plusieurs occasions
2,86 % Oui, fréquemment

32. En tant que DPO, avez-vous déjà été la cible de l'une (ou de plusieurs) des formes que peuvent prendre les menaces et pressions à votre encontre ?

14 % Discours tenant à vous culpabiliser (« *Si le projet échoue ce sera de ta faute* »)
14 % Autre
13 % Surcharge de travail (y compris par un travail inutile)
10 % Absence de promotion ou de retard dans la promotion freins à l'avancement de carrière
7 % Isolement (mise au placard)
6 % Dénigrement systématique (de vos compétences)
6 % Refus de l'octroi d'avantages dont bénéficient d'autres salariés
4 % Retrait de moyens d'aide
4 % Mauvaise notation
4 % Non affectation d'une prime (totale ou partielle)
3 % Mutation interne « forcée » (de poste et/ou géographique)
2 % Remplacement par un autre salarié « à l'échine plus souple »
1 % Convocation pour un entretien préalable à un licenciement
1 % Interruption de la période d'essai
1 % Non reconduction du CDD
1 % Remplacement par un prestataire externe

Le questionnaire se poursuivait sur l'impact sur les DPO de la pression qui peut être exercée sur eux :

33. Vous est-il déjà arrivé par crainte d'une mauvaise réaction de votre direction (voire d'une sanction) ...

23,04 % De vous auto-censurer, en minimisant par exemple votre avis
10,99 % De ne pas mener une action qui fait pourtant partie de vos missions de DPO
10,47 % De modifier l'un de vos avis (qui déplaisait) pour le rendre « acceptable »
9,95 % De ne pas envoyer au responsable de traitement une note qui vous paraissait pourtant utile
5,76 % De porter comme conforme au registre un traitement alors que vous avez un avis différent
39,79 % Non, rien de tout cela ne m'est jamais arrivé

34. En tant que DPO, vous est-il déjà arrivé d'être inquiet concernant votre avenir dans l'organisme, du fait de votre indépendance ?

52,86 % Non jamais
13,57 % À de très rares occasions et cela a été corrigé à chaque fois
20 % À quelques occasions
7,86 % Souvent
5,71 % Je suis inquiet en permanence

Une saisie libre permettait aux répondants d'indiquer qu'elle serait pour eux la « ligne rouge » à ne pas dépasser en termes d'indépendance du DPO (Quel est l'événement qui les inciterait à changer d'employeur ?). Les deux thèmes qui ont recueilli le plus de commentaires sont l'entrave systématique à

l'exercice de la mission et l'existence de menaces et de pressions. Viennent ensuite la création de faux-documents sous la signature du DPO, le manque de reconnaissance du délégué pour le travail accompli et le refus d'être instrumentalisé dans une démarche de *RGPD Washing* : « *Je refuse d'être un DPO « cosmétique » ou de décoration* », « *Un mépris total de la réglementation mais masqué par du maquillage* ».

Enfin le questionnaire se terminait sur l'espoir de voir les choses changer :

35. D'après vous, les règles et pratiques actuelles sont-elles suffisantes pour assurer l'indépendance des DPO internes ?

5,71 % Oui, il n'a rien à modifier ni à améliorer
64,29 % Non. Il y a sûrement quelques initiatives à prendre pour corriger ce qui doit l'être
25 % Non. Nous sommes très loin d'une situation normale. Il faudrait apporter des modifications importantes
5 % Je ne sais pas

36. D'après vous, que pourrait-il être envisagé pour apporter une meilleure protection aux DPO ?

22, 42 % Que la CNIL mène des contrôles à ce sujet et publie des décisions de sanctions exemplaires
27,43 % Que les responsables de traitement soient obligés de s'engager formellement à assurer l'indépendance de leur DPO et de fournir ce document à la CNIL lors de la désignation
18,88 % Que les responsables de traitement soient obligés d'informer le CSE (représentant du personnel) de la désignation de leur DPO, lui donnant ainsi l'occasion de s'assurer de ses conditions d'exercice, dont son indépendance)
15,93 % La création d'une protection juridique spécifique (mais sans aller jusqu'au statut de salarié protégé)
14,45 % En faisant du DPO un salarié protégé
0,88 % Je ne sais pas (ou sans avis)

Les membres de l'AFCDP pouvaient répondre en saisie libre à la question « *Qu'attendez-vous très concrètement de la CNIL sur le sujet de l'indépendance du DPO ?* ». On y retrouve l'espoir de voir prochainement la Commission publier des sanctions à l'encontre de responsables de traitement qui n'assurent pas à leur DPO les conditions d'exercice prévues par le RGPD : « *Pour que l'indépendance du DPO soit prise au sérieux, il est fondamental que la CNIL effectue des vrais contrôles à ce sujet* », « *Quelle arrête de fuir ses responsabilités et qu'elle veille très concrètement (avec des sanctions si besoin) au respect par les responsables de traitement des dispositions que contient le RGPD au sujet du Délégué à la Protection des Données !* », « *Qu'elle fasse tout simplement respecter la législation et le statut du DPO, cela fait partie de ses missions.* ». Est vivement espéré également un effort de communication de la part de l'autorité de contrôle vers les responsables de traitement : *« Informer les responsables de traitement en leurs adressant une plaquette par courrier* », « *Que la CNIL soit très explicite auprès des employeurs concernant l'indépendance du DPO* », « *Une communication à destination de l'ensemble des RT ayant désigné un DPO pour poser les termes du débat et ses enjeux* », « *Qu'elle engage une action significative auprès des RT du rôle important du DPO. Un courrier devrait être adressé par la CNIL pour renforcer notre rôle* », « *Tout simplement une meilleure communication sur ce principe de droit !* ».

Quelques contributions évoquent un formalisme plus strict lors de la désignation d'un délégué à la protection des données : « *Imposer une lettre de nomination du DPO* », « *Formaliser l'engagement du responsable de traitement et l'éventuel superviseur de respecter l'indépendance du DPO* », « *Ajouter un registre obligatoire reprenant tous les avis DPO vs. les décisions du Responsable de traitement – argumenté* », « *Rendre obligatoire la lettre de mission et la prise de connaissance de la charte d'indépendance* », « *Que la CNIL exige du responsable de traitement l'engagement de respecter l'indépendance du DPO* ». Quelques contributions traduisent un besoin d'un soutien des DPO plus marqué de la part de la Commission : « *Une forme de protection qui permette au DPO de la contacter et qui permette un rappel à la loi au responsable de traitement chaque fois que nécessaire* », « *Un positionnement clair en faveur des DPO lorsque l'un d'entre*

eux l'a contactée et a justifié des manquements à son indépendance », « *Que la CNIL soit plus aidante pour les DPO mis en difficulté* ».

En revanche, peu nombreuses sont les contributions à l'appui de la piste qui consisterait à faire du DPO un salarié protégé : « *Créer un statut de protection du DPO* », « *Organiser la profession des DPO avec code de déontologie, discipline et régulation. La mise en place d'un Ordre professionnel à l'instar de celui des médecins ou experts-comptables serait bénéfique* », « *Une proposition de loi pour avoir un statut juridique protecteur* », « *En faire une profession règlementée* », « *Le poste de DPO devrait être sanctuarisé comme assurant une mission de service public essentiel, avec ce que ça suppose en respect d'une déontologie et d'une pratique au service des individus avant toute autre préoccupation* ».

Enfin le questionnaire se terminait sur la posture que prendrait le répondant si son indépendance était attaquée :

37. Envisageriez-vous de contacter la CNIL si votre responsable de traitement vient à ne pas respecter votre indépendance en tant que DPO ?

22,62 % Oui, sans hésiter, mais après en avoir échangé avec mon responsable de traitement
1,79 % Oui, sans hésiter, sans en échanger avec mon responsable de traitement
13,69 % Oui, mais je doute de l'efficacité de la démarche
19,64 % Non, car je pense que la CNIL ne prendra aucune action
21,43 % Non, car les actions de la CNIL vont me mettre en difficulté
13,69 % Non (pour d'autres raisons)
7,14 % Je ne sais pas

38. Envisageriez-vous d'agir en justice si votre responsable de traitement vient à ne pas respecter votre indépendance en tant que DPO ?

2,86 % Oui, sans hésiter
6,43 % Oui, mais j'ai peur que cela ne se termine pas en ma faveur
13,57 % Non, car j'aurai crainte de ne pas pouvoir retrouver un poste de DPO
13,57 % Non, j'essayerai d'obtenir une transaction pour partir
45 % Non, je chercherai un autre poste
18,57 % Je ne sais pas

Annexe n° 3 - Synthèse des points de contrôles sur les conditions d'exercice du DPO, sur la base de l'analyse des délibérations de la CNPD luxembourgeoise

Tiré de l'analyse des délibérations publiées par la CNPD luxembourgeoise qui témoignent des vingt-cinq contrôles qu'elle a réalisés courant 2018, voici un tableau qui synthétise les points qui avaient été vérifiés, les attentes du chef d'enquête et quelques éléments qui pouvaient être fournis à titre de preuve par le responsable de traitement.

Dans l'éventualité d'un contrôle par la CNIL, les DPO devraient vérifier leur statut sur chacun de ses aspects et commencer à préparer des éléments de preuve.

Point de contrôle	Attentes du contrôleur	Eléments de preuve
Désignation d'un DPO (art. 37.1 du RGPD)	Le chef d'enquête prend pour référence les lignes directrices du G29 relatives au DPO (WP243)	Logiquement, la CNIL doit déjà être en possession de cette information (sinon, production de la désignation du DPO auprès de la Commission)

Point de contrôle	Attentes du contrôleur	Eléments de preuve
Publication des coordonnées du DPO (art. 37.7 du RGPD)	Lors de la préparation de la mission de contrôle, le chef d'enquête a vérifié si le DPO peut être contacté par les personnes concernées	Preuve de la publication des coordonnées du DPO (il ne s'agit pas forcément de la publication de son identité mais des moyens, pour les personnes concernées, de le contacter)
Coordonnées du DPO communiquées à la CNIL (art. 37.7 du RGPD)	Lors de la préparation de la mission de contrôle, le chef d'enquête a vérifié si les coordonnées du DPO ont été communiquées à la CNIL	Logiquement, la CNIL doit déjà être en possession de cette information (sinon, production de la désignation du DPO auprès de la Commission)
Expertise et compétences du DPO suffisantes (art. 37.5 du RGPD)	Le chef d'enquête s'attend à ce que le DPD ait au minimum X années d'expérience professionnelle en matière de protection des données (par exemple 3 ans pour une entité traitant des données « sensibles ») Les compétences doivent être « élargies » (compétences juridiques et techniques) et l'expérience confirmée	*Curriculum Vitae* du DPO Démonstration de l'adéquation de l'expertise et des compétences du DPO au regard de la complexité et de la sensibilité des traitements mis en œuvre Preuves des formations suivies par le DPO Preuves de la veille réalisée par le DPO Adhésion à une association de DPO
Absence de conflit d'intérêt (art. 38.6 du RGPD)	Le chef d'enquête s'attend à ce que le DPD n'exerce aucune autre fonction qui le conduirait à déterminer les finalités et les moyens d'un fichier : en d'autres termes, il ne peut pas être « juge et partie »	Description de poste et lettre de mission du DPO suffisamment précises et détaillées pour éviter tout conflit d'intérêts Règles internes visant à éviter les conflits d'intérêts Déclaration formelle selon laquelle le DPO n'a pas de conflit d'intérêts en ce qui concerne sa fonction
Ressources suffisantes (art. 38.2 du RGPD)	Le chef d'enquête prend pour référence les lignes directrices du G29 relatives au DPO (WP243), en tenant compte de « l'importance » des traitements	Temps alloué au DPO afin qu'il puisse accomplir ses tâches Plan de travail et indicateurs Aides internes et externes mises à disposition du DPO Budget dont dispose le DPO Charte de déontologie du DPO (AFCDP) signée du Responsable de traitement et du DPO
Autonomie/Indépendance du DPO (art. 38.3 du RGPD)	Le chef d'enquête s'attend à : ce que le DPO soit rattaché au plus haut niveau de la direction afin de garantir au maximum son autonomie ; que la reddition de compte directe auprès du plus haut niveau de la direction soit formalisée ; que l'accès au responsable de traitement soit inconditionnel, facile et permanent	Organigramme montrant le rattachement du DPO au responsable de traitement Reddition de compte directe, inconditionnelle et formalisée auprès du plus haut niveau de la direction Tout document démontrant que le DPO peut agir sans recevoir d'instruction en ce qui concerne l'exercice de ses missions Budget dont dispose le DPO (lui permettant par exemple de faire réaliser les audits de son choix) Charte de déontologie du DPO (AFCDP) signée du Responsable de traitement et du DPO

Point de contrôle	Attentes du contrôleur	Eléments de preuve
DPO associé à toutes les questions relatives à la protection des données personnelles (art. 38.1 du RGPD)	Comme l'exige le RGPD, le chef d'enquête s'attend à ce que le responsable du traitement veille à ce que son DPO soit associé, d'une manière appropriée et en temps utile à toutes les questions relatives à la protection des données à caractère personnel.	Procédure ou méthode de développement de projet imposant la sollicitation du DPO Traces formelles de réunions régulières entre le DPO et les chefs de service qui traitent le plus de données personnelles Consigne donnée à chaque personne en charge d'un projet de traiter avec le DPO la question de la protection des données Preuves quant à la présentation du rapport d'activité du DPD au Comité de Direction sur une fréquence régulière
Le DPO informe et conseille le responsable de traitement et les employés (art. 39.1.a du RGPD)	Le chef d'enquête s'attend à ce que les missions d'information et de conseil du DPO à l'égard du responsable de traitement soient formalisées, par exemple avec un rapport d'activité spécifique sur la protection des données, et que le Délégué soit librement en mesure de signifier des conseils formels au responsable de traitement Le chef d'enquête s'attend à ce que l'intégralité des personnes agissant sous la responsabilité exclusive ou partielle du responsable du traitement en ce qui concerne le traitement de données personnelles suivent des formations régulières et en rapport direct avec la conformité	Traces du reporting formel des activités du DPO auprès de la direction, sur la base d'une fréquence définie Traces de conseils formels adressés par le DPO auprès du responsable de traitement Description du plan de sensibilisation de la direction, de l'encadrement et des employés Preuves de la réalisation du plan de sensibilisation Charte de déontologie du DPO (AFCDP) signée du Responsable de traitement et du DPO
Le DPO contrôle la conformité des traitements (art. 39.1.b du RGPD)	Le chef d'enquête s'attend à ce que l'organisme dispose d'un plan de contrôle formalisé en matière de protection des données, même s'il n'est pas encore exécuté	Plan de contrôle (d'audit) formel maîtrisé par le DPO et endossé par la direction Mention, dans la lettre de mission du Délégué, de sa mission de contrôle Rapport(s) d'audit(s) déjà réalisés
Le DPO assiste le responsable de traitement dans la réalisation de PIA (art. 39.1.c du RGPD)	Le chef d'enquête prend pour référence les lignes directrices du G29 relatives au DPO (WP243)	Procédure de réalisation des PIA montrant le rôle crucial du DPO PIA comportant l'avis formel et documenté du DPO

Annexe n° 4 – Questions soulevées par la CNIL dans le cadre de sa participation à l'action conjointe européenne pour 2023 portant sur les conditions d'exercice du DPO

Dans le cadre de l'action conjointe décidée pour 2023, la CNIL a commencé courant mars 2023 à réaliser des contrôles sur pièces auprès d'un certain nombre de responsables de traitement. Il est possible que, dans un second temps, la Commission procède à quelques contrôles sur place afin de vérifier la véracité des réponses qui lui auront été retournées.

Voici les questions soulevées par la CNIL (pour chacune d'entre elles, elle attend en sus des éléments de preuve, des pièces justificatives) :

1. Présenter l'organisme (activités, effectif total, chiffre d'affaires, trois derniers bilans comptables, organigramme, gouvernance, sociétés sœurs ou filiales, etc.)
2. Fournir, dans son intégralité, le registre des activités de traitement de l'organisme
3. Fournir, dans son intégralité, le registre des incidents de sécurité[136] de l'organisme
4. L'organisme a-t-il désigné un délégué à la protection des données ? Cette désignation relevait-elle d'un caractère obligatoire ? Si des documents d'analyse ont été produits en ce sens, les fournir
5. La personne désignée comme délégué à la protection des données a-t-elle été désignée pour un groupe d'organismes ou plusieurs organismes ?
6. Le délégué à la protection des données est-il un membre du personnel de l'organisme ou exerce-t-il cette fonction sur la base d'un contrat de service ? Le cas échéant, fournir une copie de ce contrat de service
7. Dans le cas où le délégué à la protection des données est un membre du personnel de l'organisme, quelle est la nature juridique des relations établies avec le délégué à la protection des données (CDI, CDD, autre) ? Dans le cas d'un contrat à durée déterminée, une procédure a-t-elle été mise en place pour le remplacement de la personne ? Fournir le contrat
8. Quelles exigences avaient été fixées pour l'attribution du poste de délégué à la protection des données lors de la publication de l'offre d'emploi ?
9. Sur la base de quelles qualifications ou diplômes a été désigné le délégué à la protection des données ?
10. Sur la base de quelles expériences professionnelles a été désigné le délégué à la protection des données ? Indiquer les différents postes précédemment occupés et le nombre d'années dans des postes en lien avec la protection des données ou avec le secteur d'activité de l'organisme
11. Où est situé géographiquement le délégué à la protection des données ?
12. La direction de l'organisme a-t-elle clairement défini et donné une description écrite des tâches du délégué à la protection des données ? Fournir tout élément formalisant ces mission (lettre de mission, avenant au contrat de travail, fiche de poste, etc.)
13. Des tâches supplémentaires à celles prévues par le RGPD ont-elles été confiées au délégué à la protection des données (tenue du registre des activités de traitement, rédaction de politiques relatives aux données à caractère personnel)
14. Le délégué à la protection des données exerce-t-il cette fonction à temps plein ?
15. Dans les cas où le délégué à la protection des données n'exerce pas à temps plein, combien d'heures de travail par semaine peut-il consacrer à l'exécution des tâches du délégué à la protection des données ?
16. Le délégué à la protection des données est-il assisté par d'autres personnes pour s'acquitter de ses tâches, par exemple un adjoint ou une équipe chargée de la protection des données (donner l'équivalent temps plein), des personnes relais ou « référente RGPD » au sein de l'organisme, un ou plusieurs partenaires (cabinet de conseil, cabinet d'avocat, etc.) ou tout autre dispositif similaire ?
17. Comment ont été évaluées les ressources en temps de travail nécessaires à la réalisation des missions du délégué à la protection des données ? Cette évaluation a-t-elle été mise à jour par la suite au regard de la charge de travail effective du délégué ?

[136] Cette formulation est surprenante. En effet, si l'article 33. 5 du RGPD dispose que « *Le responsable du traitement documente toute violation de données à caractère personnel* », il ne prévoit pas de documenter les « *incidents de sécurité* ». Comme l'indiquent par exemple les lignes directrices du CEPD sur les notifications de violations de données à caractère personnel à l'intention des institutions et organes de l'Union européenne dans leur point 26 « *Tout incident lié à la sécurité de l'information n'est pas nécessairement une violation de données à caractère personnel* ».

18. L'organisme a-t-il alloué un budget spécifique aux activités du délégué à la protection des données ? Le cas échéant, le délégué à la protection des données peut-il gérer ce budget de manière indépendante ? Sinon, préciser le circuit de validation
19. De combien d'heures de formation annuelle le délégué à la protection des données dispose-t-il/elle pour développer et maintenir son expertise professionnelle en matière de protection des données à caractère personnel ? Qui valide ces demandes de formation et sur quels critères ? Fournir la liste des formations suivies lors des années précédentes par le délégué à la protection des données, ainsi que les formations prévues pour l'année en cours
20. Si le délégué à la protection des données exerce d'autres fonctions par ailleurs (telles que directeur général des services, directeur des opérations, responsable du département marketing, responsable des ressources humaines, responsable du service informatique, etc.) supplémentaires en plus de ses tâches de délégué, quelles sont-elles ? Dans ce cadre, le délégué a-t-il un pouvoir décisionnel sur la détermination des finalités et des moyens de traitements de données à caractère personnel ? Le cas échéant, fournir tout élément produit sur l'absence de conflits d'intérêts avec les missions de délégué à la protection des données, ou les moyens mis en place pour minimiser ce(s) conflit(s) d'intérêts
21. Dans quelles situations les salariés/agents mettant en œuvre des traitements sont-ils tenus ou ont-ils la possibilité de communiquer une demande interne au délégué à la protection des données ? Par quels canaux de communication les demandes internes sont-elles adressées au délégué ? Existe-t-il un document formalisant la procédure pour entrer en contact avec le délégué ?
22. Combien de demandes internes le délégué à la protection des données reçoit-il en moyenne au cours d'un mois ?
23. Le délégué à la protection des données participe-t-il ou est-il consulté sur la sensibilisation et la formation des salariés participants aux traitements de données à caractère personnel ? Fournir les documents justificatifs (supports de formation, attestation de présence, etc.)
24. L'organisme a-t-il réalisé des analyses d'impact à la protection des données à caractère personnel ? Le cas échéant, le délégué à la protection des données a-t-il été consulté et comment cette consultation a-t-elle été formalisée ?
25. Le délégué à la protection des données peut-il facilement échanger avec les salariés/agents mettant en œuvre des traitements de données à caractère personnel ou avec les services informatiques ? Dispose-t-il d'un accès aux ressources informatiques utilisées dans le cadre de cette mise en œuvre (par exemple, accès aux bases de données) ? Cet accès est-il restreint pour certains traitement ou bases de données et, le cas échéant, selon quelles modalités ?
26. Les analyses ou recommandations du délégué à la protection des données peuvent-elles être orientées, amendées ou soumises à validation par un supérieur hiérarchique ou par un autre service ? Le cas échéant, décrire le processus de validation
27. Dans le cas où l'avis du délégué à la protection des données n'est pas suivi par l'organisme, les raisons en sont-elles documentées ? Fournir l'exemple d'une documentation établie en ce cas
28. Le délégué bénéficie-t-il de garanties lui assurant qu'il n'est pas pénalisé (par exemple, sur l'obtention d'avantages professionnels ou l'avancement de carrière) pour l'exercice de ses fonctions ? Le cas échéant, préciser ces garanties
29. Dans quel contexte la désignation du précédent délégué à la protection des données a-t-elle pris fin (changement de poste, démission, licenciement) ? Une période de formation entre l'ancien et l'actuel délégué a-t-elle été prévue ?
30. Dans le cas d'un délégué à la protection des données désigné en interne, celui-ci est-il rattaché à une direction ? Quels éléments ont poussé à ce rattachement ?
31. Le délégué à la protection des données fait-il régulièrement rapport au plus haut niveau de direction de l'organisme ? Dans l'affirmative, à quelle fréquence et selon quelle modalité ? Fournir des éléments sur ce rapport (compte-rendu, présentation, etc.)

32. Le délégué à la protection des données est-il invité à participer ou informé des suites des réunions stratégiques de l'organisme relatives aux traitements de données à caractère personnel (présence aux réunions de directions, comité d'orientation du système d'information et aux réunions transversales et métiers) ? Si oui, sur quels critères et à quelle fréquence ?
33. L'organisme a-t-il publié les coordonnées du délégué à la protection des données ? Par quel canal et sur quels supports ? Fournir une copie des supports utilisés
34. Le délégué à la protection des données participe-t-il ou est-il consulté sur les réponses à apporter aux demandes d'exercice de droit des personnes concernées (droit de rectification, droit d'effacement, etc.) ? Combien l'organisme a-t-il reçu de demandes d'exercices de droits au cours des trois précédents mois ?
35. Les personnes concernées, y compris les employés de l'organisme, ont-elles la possibilité de contacter le délégué à la protection des données pour des questions liées au traitement de leurs données à caractère personnelle ou à l'exercice de leurs droits ? Préciser par quels moyens
36. La confidentialité des échanges avec le délégué à la protection des données est-elle garantie, et le cas échéant, par quels moyens ?

De son côté, l'autorité irlandaise (DPC) a préféré adresser un sondage (et non un contrôle) à une sélection de DPO le 15 mars. Les destinataires ont jusqu'au 12 mai 2023 pour répondre, s'ils le souhaitent (ils peuvent également y répondre, mais en cochant « *Je ne souhaite pas répondre* » à certaines questions). Merci à Maître Florence Gaullier du Cabinet Vercken & Gaullier qui a signalé le document « *Questionnaire on the designation and position of data protection officers* ».

On y trouve sur certains points des questions plus précises que celles soulevées par la CNIL, ou des questions supplémentaires telles que :

- *In which of the following topics does the organisation's data protection officer (or members of their staff) have experience or expert knowledge of?,* avec les réponses possibles suivantes : *Data protection and privacy matters, Information security matters, Information systems management and/or development, Data protection processes (e.g. DPIA, Rights of the data subject, Data breach notifications), Business processes of the organisation's industry or field, Legislation on the processing and the protection of personal data, Guidelines of the supervisory authorities on the processing of personal data, Specific legislation concerning the organisation's industry or field* ;
- *When designating the data protection officer, which of the following factors were set as requirements for the role?*, avec les réponses possibles suivantes : *Expert knowledge of data protection regulation, Expert knowledge of data protection practices, Expert knowledge of data protection requirements stemming from special legislation applicable to the organisation's industry or field, Ability to fulfill the tasks pursuant to the GDPR, Other professional qualifications, No particular expertise on data protection, but the designation was compulsory* ;
- *On a yearly basis, how many hours of training does the data protection officer have in order to develop and/or maintain their professional qualities and expert knowledge on data protection law and practices*, avec les réponses possibles suivantes : *0 hours a year, 1–8 hours a year, 9–16 hours a year, 17–24 hours a year, 25–32 hours a year, >32 hours a year* ;
- *Has the data protection officer ever been dismissed or penalised by the organisation for performing their tasks and duties?* (Cette question attend une réponse en oui ou non).

Notons également la présence de la question suivante : *Would you estimate [your resources] to be sufficient in order to fulfill the tasks of the data protection officer?*, qui attend une réponse en oui ou non… ou « *Je ne souhaite pas répondre* ».

L'AEPD espagnole a mis en ligne un questionnaire très similaire à celui de la DPC irlandaise (*Cuestionario sobre la designación, posición y funciones de los Delegados de Protección de Datos*[137]) et le questionnaire soumis par Datatilsynet[138] (l'autorité de contrôle danoise) comporte (entre autres) deux questions en lien avec le sujet du présent document : « *La municipalité donne-t-elle des instructions au DPD pour l'accomplissement de ses tâches ?* » et « *La municipalité a-t-elle déjà sanctionné ou licencié un DPD pour avoir exercé ses fonctions ?* ».

Annexe n° 5 – Auto-quiz permettant d'évaluer son assertivité

L'assertivité, ou comportement assertif, est un concept de la première moitié du XXe siècle introduit par le psychologue Andrew Salter qui désigne la capacité à s'exprimer et à défendre ses droits sans empiéter sur ceux d'autrui.

Voici un auto-quiz proposé par Raffaela Bottino aux participants du Mastère Spécialisé DPO de l'ISEP, qui permet d'évaluer son assertivité (à chaque question : 4 = fréquemment / 3 = de temps en temps / 2 = presque jamais / 1= jamais) :

- Dans une réunion difficile, à l'ambiance échauffée, je suis capable de parler avec calme et confiance
- Si je ne suis pas certain d'une chose, je peux demander de l'aide facilement
- Si un collègue est devant moi et fait preuve d'un comportement agressif ou injuste, je peux intervenir et contrôler la situation avec confiance
- Si quelqu'un me fait une remarque, se montre ironique avec moi ou avec d'autres, je peux répondre sans agressivité
- Si, alors que je cherche à être compréhensif, je crois que l'on commence à abuser de moi, je suis capable de dénoncer l'abus sans hésitation
- Si quelqu'un me demande la permission de faire une chose qui ne me plaît pas (par exemple fumer en ma présence), je peux lui dire non sans me sentir coupable
- Si quelqu'un demande mon opinion sur un sujet, je me sens bien en la lui donnant, même si je sais qu'elle ne concorde pas avec la sienne ou celle de la majorité
- Je peux aborder facilement et lier connaissance avec des personnes que je considère importantes
- Lorsque je trouve une difficulté ou une incohérence dans une situation, je suis capable de l'exposer en réunion sans attaquer les autres personnes et sans me sentir mal à l'aise
- Lorsque j'ai le sentiment que quelqu'un sous-entend à mon encontre quelque chose de négatif de manière sournoise, j'aborde le sujet de manière directe pour éclairer la question

Il suffit ensuite de calculer le total obtenu. Pour disposer des résultats :

- 30-40 points = Je suis assertif
- 29-20 points = Je suis moyennement assertif
- 19-10 points = Je suis peu assertif
- Au-dessous = Je suis très peu assertif

Il existe d'autre questionnaire similaire visant le même objectif, dont celui qui figure dans le livre « *Affirmation de Soi - Mieux gérer ses relations avec les autres*[139] » de Dominique Chalvin, et qui comprend soixante items tels

[137] https://ec.europa.eu/eusurvey/runner/AEPD_02cse
[138] https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/apr/se-spoergsmaalene-undersoegelse-af-dpoer-i-kommunerne
[139] https://www.decitre.fr/livres/l-affirmation-de-soi-9782710131052.html

que « *Je dis souvent oui, alors que je voudrais dire non* », « *Quand il y a un débat, je préfère me tenir en retrait pour voir comment cela va tourner* », « *Quand je me suis fait avoir une fois, je sais prendre ma revanche à l'occasion* » ou « *Je sais écouter et je ne coupe pas la parole* ».