

// le dossier pratique

Le délégué à la protection des données

Désignation, missions, responsabilité et protection

Le délégué à la protection des données (DPD) également nommé DPO est au cœur du règlement européen sur la protection des données (RGPD). Remplaçant le correspondant informatique et libertés (CIL), il a pour mission de conseiller le service RH dans la mise en conformité au RGPD et de contrôler la bonne application en interne du règlement. Désignation, missions, ou encore protection du DPD, nous vous faisons le point dans ce dossier pratique.

Depuis le 25 mai 2018, les délégués à la protection des données (DPD) ont remplacé les correspondants informatique et libertés. Pierres angulaires du nouveau cadre juridique instauré par le **règlement à la protection des données (RGPD) du 27 avril 2016** (*Règlement (UE) 2016/679*), d'application directe, les DPD sont effectivement chargés de s'assurer de la conformité au RGPD au sein des entreprises (ou des organismes) qui les ont désignés. Dans ses **lignes directrices** adoptées dans leur version finale le 5 avril 2017, le **G29**, groupe des « Cnil » européennes, a clarifié et illustré d'exemples concrets le nouveau cadre juridique applicable. En adoptant la **loi n° 2018-1125 du 20 juin 2018**, le législateur français a adapté la loi Informatique et libertés du 6 janvier 1978 au nouveau cadre européen. Son décret d'application (*n° 2018-687*) est paru le 3 août 2018. Afin de permettre l'identification des compétences et savoir-faire du DPD, la Cnil a également adopté, le 20 septembre 2018 *via* deux délibérations, des référentiels en matière de certification de DPO.

À NOTER Une ordonnance n° 2018-1125 du 12 décembre 2018 est intervenue pour réécrire et remettre en cohérence la loi du 6 janvier 1978 et d'autres lois françaises traitant de protection des données.

1 Désignation

DANS QUELS CAS FAUT-IL DÉSIGNER UN DPD ?

Toute entreprise est tenue de désigner un délégué à la protection des données lorsque (RGPD, art. 37, § 1) :

– le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;

– les **activités de base** du responsable de traitement consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un **suivi** régulier et systématique **à grande échelle** des **personnes** concernées ;

– les activités de base du responsable de traitement ou du sous-traitant consistent en un traitement à grande échelle de **données sensibles** (données de santé par exemple).

Dans le secteur privé, les activités de base d'un responsable de traitement ont trait à ses activités principales et ne concernent pas le traitement des données personnelles en tant qu'activité auxiliaire. Elles peuvent être considérées comme les opérations essentielles nécessaires au responsable de traitement (ou du sous-traitant) pour atteindre ses objectifs.

Ainsi, les traitements de données nécessités par les fonctions support de l'entreprise, telles que, par exemple, la gestion RH ou la paie des employés, constituent des activités auxiliaires, qui n'exigent pas la désignation d'un DPD (*v. le dossier pratique -Libertés- n° 40/2018 du 28 février 2018*).

Pour les **entreprises** pour qui la désignation d'un DPD n'est **pas obligatoire**, le **G29** leur **recommande** d'y procéder dans ses lignes directrices. Cela leur permettra de confier à un expert l'identification et la coordination des actions à mener en matière de protection des données personnelles.

L'ENTREPRISE PEUT-ELLE DÉSIGNER UN DPD EXTERNE ?

Tout d'abord, la fonction peut être assurée par un **salarié** du **responsable de traitement** ou du sous-traitant : **DPD interne**. Par exemple, un salarié de leur service RH.

Mais, le délégué peut être une **personne externe**, et dans ce cas, la fonction de DPD est exercée sur la base d'un **contrat de service** conclu avec une personne physique ou morale. Une équipe de personnes travaillant pour le compte du prestataire de services externe peut, dans les faits, exercer les missions du délégué en tant que groupe, sous la responsabilité d'une personne de contact principale responsable du client. Dans ce cas, il est essentiel que chaque membre de l'entité exerçant les fonctions de DPD remplisse l'ensemble des exigences requises pour être désigné en cette qualité. Le G29 recommande de prévoir dans le contrat de service une répartition claire des tâches au sein de l'équipe externe chargée de la fonction de DPD et de désigner une seule personne en qualité de personne de contact principale responsable du client (*RGPD, art. 37, § 6 et lignes directrices du G29, annexe, point 7*).

LE DÉLÉGUÉ PEUT-IL ÊTRE DÉSIGNÉ PAR PLUSIEURS ENTREPRISES ?

Un **groupe d'entreprises** peut désigner un seul DPD, à condition qu'il soit « facilement joignable à partir de chaque lieu d'établissement » (*RGPD, art. 37, § 2*).

La notion de « joignabilité » renvoie aux missions du délégué en tant que point de contact pour les personnes concernées, pour l'autorité de contrôle et également en interne au sein de l'entreprise. Afin de veiller à ce que le DPD, qu'il soit interne ou externe, soit joignable, il est important de s'assurer que ses coordonnées sont mises à disposition. Le délégué, avec l'aide d'une équipe si nécessaire, doit être en mesure de communiquer efficacement avec les personnes concernées et de coopérer avec les autorités de contrôle compétentes, ce qui implique que cette communication s'effectue dans la ou les langues utilisées par les autorités de contrôle et les personnes concernées en question. La disponibilité d'un DPD (qu'il se trouve physiquement dans le même lieu que les salariés ou qu'il soit joignable à travers un service d'assistance téléphonique ou d'autres moyens de communication sécurisés) est essentielle pour que les personnes concernées puissent prendre contact avec lui (*Lignes directrices du G29, annexe, point 7*).

QUI PEUT ÊTRE DÉSIGNÉ DPD ?

Quelle que soit la solution retenue, le DPD doit être désigné « sur la base de ses **qualités professionnelles** et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir [ses] missions » (*RGPD, art. 37, § 5*). Les anciens CIL ont naturellement vocation à devenir DPD.

La personne doit également pouvoir réunir les qualités et compétences suivantes :

- l'**aptitude à communiquer efficacement** et à **exercer** ses fonctions et **missions** en toute indépendance. Le délégué ne doit **pas** avoir de **conflit d'intérêts** avec ses autres missions, de sorte qu'il ne peut occuper des fonctions,

au sein de l'entreprise, qui le conduisent à déterminer les finalités et les moyens d'un traitement – il ne peut pas être juge et partie. Par exemple, le responsable ou le directeur des ressources humaines dont les fonctions le conduisent à déterminer les finalités et les moyens des traitements RH (évaluation des salariés par exemple) ne peut être désigné DPD ;

- une **expertise** en matière de **législations** et **pratiques** relatives à la **protection des données**, acquise notamment grâce à une formation continue. Le niveau d'expertise doit être adapté à l'activité de l'entreprise et à la sensibilité des traitements mis en œuvre ;

- une **bonne connaissance** du secteur d'activité et de l'organisation de l'entreprise, et en particulier des **opérations de traitement**, des **systèmes d'information** et des besoins de l'organisme en matière de protection et de sécurité des données ;

- un **positionnement** efficace en interne pour être en capacité de **faire directement** rapport au niveau le plus élevé de l'entreprise et également d'animer un réseau de relais au sein des filiales d'un groupe par exemple et/ou d'une équipe d'experts en interne (expert informatique, juriste, expert en communication, traducteur, etc.).

Il n'existe donc **pas de profil type** du délégué à la protection des données, qui peut être une personne issue du domaine technique, juridique ou autre. Le service RH sera tout particulièrement vigilant dans le fait de garantir au DPD, dans l'hypothèse où cette fonction est internalisée, un cadre professionnel lui permettant d'exercer pleinement sa mission.

À NOTER Dans un questions/réponses « Devenir délégué à la protection des données » mis en ligne le 23 mai 2017, la Cnil fournit une liste non exhaustive de fonctions susceptibles de donner lieu à un conflit d'intérêts faisant obstacle à la désignation en qualité de DPD : directeur général des services, secrétaire général, directeur général, directeur financier, directeur opérationnel, responsable du département marketing, RRH, ou encore responsable du service informatique. D'autres fonctions peuvent donner lieu à conflit d'intérêt si elles supposent la détermination des finalités et des moyens du traitement. En externe, l'avocat du responsable de traitement le représentant dans des contentieux impliquant des désaccords sur la protection des données personnelles ne peut pas non plus être désigné en qualité de DPD.

COMMENT PROCÉDER ?

■ Déclaration à la Cnil

Il revient au responsable du traitement ou sous-traitant de désigner un délégué à la protection des données (*RGPD, art. 37 ; Loi du 6 janvier 1978, art. 70-17 modifié ; D. n° 2005-1309 du 20 octobre 2005, art. 42 modifié*). Ceux-ci sont tenus de publier les coordonnées du DPD et de les communiquer à la Cnil.

La liste des informations devant être communiquées, que le DPD soit une personne physique ou morale, est la suivante (*Décret précité, art. 43 modifié*) :

- les **nom, prénom** et **coordonnées** professionnelles du **responsable du traitement** ou du sous-traitant ou, le cas échéant, ceux de son représentant. Si le responsable de traitement et/ou le sous-traitant sont des personnes morales, leur dénomination, leur siège social ainsi que l'organe qui les représente légalement ;

- les **nom, prénom** et **coordonnées** professionnelles du **DPD**. Si ce dernier est une personne morale, sa déno-

mination, son siège social ainsi que l'organe qui le représente légalement.

Ces **coordonnées**, ainsi que leurs modifications éventuelles, doivent être **transmises sans délai** et **par voie électronique** à la Cnil, via un téléservice sur www.cnil.fr. La désignation prendra effet le lendemain de la transmission des informations en ligne.

Parmi ces données, la dénomination et les coordonnées professionnelles de l'organisme de même que les moyens de contacter le DPD sont diffusés sous format ouvert et aisément réutilisable par la Cnil (*Décret précité, art. 43 modifié*). À titre de bonne pratique, le G29 recommande également la communication par l'organisme du nom et des coordonnées du DPD à ses employés : sur l'intranet, dans le répertoire téléphonique, ou encore dans les organigrammes de l'organisme.

■ Le DPD doit-il être certifié ?

La certification des compétences du délégué prévue par la délibération n° 2018-318 (*v. encadré*) n'est **pas obligatoire** pour exercer les fonctions de DPD. Inversement, nul besoin d'être DPD pour être candidat à la certification des compétences. La Cnil explique sur son site qu'il s'agit « d'un mécanisme volontaire per-

mettant aux personnes physiques de justifier qu'elles répondent aux exigences de compétences et de savoir-faire du DPD prévues par le règlement ».

La Cnil ne délivrera pas elle-même la certification. Ce sont les organismes certificateurs, lorsqu'ils auront été agréés par la Cnil, qui le feront. Pour être agréés, les organismes doivent respecter un référentiel de la Cnil adopté le 20 septembre 2018 (*Délibération n° 2018-317 du 20 septembre 2018*) et déposer une demande auprès de la commission. Cet agrément n'est obligatoire que pour les organismes qui souhaitent délivrer une certification DPD sur la base du référentiel élaboré par la Cnil. Autrement dit, tout organisme peut certifier des DPD sur la base de son propre référentiel de certification, non approuvé par la Cnil, comme c'est déjà le cas aujourd'hui.

SANCTIONS EN CAS D'ABSENCE DE DÉSIGNATION

L'entreprise est passible, en sa qualité de responsable de traitement, d'une amende administrative pouvant atteindre 10 000 000 € ou 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu (*RGPD, art. 83, § 4, a*).

LISTE DES COMPÉTENCES ET SAVOIR-FAIRE ATTENDUS POUR ÊTRE CERTIFIÉ

Un référentiel de certification de la Cnil adopté le 20 septembre 2018 fixe les conditions attendues pour être certifié en tant que DPO. Pour pouvoir accéder à la phase d'évaluation, le candidat doit (*Délibération n° 2018-318 du 20 septembre 2018, JO du 11 octobre 2018*) :

- **soit** justifier d'une **expérience professionnelle d'au moins deux ans** dans des projets, **activités** ou tâches **en lien** avec les missions du DPO s'agissant de la protection des données personnelles ;
- **soit** justifier d'une **expérience professionnelle d'au moins deux ans** ainsi que d'une **formation d'au moins 35 heures** en matière de **protection des données** personnelles reçue par un organisme de formation.

Pour être certifié en tant que DPO, le **candidat doit savoir** :

- identifier la base juridique d'un traitement ;
- déterminer les mesures appropriées et le contenu de l'information à fournir aux personnes concernées ;
- établir des procédures pour recevoir et gérer les demandes d'exercice des droits des personnes concernées ;
- identifier l'existence de transferts de données hors Union européenne et déterminer les instruments juridiques de transfert susceptibles d'être utilisés ;
- **élaborer** et mettre en œuvre une **politique** ou des règles internes en matière de **protection des données** ;
- **organiser** et participer à des **audits** en matière de protection des données ;
- identifier des mesures de protection des données dès la conception et par défaut adaptées aux risques et à la nature des opérations de traitement ;
- participer à l'identification des mesures de sécurité adaptées aux risques et à la nature des opérations de traitement ;
- **identifier** les **violations de données personnelles** nécessitant une notification à l'autorité de contrôle et celles nécessitant une communication aux personnes concernées ;
- déterminer s'il est nécessaire ou non d'effectuer une AIPD et en vérifier l'exécution ;
- dispenser des **conseils** en matière d'AIPD (en particulier sur la méthodologie, l'éventuelle sous-traitance, les mesures techniques et organisationnelles à adopter) ;
- gérer les relations avec les autorités de contrôle, en répondant à leurs sollicitations et en facilitant leur action (instruction des plaintes et contrôles en particulier).
- élaborer, mettre en œuvre et être en capacité de dispenser des programmes de formation et de sensibilisation du personnel et des instances dirigeantes en matière de protection des données ;
- assurer la traçabilité de ses activités, notamment à l'aide d'outils de suivi ou de bilan annuel.

Il doit également connaître :

- le cadre juridique relatif à la sous-traitance en matière de traitement de données personnelles ;
- le contenu du registre d'activités de traitement, du registre des catégories d'activités de traitement et de la documentation des violations de données ainsi que de la documentation nécessaire pour prouver la conformité à la réglementation en matière de protection des données ;
- les principes de licéité du traitement, de limitation des finalités, de minimisation des données, d'exactitude des données, de conservation limitée des données, d'intégrité, de confidentialité et de responsabilité.

2 Missions

« Chef d'orchestre » de la protection des données au sein de l'entreprise, le DPD est notamment chargé d'informer et de conseiller le responsable de traitement ou le sous-traitant ainsi que leurs employés en matière de protection des données (RGPD, art. 39, § 1, a). Mais ses missions ne se limitent pas à cela.

À NOTER Le G29 recommande, dans ses lignes directrices, que le responsable de traitement décrive clairement, dans le contrat du délégué et dans les informations fournies à l'encadrement et aux employés, le champ d'application et les missions précises du DPD. L'article 39 du RGPD, qui dresse une liste des missions du délégué, n'étant pas exhaustive, rien ne s'oppose, par exemple, à ce que le responsable du traitement ou le sous-traitant confie au DPD la mission de tenir le registre des opérations de traitement effectuées sous leur responsabilité (RGPD, art. 30). Pour le G29, ce registre doit être considéré comme l'un des outils permettant au délégué d'exercer ses missions.

MISSIONS PRINCIPALES

▣ Contrôler le respect du RGPD

Le DPD a la tâche de contrôler le respect du RGPD (RGPD, art. 39, § 1, b). Selon le G29, il peut notamment :

- recueillir des informations permettant de recenser les activités de traitement ;
- analyser et vérifier la conformité des activités de traitement ;
- informer et conseiller le responsable du traitement ou le sous-traitant et formuler des recommandations à son intention.

Attention, souligne le G29 dans ses lignes directrices, cela ne signifie pas que le DPD est personnellement responsable en cas de non-respect du RGPD. Seul le responsable du traitement est tenu de mettre « en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement » (RGPD, art. 24, § 1). Autrement dit, cela signifie que le délégué ne peut pas être sanctionné en cas de non-respect de la protection des données. C'est la responsabilité sociale du responsable du traitement des données qui peut être mise en jeu et non celle du DPD.

LE DPD : QUEL COÛT ?

Si le DPD est interne à l'entreprise, il pourra occuper cette fonction à plein-temps. Il peut néanmoins exécuter d'autres tâches, et si tel est le cas, sa rémunération en qualité de DPD devra s'additionner à la rémunération afférente à ses autres fonctions au sein de la société. Pour le moment, il semble qu'un salaire annuel de DPD va d'environ 35 000 € brut pour les profils juniors, à presque 50 000 € pour les profils avec cinq ans d'expérience en juridique ou en data selon *Les Échos* (17/10/2018).

S'agissant des DPD externes à l'entreprise, plusieurs bureaux de conseil se développent actuellement afin de proposer l'externalisation de service d'un DPD. Si l'entreprise opte pour cette voie, le coût peut varier selon l'ampleur des traitements et le niveau de protection des données et en fonction du secteur d'activité de l'entreprise.

▣ Conseiller l'organisme sur la réalisation d'une analyse d'impact relative à la protection des données (AIPD)

Il incombe au responsable du traitement, et non au DPD, d'effectuer, le cas échéant, une analyse d'impact relative à la protection des données (AIPD). Toutefois, le DPD est chargé de dispenser des conseils, sur demande du responsable de traitement, en ce qui concerne cette analyse. Il est également tenu d'en vérifier la bonne exécution (RGPD, art. 39, § 1, c et *Délibération Cnil n° 2018-326 du 11 octobre 2018, v. « Conditions de réalisation d'une AIPD »*).

Dans ses lignes directrices, le G29 recommande que le responsable de traitement s'enquière notamment auprès du délégué de :

- savoir s'il convient ou non de procéder à une AIPD ;
- la méthodologie à suivre pour réaliser l'analyse d'impact ;
- savoir s'il convient de sous-traiter l'AIPD ou de l'effectuer en interne ;
- quelles mesures (y compris techniques et organisationnelles) appliquer pour atténuer les risques éventuels pour les droits et libertés des personnes concernées ;
- savoir si l'analyse d'impact a été correctement réalisée et si ses conclusions sont conformes au RGPD (opportunité ou non de procéder au traitement et garanties à mettre en place).

Le conseil fourni par le DPD doit ensuite impérativement être formalisé dans l'AIPD (*Délibération n° 2018-326, v. « Conditions de réalisation d'une AIPD »*).

À NOTER Si le responsable de traitement n'est pas du même avis que le DPD, le G29 recommande qu'il justifie par écrit dans l'AIPD de la raison pour laquelle il n'a pas pris l'avis du délégué en considération.

▣ Coopérer avec la Cnil et être son point de contact

Le DPD doit être le point de contact de l'autorité de contrôle et coopérer avec elle. À ce titre, il doit faciliter l'accès de la Cnil aux informations et aux documents dans le cadre de l'exercice de ses pouvoirs et de ses missions (RGPD, art. 39, § 1, d et e), par exemple :

- lors de l'instruction d'une plainte portée devant la Cnil ;
- dans le cadre d'un contrôle effectué par la commission ;
- en cas de besoin de précisions sur un projet en cours.

À NOTER Le délégué est soumis à une obligation de confidentialité concernant l'exercice de ses missions, ou au secret professionnel (RGPD, art. 38, § 5). Mais cela ne lui interdit pas de solliciter les conseils de la Cnil en cas de besoin. Il peut en effet la consulter sur tout autre sujet, si nécessaire (RGPD, art. 39, § 1, e).

EXERCICE DE SES MISSIONS

Le DPD doit avoir une approche sélective et pragmatique des opérations de traitement. Il doit tenir « dûment compte [...] du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement » (RGPD, art. 39, § 2).

Autrement dit, lorsqu'il effectue son travail quotidien, le DPD doit établir des priorités et concentrer ses efforts sur les questions représentant un risque élevé pour les droits et libertés. Cela ne signifie pas qu'il est autorisé à négliger les opérations de traitement présentant un niveau de risque inférieur, mais qu'il doit donner la priorité à celles présentant les risques les

plus élevés. Il doit leur consacrer une part plus importante de ses ressources et de son temps.

MOYENS D'ACTION

Le DPD doit bénéficier du soutien de l'entreprise dans l'exercice de ses missions. Celle-ci doit en particulier (RGPD, art. 38):

- s'assurer à ce que le délégué à la protection des données soit **associé** dans toutes les questions relatives à la protection des données, d'une manière appropriée et en temps utile (par exemple, communication sur sa désignation aux employés et à la Cnil);
- lui fournir les ressources nécessaires à la réalisation de ses tâches (formation, moyens humains et matériels adéquats, temps suffisant, ou encore ressources financières);
- lui permettre d'agir en toute indépendance (v. page 2);
- lui faciliter l'accès aux opérations de traitement et aux données;
- veiller à l'absence de conflit d'intérêts (v. page 2).

3 Responsabilité

La responsabilité du DPD est similaire à celle du CIL. Il n'est pas responsable en cas de non-respect du règlement (v. page 4). La protection des données incombe au responsable de traitement ou au sous-traitant. Elle ne peut pas être transférée au DPD par délégation de pouvoir, puisque « cela reviendrait à conférer au délégué un pouvoir décisionnel sur la finalité et les moyens du traitement ce qui serait constitutif d'un conflit d'intérêts », souligne la Cnil dans ses questions/réponses « Devenir délégué à la protection des données » mis en ligne le 23 mai 2017.

Il existe toutefois des situations dans lesquelles le DPD peut voir sa responsabilité pénale engagée :

- s'il enfreint intentionnellement les dispositions pénales de la loi Informatique et libertés;
- s'il est complice du responsable de traitement ou du sous-traitant ayant enfreint ces dispositions (en d'autres termes, s'il les aide à violer la loi).

4 Protection du DPD salarié

Le délégué interne à l'entreprise doit bénéficier d'une protection suffisante pour pouvoir exercer ses missions. Il ne peut donc pas être sanctionné pour l'exercice de ses missions de DPD. Il pourra, en revanche, être sanctionné sur d'autres fondements.

PAS DE SANCTION POUR L'EXERCICE DE SES MISSIONS DE DPD

Il ne peut être ni relevé de ses fonctions, ni pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions (RGPD, art. 38, § 3). Si le délégué est un salarié de l'entreprise, l'employeur ne peut donc pas le sanctionner dans le cadre de l'exercice de sa mission de DPD. Ainsi, si un délégué estime qu'un traitement est susceptible d'engendrer un risque élevé et qu'il conseille à l'employeur de procéder à une analyse d'impact, l'employeur qui n'est pas d'accord avec cette analyse ne peut pas relever le délégué de sa fonction pour avoir formulé ce conseil.

QUELLES DIFFÉRENCES AVEC LES ANCIENS CIL ?

Les **statuts** du DPD et du CIL sont **similaires**. Pour la Cnil, les DPD sont les successeurs naturels des CIL. Mais ils n'en restent pas moins distincts. D'abord, les **prérequis nécessaires** pour être DPD sont **plus précis** que ce qui était prévu pour les CIL en termes de qualifications (connaissances spécialisées en protection des données, qualités professionnelles, etc.) ou même de formation (entretien relatif aux connaissances spécialisées du DPD).

Ensuite, les **prérogatives et missions** du DPD sont **renforcées**, s'agissant notamment de son rôle de conseil et de sensibilisation relatif aux nouvelles obligations du RGPD (sur l'AIPD par exemple). Et les entreprises doivent lui fournir les moyens d'exercer ses missions : l'associer à toutes les questions relatives à la protection des données d'une manière appropriée et en temps utile, lui donner accès aux données, etc.

Enfin, la désignation du DPD peut être obligatoire, contrairement au CIL dont la désignation est toujours facultative.

Les **sanctions interdites** peuvent prendre des formes **diverses**, et être **directes ou indirectes**. Il peut s'agir :

- d'absence ou retard de promotion;
- de freins à l'avancement de carrière;
- de refus de l'octroi d'avantages dont bénéficient d'autres salariés.

Sans même avoir été jusqu'à mettre en œuvre la sanction, la seule menace de le faire est interdite dès lors que l'employeur la brandit pour des motifs liés aux activités du salarié en tant que DPD (*Lignes directrices du G29, 3.4*).

SANCTIONS AUTORISÉES POUR D'AUTRES MOTIFS

Le DPD pourra toujours être sanctionné (jusqu'à la sanction la plus grave : le licenciement), pour des motifs autres que l'exercice de sa mission de délégué (par exemple, vol, harcèlement). Mais le G29 conseille malgré tout, afin d'anticiper le remplacement du DPD mais aussi de le garantir contre un licenciement abusif, de conclure un contrat stable avec le salarié occupant les fonctions de DPD (*Lignes directrices du G29, point 3.4*).

À NOTER Le DPD n'est pas un salarié protégé au sens de l'article L. 2411-1 du Code du travail. Si son licenciement est envisagé pour des motifs non liés à sa fonction de délégué, la procédure de droit commun s'applique donc. Ni l'avis du comité d'entreprise (ou comité social et économique), ni l'autorisation de l'inspecteur du travail ne sont requis.

SOURCES // • Ord. n° 2018-1125 du 12 décembre 2018, JO 13 décembre, NOR : JUSC1829503R • Délibérations n° 2018-317 et n° 2018-318 du 20 septembre 2018, JO 11 octobre, NOR : CNIL1827455X et CNIL1827457X • D. n° 2018-687 du 1^{er} août 2018, JO 3 août, NOR : JUSC1815709D • Loi n° 2018-493 du 20 juin 2018, JO 21 juin, NOR : JUSC1732261L • Lignes directrices concernant les délégués à la protection des données (DPD) adoptées le 13 décembre 2016, version révisée et adoptée le 5 avril 2017 par le groupe de travail « article 29 » sur la protection des données institué par l'article 29 de la directive 95/46/CE • Règlement (UE) 2016/679 du 27 avril 2016

 CONSULTER LES DOCUMENTS SUR :
liaisons-sociales.fr

VOIR AUSSI

Dossier pratique -Libertés- n° 40/2018 du 28 février 2018
Dossier pratique -Libertés- n° 101/2017 du 2 juin 2017