GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

16/FR
WP 243 rev.01

Lignes directrices concernant les délégués à la protection des données (DPD)

Adoptées le 13 décembre 2016

Version révisée et adoptée le 5 avril 2017

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et état de droit) de la direction générale de la justice et des consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO59 03/068.

Site web: http://ec.europa.eu/justice/data-protection/index_fr.htm

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30 de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LES PRÉSENTES LIGNES DIRECTRICES:

Table des matières

1 Introduction

Le règlement général sur la protection des données (RGPD)[1], qui devrait prendre effet le 25 mai 2018, fournit un cadre de conformité modernisé, fondé sur la responsabilité, en matière de protection des données en Europe. Les délégués à la protection des données (DPD) seront au cœur de ce nouveau cadre juridique pour de nombreux organismes, pour faciliter la conformité avec les dispositions du RGPD.

En vertu du RGPD, certains responsables du traitement et sous-traitants ont l'obligation de désigner un DPD[2]. Cette obligation s'appliquera à l'ensemble des autorités et organismes publics (indépendamment de la nature des données qu'ils traitent), ainsi qu'à d'autres organismes dont les activités de base consistent en un suivi systématique à grande échelle de personnes ou en un traitement à grande échelle de catégories particulières de données à caractère personnel.

Même lorsque le RGPD n'exige pas spécifiquement la désignation d'un DPD, les organismes peuvent parfois juger utile d'en désigner un sur une base volontaire. Le groupe de travail «Article 29» sur la protection des données («G29») encourage ces efforts déployés sur une base volontaire.

La notion de DPD n'est pas nouvelle. Bien que la directive 95/46/CE[3] ne contraigne aucun organisme à désigner un DPD, la pratique consistant à désigner un DPD s'est néanmoins installée dans plusieurs États membres au fil des ans.

Avant l'adoption du RGPD, le G29 avait fait valoir que le DPD était l'une des pierres angulaires du régime de responsabilité et que la désignation d'un DPD pouvait faciliter le respect des règles et, en outre, devenir un avantage concurrentiel pour les entreprises[4]. Outre qu'ils favorisent le respect des règles grâce à la mise en œuvre d'outils de responsabilité (comme la facilitation d'analyses d'impact relatives à la protection des données et la facilitation ou la réalisation d'audits relatifs à la protection des données), les DPD agissent comme intermédiaires entre les acteurs concernés (par exemple, les autorités de contrôle, les personnes concernées et les entités économiques au sein d'un organisme).

---

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016,). Le règlement général présente de l'intérêt pour l'EEE et s'y appliquera après son intégration dans l'accord sur l'EEE.

[2] La désignation d'un DPD est également obligatoire pour les autorités compétentes en vertu de l'article 32 de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89), ainsi que de la législation de transposition nationale. Bien que les présentes lignes directrices portent essentiellement sur les DPD désignés en vertu du RGPD, elles sont également pertinentes pour les DPD désignés en vertu de la directive 2016/680, en ce qui concerne les dispositions similaires des deux actes.

[3] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31).

[4] Voir http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_fr.pdf

Les DPD ne sont pas personnellement responsables en cas de non-respect du RGPD. Ce dernier établit clairement que c'est le responsable du traitement ou le sous-traitant qui est tenu de s'assurer et d'être en mesure de démontrer que le traitement est effectué conformément à ses dispositions (article 24, paragraphe 1). Le respect de la protection des données relève de la responsabilité du responsable du traitement ou du sous-traitant.

Le responsable du traitement ou le sous-traitant jouent également un rôle essentiel pour permettre l'exécution efficace des missions du DPD. La désignation d'un DPD est une première étape, mais celui-ci doit aussi disposer d'une autonomie et de ressources suffisantes pour s'acquitter efficacement de ses missions.

Le RGPD reconnaît le DPD en tant qu'acteur clé dans le nouveau système de gouvernance des données et établit les conditions relatives à sa désignation, à sa fonction et à ses missions. L'objectif des présentes lignes directrices est de préciser les dispositions pertinentes du RGPD afin d'aider les responsables du traitement et les sous-traitants à respecter la législation, mais aussi d'assister les DPD dans leur rôle. Les présentes lignes directrices formulent également des recommandations en matière de bonnes pratiques, en s'appuyant sur l'expérience acquise dans certains États membres de l'Union. Le G29 assurera le suivi de la mise en œuvre des présentes lignes directrices et pourrait les compléter avec des précisions supplémentaires si nécessaire.

2 Désignation d'un DPD

2.1. Désignation obligatoire

L'article 37, paragraphe 1, du RGPD requiert la désignation d'un DPD dans trois cas spécifiques[5]:

a) lorsque le traitement est effectué par une autorité publique ou un organisme public[6];
b) lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou
c) lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données[7] ou[8] de données à caractère personnel relatives à des condamnations pénales et à des infractions[9].

Dans les points ci-après, le G29 donne des orientations en ce qui concerne les critères et la terminologie figurant à l'article 37, paragraphe 1.

[5] Il est à noter que, conformément à l'article 37, paragraphe 4, le droit de l'Union ou des États membres peut exiger la désignation de DPD dans d'autres situations également.
[6] À l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle. Voir article 32 de la directive (UE) 2016/680.
[7] Conformément à l'article 9, ces catégories incluent les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale; est également visé le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.
[8] L'article 37, paragraphe 1, point c), utilise le terme «*et*». Voir le point 2.1.5 ci-dessous pour des explications concernant l'utilisation du terme «*ou*» au lieu du terme «*et*».
[9] Article 10.

À moins qu'il soit évident qu'un organisme n'est pas tenu de désigner un DPD, le G29 recommande que les responsables du traitement et les sous-traitants documentent l'analyse interne effectuée afin de déterminer si, oui ou non, il y a lieu de désigner un DPD, afin qu'ils soient en mesure de démontrer que les facteurs pertinents ont été correctement pris en considération[10]. Cette analyse fait partie de la documentation requise au titre du principe de responsabilité. Elle peut être exigée par l'autorité de contrôle et doit être tenue à jour le cas échéant, par exemple si les responsables du traitement ou les sous-traitants exercent de nouvelles activités ou s'ils proposent de nouveaux services susceptibles de correspondre aux cas énumérés à l'article 37, paragraphe 1.

Lorsqu'un organisme désigne un DPD sur une base volontaire, les conditions prévues aux articles 37 à 39 s'appliquent à la désignation, à la fonction et aux missions de celui-ci comme si la désignation avait été obligatoire.

Rien n'empêche un organisme qui n'est pas tenu légalement de désigner un DPD et ne souhaite pas en désigner sur une base volontaire d'employer du personnel ou des consultants extérieurs chargés de missions liées à la protection des données à caractère personnel. En pareil cas, il importe de veiller à ce qu'il n'y ait pas de confusion quant à leur titre, leur statut, leur fonction et leurs missions. Ainsi, il convient d'indiquer clairement, dans toute communication au sein de l'entreprise ainsi qu'avec les autorités chargées de la protection des données, les personnes concernées et le public au sens large, que cette personne ou ce consultant ne porte pas le titre de délégué à la protection des données (DPD).[11]

Le DPD, que sa désignation soit obligatoire ou volontaire, est désigné pour toutes les opérations de traitement effectuées par le responsable du traitement ou le sous-traitant.

2.1.1 «UNE AUTORITE PUBLIQUE OU UN ORGANISME PUBLIC»

Le RGPD ne définit pas ce qu'il convient d'entendre par «*une autorité publique ou un organisme public*». Le G29 considère que cette notion doit être définie en fonction du droit national. En conséquence, les autorités publiques et les organismes publics incluent les autorités nationales, régionales et locales, mais, au regard des législations nationales applicables, cette notion englobe aussi généralement une série d'autres organismes de droit public[12]. En pareils cas, la désignation d'un DPD est obligatoire.

Les autorités publiques et les organismes publics ne sont pas les seuls à pouvoir effectuer des missions de service public ou exercer l'autorité publique[13]; d'autres personnes physiques ou morales de droit public ou privé peuvent également le faire, dans des domaines variant en fonction de la réglementation nationale de chaque État membre, tels que les services de transports publics, l'approvisionnement en eau et en énergie, les infrastructures routières, la radiodiffusion publique, le logement social ou les organes disciplinaires pour les professions réglementées.

Dans ces cas, les personnes concernées peuvent se trouver dans une situation très similaire à celle dans laquelle leurs données sont traitées par une autorité publique ou un organisme public. En particulier,

[10] Voir l'article 24, paragraphe 1.

[11] Cela vaut également pour les responsables de la protection de la vie privée (*chief privacy officers*) ou les autres professionnels chargés des questions de confidentialité qui sont déjà employés dans certaines entreprises et qui, s'ils ne respectent pas les critères établis par le RGPD, notamment pour ce qui est des ressources disponibles ou des garanties d'indépendance, ne peuvent être considérés ni désignés comme DPD.

les données peuvent être traitées à des fins similaires, et les particuliers n'ont souvent guère ou pas le choix quant au traitement même des données les concernant ou aux modalités de ce traitement et peuvent donc requérir la protection supplémentaire que peut apporter la désignation d'un DPD.

Bien qu'il n'y ait pas d'obligation dans ce cas, le G29 recommande, à titre de bonne pratique, que les organismes privés chargés d'effectuer des missions de service public ou exerçant l'autorité publique désignent un DPD. Les activités de ce DPD couvrent l'ensemble des opérations de traitement effectuées, y compris celles qui ne sont pas liées à la réalisation d'une mission de service public ou à l'exercice d'une charge officielle (par exemple, la gestion d'une base de données des employés).

2.1.2 «ACTIVITES DE BASE»

L'article 37, paragraphe 1, points b) et c), du RGPD fait référence aux «*activités de base du responsable du traitement ou du sous-traitant*». Le considérant 97 précise que «*les activités de base d'un responsable du traitement ont trait à ses activités principales et ne concernent pas le traitement des données à caractère personnel en tant qu'activité auxiliaire*». Les «activités de base» peuvent être considérées comme les opérations essentielles nécessaires pour atteindre les objectifs du responsable du traitement ou du sous-traitant.

Toutefois, les «activités de base» ne doivent pas être interprétées comme excluant les activités pour lesquelles le traitement de données fait partie intégrante de l'activité du responsable du traitement ou du sous-traitant. Par exemple, l'activité de base d'un hôpital est de fournir des soins de santé. Toutefois, un hôpital ne peut fournir de soins de santé de manière sûre et efficace sans traiter des données concernant la santé, telles que les dossiers médicaux des patients. Par conséquent, le traitement de ces données doit être considéré comme l'une des activités de base de tout hôpital, et les hôpitaux doivent donc désigner un DPD.

On peut aussi citer l'exemple d'une société de sécurité privée qui assure la surveillance d'un certain nombre de centres commerciaux privés et d'espaces publics. L'activité de base de la société est la surveillance, qui est elle-même indissociablement liée au traitement de données à caractère personnel. Par conséquent, cette société doit également désigner un DPD.

En revanche, tous les organismes exercent certaines activités comme la rémunération de leurs employés ou les activités d'assistance informatique classiques. Ces activités constituent des exemples de fonctions de soutien nécessaires à l'activité de base ou principale de l'organisme. Bien que ces activités soient nécessaires ou essentielles, elles sont généralement considérées comme des fonctions auxiliaires plutôt que comme l'activité de base.

2.1.3 «À GRANDE ECHELLE»

L'article 37, paragraphe 1, points b) et c), exige que le traitement des données à caractère personnel soit effectué à grande échelle pour que la désignation d'un DPD soit obligatoire. Si le RGPD ne définit

[12] Voir, par exemple, les définitions de l'«*organisme du secteur public*» et de l'«*organisme de droit public*» énoncées respectivement à l'article 2, point 1), et à l'article 2, point 2), de la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public (JO L 345 du 31.12.2003, p. 90).

[13] Article 6, paragraphe 1, point e).

pas la notion de traitement à «grande échelle», le considérant 91 fournit toutefois certaines orientations[14].

En effet, il n'est pas possible de donner un chiffre précis, que ce soit pour la quantité de données traitées ou le nombre d'individus concernés, qui soit applicable dans toutes les situations. Cela n'exclut toutefois pas la possibilité qu'au fil du temps, une pratique courante puisse émerger, permettant de déterminer en des termes plus spécifiques ou quantitatifs ce qui constitue un traitement «*à grande échelle*» pour certains types d'activités de traitement courantes. Le G29 prévoit également de contribuer à cette évolution, en partageant et faisant connaître des exemples de seuils pertinents pour la désignation d'un DPD.

En tout état de cause, le G29 recommande que les facteurs suivants, en particulier, soient pris en considération pour déterminer si le traitement est mis en œuvre à grande échelle:

- le nombre de personnes concernées, soit en valeur absolue, soit en valeur relative par rapport à la population concernée;
- le volume de données et/ou le spectre des données traitées;
- la durée, ou la permanence, des activités de traitement des données;
- l'étendue géographique de l'activité de traitement.

[14] Selon ce considérant, les «*opérations de traitement à grande échelle qui visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées et qui sont susceptibles d'engendrer un risque élevé*» devraient être incluses en particulier. Par ailleurs, le considérant indique spécifiquement que le «*traitement de données à caractère personnel ne devrait pas être considéré comme étant à grande échelle si le traitement concerne les données à caractère personnel de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel*». Il importe de souligner que, si le considérant donne des exemples extrêmes dans un sens comme dans l'autre (le traitement par un médecin exerçant à titre individuel par rapport au traitement des données d'un pays entier ou dans l'ensemble de l'Europe), il existe une large zone grise entre ces deux extrêmes. En outre, il convient de garder à l'esprit que ce considérant concerne les analyses d'impact relatives à la protection des données, ce qui signifie que certains éléments pourraient être spécifiques à ce contexte et ne pas nécessairement s'appliquer exactement de la même manière à la désignation de DPD.

Exemples de traitement à grande échelle:

- traitement des données de patients par un hôpital dans le cadre du déroulement normal de ses activités;
- traitement des données de voyage des passagers utilisant un moyen de transport public urbain (par exemple, suivi par les titres de transport);
- traitement des données de géolocalisation en temps réel des clients d'une chaîne internationale de restauration rapide à des fins statistiques par un sous-traitant spécialisé dans la fourniture de ces services;
- traitement des données de clients par une compagnie d'assurance ou une banque dans le cadre du déroulement normal de ses activités;
- traitement des données à caractère personnel par un moteur de recherche à des fins de publicité comportementale;
- traitement des données (contenu, trafic, localisation) par des fournisseurs de services de téléphonie ou internet.

Exemples ne constituant pas un traitement à grande échelle:

- traitement, par un médecin exerçant à titre individuel, des données de ses patients;
- traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions par un avocat exerçant à titre individuel.

2.1.4 «SUIVI REGULIER ET SYSTEMATIQUE»

La notion de suivi régulier et systématique des personnes concernées n'est pas définie dans le RGPD, mais celle de «*suivi du comportement des personnes concernées*» est mentionnée au considérant 24[15] et inclut clairement toutes les formes de suivi et de profilage sur l'internet, y compris à des fins de publicité comportementale.

Toutefois, la notion de suivi n'est pas limitée à l'environnement en ligne et le suivi en ligne ne doit être considéré que comme un exemple de suivi du comportement des personnes concernées[16].

Le G29 interprète le terme «régulier» comme recouvrant une ou plusieurs des significations suivantes:

- continu ou se produisant à intervalles réguliers au cours d'une période donnée;
- récurrent ou se répétant à des moments fixes;
- ayant lieu de manière constante ou périodique.

Le G29 interprète le terme «systématique» comme recouvrant une ou plusieurs des significations suivantes:

[15] *«Afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit.»*

[16] Il est à noter que le considérant 24 porte en particulier sur l'application extraterritoriale du RGPD. En outre, il existe également une différence entre l'expression «*le suivi du comportement de ces personnes*» [article 3, paragraphe 2, point b)], et l'expression «*un suivi régulier et systématique [...] des personnes concernées*» [article 37, paragraphe 1, point b)], qui pourrait donc être considéré comme une notion différente.

- se produisant conformément à un système;
- préétabli, organisé ou méthodique;
- ayant lieu dans le cadre d'un programme général de collecte de données;
- effectué dans le cadre d'une stratégie.

Exemples d'activités pouvant constituer un suivi régulier et systématique des personnes concernées: exploitation d'un réseau de télécommunications; fourniture de services de télécommunications; reciblage par courrier électronique; activités de marketing fondées sur les données; profilage et notation à des fins d'évaluation des risques (par exemple, aux fins de l'évaluation du risque de crédit, de l'établissement des primes d'assurance, de la prévention de la fraude ou de la détection du blanchiment d'argent); géolocalisation, par exemple, par des applications mobiles; programmes de fidélité; publicité comportementale; surveillance des données sur le bien-être, la santé et la condition physique au moyen de dispositifs portables; systèmes de télévision en circuit fermé; dispositifs connectés tels que les voitures et compteurs intelligents, la domotique, etc.

2.1.5 CATEGORIES PARTICULIERES DE DONNEES ET DONNEES RELATIVES A DES CONDAMNATIONS PENALES ET A DES INFRACTIONS

L'article 37, paragraphe 1, point c), concerne le traitement de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10. Bien que cette disposition utilise le terme «et», il n'existe aucune raison de principe qui voudrait que les deux critères doivent être appliqués simultanément. Il convient donc de lire le texte comme voulant dire «ou».

2.2. DPD du sous-traitant

L'article 37 s'applique à la fois aux responsables du traitement[17] et aux sous-traitants[18] en ce qui concerne la désignation d'un DPD. En fonction de la personne qui remplit les critères de désignation obligatoire, dans certains cas, seul le responsable du traitement ou le sous-traitant est tenu de désigner un DPD, dans d'autres, le responsable de traitement et le sous-traitant sont tenus de désigner chacun un DPD (les deux DPD devant alors collaborer entre eux).

Il est important de souligner que, même si le responsable du traitement remplit les critères de désignation obligatoire, son sous-traitant n'est pas nécessairement tenu de désigner un DPD. Il peut toutefois s'agir d'une bonne pratique.

Exemples:

- Une petite entreprise familiale active dans le secteur de la distribution d'appareils électroménagers dans une seule ville recourt aux services d'un sous-traitant dont l'activité de base consiste à fournir des services d'analyse de sites internet et d'assistance à la publicité et

[17] Le responsable du traitement est défini à l'article 4, point 7), comme la personne ou l'organisme qui détermine les finalités et les moyens du traitement.

[18] Le sous-traitant est défini à l'article 4, point 8), comme la personne ou l'organisme qui traite des données pour le compte du responsable du traitement.

au marketing ciblés. Les activités de l'entreprise familiale et ses clients n'entraînent pas de traitement de données à «grande échelle», compte tenu du faible nombre de clients et des activités relativement limitées. Toutefois, prises globalement, les activités du sous-traitant, qui dispose d'un grand nombre de clients comme cette petite entreprise, consistent en un traitement à grande échelle. Le sous-traitant doit donc désigner un DPD en vertu de l'article 37, paragraphe 1, point b), tandis que l'entreprise familiale elle-même n'est pas soumise à l'obligation de désigner un DPD.

- Une entreprise de taille moyenne spécialisée dans la fabrication de carrelage sous-traite ses services de médecine du travail à un sous-traitant externe, qui dispose d'un grand nombre de clients similaires. Le sous-traitant doit désigner un DPD en vertu de l'article 37, paragraphe 1, point c), dans la mesure où le traitement s'effectue à grande échelle. En revanche, le fabricant n'est pas nécessairement tenu de désigner un DPD.

Le DPD désigné par un sous-traitant supervise également les activités menées par l'organisme sous-traitant lorsque celui-ci agit lui-même en qualité de responsable du traitement (par exemple, ressources humaines, informatique, logistique).

2.3. Désignation d'un DPD unique pour plusieurs organismes

L'article 37, paragraphe 2, autorise un groupe d'entreprises à désigner un seul DPD à condition qu'il soit «*facilement joignable à partir de chaque lieu d'établissement*». La notion de joignabilité renvoie aux missions du DPD en tant que point de contact pour les personnes concernées[19], pour l'autorité de contrôle[20], mais également en interne au sein de l'organisme, compte tenu du fait que l'une des missions du DPD consiste à «*informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement*»[21].

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 conformément aux exigences du RGPD[22].

Il doit être en mesure, avec l'aide d'une équipe si nécessaire, de communiquer efficacement avec les personnes concernées[23] et de coopérer[24] avec les autorités de contrôle compétentes, ce qui implique

[19] Article 38, paragraphe 4: «*Les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le présent règlement*».

[20] Article 39, paragraphe 1, point e): «*faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet*».

[21] Article 39, paragraphe 1, point a).

[22] Voir à cet égard le point 2.6 ci-dessous.

[23] Article 12, paragraphe 1: *«Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant».*

[24] Article 39, paragraphe 1, point d): *«coopérer avec l'autorité de contrôle».*

également 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 employés 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.

En vertu de l'article 37, paragraphe 3, un seul délégué à la protection des données peut être désigné pour plusieurs autorités publiques ou organismes publics, compte tenu de leur structure organisationnelle et de leur taille. Les mêmes considérations en matière de ressources et de communication s'appliquent. Étant donné que le DPD est chargé d'une série de missions, le responsable du traitement ou le sous-traitant doit s'assurer qu'un seul DPD peut, avec l'aide d'une équipe si nécessaire, s'acquitter efficacement de ces missions en dépit du fait qu'il soit désigné par plusieurs autorités publiques et organismes publics.

2.4. Joignabilité et localisation du DPD

Conformément à la section 4 du RGPD, la joignabilité du DPD doit être effective.

Afin de garantir que le DPD soit joignable, le G29 recommande que celui-ci se trouve dans l'Union européenne, que le responsable du traitement ou le sous-traitant soit ou non établi dans l'Union.

Toutefois, il ne peut être exclu que, dans certaines situations où le responsable du traitement ou le sous-traitant ne possède pas d'établissement dans l'Union européenne[25], le DPD puisse mener ses activités de manière plus efficace s'il se trouve en dehors de l'Union.

2.5. Expertise et compétences du DPD

L'article 37, paragraphe 5, dispose que le DPD «*est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39*». Le considérant 97 indique que le niveau de connaissances spécialisées requis devrait être déterminé en fonction des opérations de traitement de données effectuées et de la protection exigée pour les données à caractère personnel traitées.

- **Niveau d'expertise**

Le niveau d'expertise requis n'est pas strictement défini, mais il doit être proportionné à la sensibilité, à la complexité et au volume des données traitées par un organisme. Par exemple, lorsqu'une opération de traitement de données est particulièrement complexe, ou lorsqu'une grande quantité de données sensibles est concernée, il est possible que le DPD doive disposer d'un niveau plus élevé d'expertise et de soutien. Il existe également une différence selon que l'organisme transfère systématiquement des données à caractère personnel hors de l'Union européenne ou, au contraire, que les transferts de ce

[25] Voir l'article 3 du RGPD concernant le champ d'application territorial.

type sont occasionnels. Il convient donc de choisir le DPD soigneusement, en prenant dûment en considération les questions relatives à la protection des données qui se posent au sein de l'organisme.

- **Qualités professionnelles**

Bien que l'article 37, paragraphe 5, ne précise pas les qualités professionnelles à prendre en considération lors de la désignation du DPD, il est nécessaire que les DPD disposent d'une expertise dans le domaine des législations et pratiques nationales et européennes en matière de protection des données, ainsi que d'une connaissance approfondie du RGPD. Il est également utile que les autorités de contrôle encouragent la formation adéquate et régulière des DPD.

La connaissance du secteur d'activité et de l'organisme du responsable du traitement est utile. Le DPD devrait également disposer d'une bonne compréhension des opérations de traitement effectuées, ainsi que des systèmes d'information et des besoins du responsable du traitement en matière de protection et de sécurité des données.

Dans le cas d'une autorité publique ou d'un organisme public, le DPD devrait également avoir une bonne connaissance des règles et procédures administratives de l'organisme.

- **Aptitude à exercer ses missions**

L'aptitude à exercer les missions qui incombent au DPD doit être interprétée tant au regard des qualités personnelles et connaissances du DPD que de sa fonction au sein de l'organisme. Parmi les qualités personnelles figurent par exemple l'intégrité et un haut niveau de déontologie; la préoccupation première du DPD doit être de permettre le respect du RGPD. Le DPD joue un rôle clé dans la promotion d'une culture de la protection des données au sein de l'organisme et contribue à mettre en œuvre des éléments essentiels du RGPD, tels que les principes relatifs au traitement des données[26], les droits des personnes concernées[27], la protection des données dès la conception et la protection des données par défaut[28], le registre des activités de traitement[29], la sécurité du traitement[30] ainsi que la notification et la communication des violations de données[31].

- **DPD sur la base d'un contrat de service**

La fonction du DPD peut aussi être exercée sur la base d'un contrat de service conclu avec une personne ou un organisme indépendant de l'organisme du responsable du traitement ou du sous-traitant. Dans ce cas, il est essentiel que chaque membre de l'organisme exerçant les fonctions de DPD remplisse l'ensemble des exigences applicables établies à la section 4 du RGPD (par exemple, il est essentiel qu'aucun des membres de l'organisme n'ait de conflit d'intérêts). Il est tout aussi important que chaque membre soit protégé par les dispositions du RGPD (par exemple, pas de résiliation abusive du contrat de service pour les activités de DPD pas plus que de licenciement abusif d'un membre de l'organisme exerçant les missions du DPD). Dans le même temps, les compétences et les atouts

[26] Chapitre II.
[27] Chapitre III.
[28] Article 25.
[29] Article 30.
[30] Article 32.
[31] Articles 33 et 34.

individuels peuvent être combinés de sorte que plusieurs personnes, travaillant en équipe, puissent mieux servir leurs clients.

Dans un souci de clarté juridique et de bonne organisation, et afin d'éviter les conflits d'intérêts pour les membres de l'équipe, il est recommandé de prévoir une répartition claire des tâches au sein de l'équipe chargée de la fonction de DPD et de désigner, pour chaque client, une seule personne comme personne de contact principale «responsable» de ce client. En règle générale, il serait également utile de préciser ces points dans le contrat de service.

2.6. Publication et communication des coordonnées du DPD

L'article 37, paragraphe 7, du RGPD dispose que le responsable du traitement ou le sous-traitant:

- publie les coordonnées du DPD et
- communique ces coordonnées à l'autorité de contrôle compétente.

Ces exigences visent à garantir que les personnes concernées (tant à l'intérieur qu'à l'extérieur de l'organisme) et les autorités de contrôle puissent aisément et directement prendre contact avec le DPD sans devoir s'adresser à un autre service de l'organisme. La confidentialité est également un aspect important: les employés pourraient par exemple hésiter à se plaindre auprès du DPD si la confidentialité de leurs communications n'est pas garantie
Le DPD est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions, conformément au droit de l'Union ou au droit des États membres (article 38, paragraphe 5).

Les coordonnées du DPD doivent contenir des informations permettant aux personnes concernées et aux autorités de contrôle de joindre celui-ci facilement (une adresse postale, un numéro de téléphone spécifique et/ou une adresse de courrier électronique spécifique). Le cas échéant, aux fins de la communication avec le public, d'autres moyens de communication pourraient également être prévus, par exemple, une assistance par téléphone spécifique, ou un formulaire de contact spécifique adressé au DPD sur le site web de l'organisme.

L'article 37, paragraphe 7, n'exige pas que les coordonnées publiées incluent le nom du DPD. Si la publication du nom du DPD peut constituer une bonne pratique, il appartient au responsable du traitement, ou au sous-traitant, et au DPD de décider si elle est nécessaire ou utile dans les circonstances particulières du cas considéré[32].

Toutefois, la communication du nom du DPD à l'autorité de contrôle est essentielle pour que le DPD puisse faire office de point de contact entre l'organisme et l'autorité de contrôle [article 39, paragraphe 1, point e)].

À titre de bonne pratique, le G29 recommande également que tout organisme communique le nom et les coordonnées du DPD à ses employés. Par exemple, le nom et les coordonnées du DPD pourraient

[32] Il est à noter qu'à la différence de l'article 37, paragraphe 7, l'article 33, paragraphe 3, point b), qui décrit les informations à communiquer à l'autorité de contrôle et à la personne concernée en cas de violation de données à caractère personnel, exige explicitement la communication du nom du DPD (et pas uniquement de ses coordonnées).

être publiés en interne sur l'intranet, dans le répertoire téléphonique et dans les organigrammes de l'organisme.

3 Fonction du DPD

3.1. Association du DPD à toutes les questions relatives à la protection des données à caractère personnel

L'article 38 du RGPD dispose que le responsable du traitement et le sous-traitant doivent veiller à ce que le DPD «*soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel*».

Il est essentiel que le DPD, ou son équipe, soit associé dès le stade le plus précoce possible à toutes les questions relatives à la protection des données. En ce qui concerne les analyses d'impact relatives à la protection des données, le RGPD prévoit expressément la participation du DPD à un stade précoce et précise que le responsable du traitement doit demander conseil au DPD lorsqu'il effectue une analyse de ce type[33]. L'information et la consultation du DPD dès le début permettront de faciliter le respect du RGPD et d'encourager une approche fondée sur la protection des données dès la conception; il devrait donc s'agir d'une procédure habituelle au sein de la gouvernance de l'organisme. En outre, il importe que le DPD soit considéré comme un interlocuteur au sein de l'organisme et qu'il soit membre des groupes de travail consacrés aux activités de traitement de données au sein de l'organisme.

Par conséquent, l'organisme devrait veiller, par exemple, à ce que:

- le DPD soit invité à participer régulièrement aux réunions de l'encadrement supérieur et intermédiaire;
- sa présence soit recommandée lorsque des décisions ayant des implications en matière de protection des données sont prises. Toutes les informations pertinentes doivent être transmises au DPD en temps utile afin de lui permettre de fournir un avis adéquat;
- l'avis du DPD soit toujours dûment pris en considération. En cas de désaccord, le G29 recommande, à titre de bonne pratique, de consigner les raisons pour lesquelles l'avis du DPD n'a pas été suivi;
- le DPD soit immédiatement consulté lorsqu'une violation de données ou un autre incident se produit.

Le cas échéant, le responsable du traitement ou le sous-traitant pourrait élaborer des lignes directrices ou des programmes en matière de protection des données indiquant les cas dans lesquels le DPD doit être consulté.

[33] Article 35, paragraphe 2.

3.2. Ressources nécessaires

L'article 38, paragraphe 2, du RGPD exige que l'organisme aide son DPD *en fournissant les ressources nécessaires pour exercer [ses] missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées*. Les aspects suivants, en particulier, doivent être pris en considération:

- soutien actif de la fonction du DPD par l'encadrement supérieur (par exemple, au niveau du conseil d'administration);
- 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;
- soutien adéquat du point de vue des ressources financières, des infrastructures (locaux, installations, équipements) et du personnel, le cas échéant;
- communication officielle de la désignation du DPD à l'ensemble du personnel afin de veiller à ce que l'existence et la fonction de celui-ci soient connues au sein de l'organisme;
- 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;
- formation continue. Les DPD doivent avoir la possibilité de maintenir leurs connaissances à jour en ce qui concerne les évolutions dans le domaine de la protection des données. L'objectif devrait être d'augmenter constamment le niveau d'expertise des DPD et ceux-ci devraient être encouragés à participer à des cours de formation sur la protection des données ainsi qu'à d'autres formes de développement professionnel, telles que la participation à des forums sur la protection de la vie privée, des ateliers, etc.;
- compte tenu de la taille et de la structure de l'organisme, il est possible qu'il faille mettre en place une équipe de DPD (un DPD et son personnel). En pareils cas, la structure interne de l'équipe ainsi que les tâches et responsabilités de chacun de ses membres doivent être clairement établies. De même, lorsque la fonction du DPD est exercée par un prestataire de services externe, une équipe de personnes travaillant pour le compte de cette entité peut exercer, dans les faits, les missions du DPD en tant que groupe, sous la responsabilité d'une personne de contact principale désignée pour le client.

D'une manière générale, plus les opérations de traitement sont complexes ou sensibles, plus les ressources octroyées au DPD devront être importantes. La fonction de protection des données doit être effective et dotée de ressources adéquates au regard du traitement de données réalisé.

3.3. Instructions et exercice de «leurs fonctions et missions en toute indépendance»

L'article 38, paragraphe 3, prévoit certaines garanties de base destinées à faire en sorte que les DPD soient en mesure d'exercer leurs missions avec un degré suffisant d'autonomie au sein de leur

organisme. En particulier, les responsables du traitement/sous-traitants doivent veiller à ce que le DPD «*ne reçoive aucune instruction en ce qui concerne l'exercice des missions*». Le considérant 97 indique en outre que les DPD, «*qu'ils soient ou non des employés du responsable du traitement, devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance*».

Cela signifie que, dans l'exercice de leurs missions au titre de l'article 39, les DPD ne doivent pas recevoir d'instructions sur la façon de 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. En outre, ils ne peuvent être tenus d'adopter un certain point de vue sur une question liée à la législation en matière de protection des données, par exemple, une interprétation particulière du droit.

L'autonomie des DPD ne signifie cependant pas qu'ils disposent de pouvoirs de décision allant au-delà des missions leur incombant conformément à l'article 39.

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[34]. Si le responsable du traitement ou le sous-traitant prend des décisions qui sont incompatibles avec le RGPD et l'avis du DPD, ce dernier devrait avoir la possibilité d'indiquer clairement son avis divergent au niveau le plus élevé de la direction et aux décideurs. À cet égard, l'article 38, paragraphe 3, dispose que le DPD «*fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant*». Une telle reddition de compte directe garantit que l'encadrement supérieur (par ex., le conseil d'administration) a connaissance des avis et recommandations du DPD qui s'inscrivent dans le cadre de la mission de ce dernier consistant à informer et à conseiller le responsable du traitement ou le sous-traitant. L'élaboration d'un rapport annuel sur les activités du DPD destiné au niveau le plus élevé de la direction constitue un autre exemple de reddition de compte directe.

3.4. Licenciement ou sanction pour l'exercice des missions du DPD

L'article 38, paragraphe 3, dispose que le DPD ne devrait pas être «*relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions*».

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.

Le RGPD n'interdit les sanctions que si elles sont imposées au DPD à la suite de l'exercice de ses missions de DPD. Par exemple, si un DPD considère qu'un traitement particulier est susceptible d'engendrer un risque élevé et conseille au responsable du traitement ou au sous-traitant de procéder à une analyse d'impact relative à la protection des données, mais que le responsable du traitement ou le sous-traitant n'est pas d'accord avec l'évaluation du DPD, ce dernier ne peut être relevé de ses fonctions pour avoir formulé cet avis.

Les sanctions peuvent prendre des formes diverses et peuvent être directes ou indirectes. Il peut s'agir, par exemple, d'absence de promotion ou de retard dans la promotion, de freins à l'avancement de carrière ou du refus de l'octroi d'avantages dont bénéficient d'autres travailleurs. Il n'est pas

[34] Article 5, paragraphe 2.

nécessaire que ces sanctions soient effectivement mises en œuvre, une simple menace suffit pour autant qu'elle soit utilisée pour sanctionner le DPD pour des motifs liés à ses activités de DPD.

Dans le cadre d'une gestion normale, et comme c'est le cas pour tout autre employé ou sous-traitant conformément au droit des contrats ou au droit du travail et au droit pénal applicables au niveau national, et selon les conditions qui y sont fixées, un DPD pourra toujours être licencié légitimement pour des motifs autres que l'exercice de ses missions de DPD (par exemple, en cas de vol, de harcèlement physique, moral ou sexuel ou d'autres fautes graves similaires).

Dans ce contexte, il convient de noter que le RGPD ne précise pas comment et quand un DPD peut être licencié ou remplacé par une autre personne. Toutefois, plus le contrat d'un DPD est stable et plus il existe de garanties contre le licenciement abusif, plus il est probable que le DPD pourra agir en toute indépendance. Par conséquent, le G29 encourage les efforts déployés par les organismes à cet effet.

3.5. Conflits d'intérêts

L'article 38, paragraphe 6, autorise les DPD à «*exécuter d'autres missions et tâches*». Il exige toutefois que l'organisme veille à ce que «*ces missions et tâches n'entraînent pas de conflit d'intérêts*».

L'absence de conflit d'intérêts est étroitement liée à l'obligation d'agir en toute indépendance. Bien que les DPD soient autorisés à exercer d'autres fonctions, un DPD ne peut se voir confier d'autres missions et tâches qu'à condition que celles-ci ne donnent pas lieu à un conflit d'intérêts. Cela signifie en particulier que le DPD ne peut exercer au sein de l'organisme une fonction qui l'amène à déterminer les finalités et les moyens du traitement de données à caractère personnel. En raison de la structure organisationnelle spécifique de chaque organisme, cet aspect doit être étudié au cas par cas.

En règle générale, parmi les fonctions susceptibles de donner lieu à un conflit d'intérêts au sein de l'organisme peuvent figurer les fonctions d'encadrement supérieur (par exemple, directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique), mais aussi d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement. En outre, il peut également y avoir conflit d'intérêts, par exemple, si un DPD externe est appelé à représenter le responsable du traitement ou le sous-traitant devant les tribunaux dans des affaires ayant trait à des questions liées à la protection des données.

En fonction des activités, de la taille et de la structure de l'organisme, il peut être de bonne pratique pour les responsables du traitement ou les sous-traitants:

- de recenser les fonctions qui seraient incompatibles avec celle de DPD;
- d'établir des règles internes à cet effet, afin d'éviter les conflits d'intérêts;
- d'inclure une explication plus générale concernant les conflits d'intérêts;
- de déclarer que leur 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;
- de 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. Dans ce contexte, il convient également de garder à l'esprit que les conflits d'intérêts peuvent prendre différentes formes selon que le DPD est recruté en interne ou à l'extérieur.

4 Missions du DPD

4.1. Contrôle du respect du RGPD

L'article 39, paragraphe 1, point b), confie au DPD, entre autres missions, la tâche de contrôler le respect du RGPD. Le considérant 97 précise en outre que le DPD «*devrait aider le responsable du traitement ou le sous-traitant à vérifier le respect, au niveau interne, du présent règlement*».

Dans le cadre de ces tâches de contrôle du respect du RGPD, les DPD peuvent 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.

Le contrôle du respect du RGPD ne signifie pas que le DPD est personnellement responsable en cas de non-respect de celui-ci. Le RGPD établit clairement que c'est le responsable du traitement, et non le DPD, qui 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*» (article 24, paragraphe 1). Le respect de la protection des données relève de la responsabilité sociale du responsable du traitement des données, et non du DPD.

4.2. Rôle du DPD dans les analyses d'impact relatives à la protection des données

Conformément à l'article 35, paragraphe 1, il incombe au responsable du traitement, et non au DPD, d'effectuer, si nécessaire, une analyse d'impact relative à la protection des données. Toutefois, le DPD peut jouer un rôle d'assistance du responsable du traitement très important et très utile. Conformément au principe de protection des données dès la conception, l'article 35, paragraphe 2, exige expressément que le responsable du traitement «*demande conseil*» au DPD lorsqu'il réalise une analyse d'impact relative à la protection des données. L'article 39, paragraphe 1, point c), donne pour sa part mission au DPD de «*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*».

Le G29 recommande que le responsable du traitement demande conseil au DPD sur les questions suivantes notamment[35]:

- la question de savoir s'il convient ou non de procéder à une analyse d'impact relative à la protection des données;
- la méthodologie à suivre lors de la réalisation d'une analyse d'impact relative à la protection des données;

[35] L'article 39, paragraphe 1, énumère les missions du DPD et indique que ces missions sont «*au moins*» les suivantes. Par conséquent, rien ne s'oppose à ce que le responsable du traitement confie au DPD des missions autres que celles qui sont expressément mentionnées à l'article 39, paragraphe 1, ou précise ces missions de manière plus détaillée.

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

Si le responsable du traitement est en désaccord avec l'avis fourni par le DPD, la documentation de l'analyse d'impact relative à la protection des données devrait expressément justifier, par écrit, la raison pour laquelle l'avis n'a pas été pris en considération[36]

Le G29 recommande en outre que le responsable du traitement décrive clairement, par exemple dans le contrat du DPD, mais aussi dans les informations fournies aux employés et à l'encadrement (ainsi qu'à d'autres parties prenantes, le cas échéant), les missions précises du DPD et leur champ d'application, notamment en ce qui concerne la réalisation des analyses d'impact relatives à la protection des données.

4.3. Coopérer avec l'autorité de contrôle et faire office de point de contact

Conformément à l'article 39, paragraphe 1, points d) et e), le DPD devrait: «*coopérer avec l'autorité de contrôle*» et «*faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet*».

Ces missions ont trait au rôle de «facilitateur» du DPD mentionné dans l'introduction des présentes lignes directrices. Le DPD fait office de point de contact pour faciliter l'accès de l'autorité de contrôle aux documents et informations nécessaires à l'exécution des missions mentionnées à l'article 57, ainsi qu'à l'exercice de ses pouvoirs d'enquête, de ses pouvoirs d'adopter des mesures correctrices, de ses pouvoirs d'autorisation et de ses pouvoirs consultatifs visés à l'article 58. Comme cela a déjà été mentionné, le DPD est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions, conformément au droit de l'Union ou au droit des États membres (article 38, paragraphe 5). Toutefois, l'obligation de secret professionnel/confidentialité n'interdit pas au DPD de prendre contact avec l'autorité de contrôle pour solliciter son avis. L'article 39, paragraphe 1, point e), dispose que le DPD peut mener des consultations auprès de l'autorité de contrôle sur tout autre sujet, le cas échéant.

[36] L'article 24, paragraphe 1, dispose que, «*[c]ompte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met 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. Ces mesures sont réexaminées et actualisées si nécessaire*».

4.4. Approche fondée sur les risques

L'article 39, paragraphe 2, requiert que le DPD tienne «*dûment compte [...] du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement*».

Cet article rappelle un principe général de bon sens, qui peut s'appliquer à de nombreux aspects du travail quotidien d'un DPD. En substance, il exige des DPD qu'ils établissent des priorités dans leurs activités et concentrent leurs efforts sur les questions qui représentent un risque élevé en matière de protection des données. Cela ne signifie pas qu'ils doivent négliger la vérification de la conformité des opérations de traitement présentant un niveau de risque inférieur, mais plutôt qu'ils doivent se concentrer, en premier lieu, sur les secteurs présentant un risque élevé.

Cette approche sélective et pragmatique devrait aider les DPD à conseiller le responsable du traitement sur la méthode à utiliser lors de la réalisation d'une analyse d'impact sur la protection des données, sur les domaines qui devraient être soumis à un audit interne ou externe en matière de protection des données, sur les activités de formation à proposer au personnel ou aux membres de l'encadrement responsables des activités de traitement des données et sur les opérations de traitement auxquelles il devrait consacrer une part plus importante de son temps et de ses ressources.

4.5. Rôle du DPD dans la tenue du registre

En vertu de l'article 30, paragraphes 1 et 2, c'est le responsable du traitement ou le sous-traitant, et non le DPD, qui doit tenir «*un registre des activités de traitement effectuées sous [sa] responsabilité*» ou «*un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement*».

Dans la pratique, les DPD dressent souvent des inventaires et tiennent un registre des opérations de traitement sur la base des informations qui leur ont été fournies par les différents services dans leur organisme responsables du traitement de données à caractère personnel. Cette pratique a été inscrite dans de nombreuses législations nationales ainsi que dans les règles en matière de protection des données applicables aux institutions et organes de l'Union européenne[37].

L'article 39, paragraphe 1, établit une liste des missions que le DPD doit au moins se voir confier. Par conséquent, rien ne s'oppose 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 la responsabilité du responsable du traitement ou du sous-traitant. Ce registre doit être considéré comme l'un des outils permettant au DPD d'exercer ses missions de contrôle du respect du RGPD ainsi que d'information et de conseil du responsable du traitement ou du sous-traitant.

En tout état de cause, le registre qui doit être tenu au titre de l'article 30 doit aussi être considéré comme un outil permettant au responsable du traitement et à l'autorité de contrôle de disposer, sur demande, d'une vue d'ensemble de toutes les activités de traitement de données à caractère personnel effectuées par un organisme. Il s'agit donc d'une condition préalable nécessaire au respect du RGPD et, à ce titre, d'une mesure de responsabilisation efficace.

[37] Article 24, paragraphe 1, point d), du règlement (CE) nº 45/2001.

5 ANNEXE – LIGNES DIRECTRICES CONCERNANT LES DPD: CE QU'IL FAUT SAVOIR

L'objectif de la présente annexe est de répondre, dans un format simplifié et facile à lire, à certaines des principales questions que peuvent se poser les organismes au sujet des nouvelles exigences prévues par le règlement général sur la protection des données (RGPD) en matière de désignation d'un DPD.

Désignation du DPD

1 Quels sont les organismes tenus de désigner un DPD

La désignation d'un DPD est obligatoire:

- si le traitement est effectué par une autorité publique ou un organisme public, quelles que soient les données qui sont traitées;
- si les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui exigent un suivi régulier et systématique à grande échelle des personnes concernées;
- si les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données ou de données à caractère personnel relatives à des condamnations pénales et à des infractions.

Il est à noter que le droit de l'Union ou des États membres peut exiger la désignation de DPD dans d'autres situations également. Enfin, même si la désignation d'un DPD n'est pas obligatoire, les organismes peuvent parfois estimer utile d'en désigner un sur une base volontaire. Le groupe de travail «Article 29» sur la protection des données («G29») encourage ces efforts déployés sur une base volontaire. Lorsqu'un organisme désigne un DPD sur une base volontaire, les mêmes conditions s'appliquent à la désignation, à la fonction et aux missions de celui-ci que si la désignation avait été obligatoire.

Sources: article 37, paragraphe 1, du RGPD

2 Qu'entend-on par «activités de base»?

Les «activités de base» peuvent être considérées comme les opérations essentielles pour atteindre les objectifs du responsable du traitement ou du sous-traitant. Elles comprennent également toutes les activités pour lesquelles le traitement de données fait partie intégrante de l'activité du responsable du traitement ou du sous-traitant. Par exemple, le traitement des données concernant la santé telles que les dossiers médicaux des patients doit être considéré comme l'une des activités de base des hôpitaux, et ces derniers doivent donc désigner un DPD.

En revanche, tous les organismes exercent certaines activités de soutien comme la rémunération de leurs employés ou les activités d'assistance informatique classiques. Ces activités constituent des exemples de fonctions de soutien nécessaires à l'activité de base ou principale de l'organisme. Bien que ces activités soient nécessaires ou essentielles, elles sont généralement considérées comme des fonctions auxiliaires plutôt que comme l'activité de base.

Sources: article 37, paragraphe 1, points b) et c), du RGPD

3 Qu'entend-on par «à grande échelle»?

Le RGPD ne définit pas la notion de traitement «à grande échelle». Le G29 recommande que les facteurs suivants, en particulier, soient pris en considération pour déterminer si le traitement est mis en œuvre à grande échelle:

- le nombre de personnes concernées, soit en valeur absolue, soit en valeur relative par rapport à la population concernée;
- le volume de données et/ou le spectre des données traitées;
- la durée, ou la permanence, des activités de traitement des données;
- l'étendue géographique de l'activité de traitement.

Exemples de traitement à grande échelle:

- traitement des données de patients par un hôpital dans le cadre du déroulement normal de ses activités;
- traitement des données de voyage des passagers utilisant un moyen de transport public urbain (par exemple, suivi par les titres de transport);
- traitement des données de géolocalisation en temps réel des clients d'une chaîne internationale de restauration rapide à des fins statistiques par un sous-traitant spécialisé dans ces activités;
- traitement des données de clients par une compagnie d'assurance ou une banque dans le cadre du déroulement normal de ses activités;
- traitement des données à caractère personnel par un moteur de recherche à des fins de publicité comportementale;
- traitement des données (contenu, trafic, localisation) par des fournisseurs de services de téléphonie ou internet.

Exemples ne constituant pas un traitement à grande échelle:

- traitement, par un médecin exerçant à titre individuel, des données de ses patients;
- traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions par un avocat exerçant à titre individuel.

Sources: article 37, paragraphe 1, points b) et c), du RGPD

4 Qu'entend-on par «suivi régulier et systématique»

La notion de suivi régulier et systématique des personnes concernées n'est pas définie dans le RGPD, mais inclut clairement toutes les formes de suivi et de profilage sur l'internet, y compris à des fins de publicité comportementale. La notion de suivi ne se limite toutefois pas à l'environnement en ligne.

Exemples d'activités pouvant constituer un suivi régulier et systématique des personnes concernées: exploitation d'un réseau de télécommunications; fourniture de services de télécommunications; reciblage par courrier électronique; activités de marketing fondées sur les données; profilage et notation à des fins d'évaluation des risques (par exemple, aux fins de l'évaluation du risque de crédit, de l'établissement des primes d'assurance, de la prévention de la fraude ou de la détection du blanchiment d'argent); géolocalisation, par exemple, par des applications mobiles; programmes de fidélité; publicité comportementale; surveillance des données sur le bien-être, la santé et la condition physique au moyen de dispositifs portables; systèmes de télévision en circuit fermé; dispositifs connectés tels que les voitures et compteurs intelligents, la domotique, etc.

Le G29 interprète le terme «régulier» comme recouvrant une ou plusieurs des significations suivantes:

- continu ou se produisant à intervalles réguliers au cours d'une période donnée;
- récurrent ou se répétant à des moments fixes;
- ayant lieu de manière constante ou périodique.

Le G29 interprète le terme «systématique» comme recouvrant une ou plusieurs des significations suivantes:

- se produisant conformément à un système;
- préétabli, organisé ou méthodique;
- ayant lieu dans le cadre d'un programme général de collecte de données;
- effectué dans le cadre d'une stratégie.

Sources: article 37, paragraphe 1, point b), du RGPD

5 Des organismes peuvent-ils désigner un DPD conjointement? Dans l'affirmative, à quelles conditions?

Oui. Un groupe d'entreprises peut désigner un seul DPD à condition qu'il soit «*facilement joignable à partir de chaque lieu d'établissement*». La notion de joignabilité renvoie aux missions du DPD en tant que point de contact pour les personnes concernées, pour l'autorité de contrôle et également en interne au sein de l'organisme. 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 DPD, 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 employés 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.

Un seul délégué à la protection des données peut être désigné pour plusieurs autorités publiques ou organismes publics, compte tenu de leur structure organisationnelle et de leur taille. Les mêmes considérations en matière de ressources et de communication s'appliquent. Étant donné que le DPD est chargé d'une série de missions, le responsable du traitement ou le sous-traitant doit s'assurer qu'un seul DPD peut, avec l'aide d'une équipe si nécessaire, s'acquitter efficacement de ces missions en dépit du fait qu'il soit désigné par plusieurs autorités publiques et organismes publics.

Sources: article 37, paragraphes 2 et 3, du RGPD

6 Où le DPD doit-il se trouver?

Afin de garantir que le DPD soit joignable, le G29 recommande que celui-ci se trouve dans l'Union européenne, que le responsable du traitement ou le sous-traitant soit ou non établi dans l'Union. Toutefois, il ne peut être exclu que, dans certaines situations où le responsable du traitement ou le sous-traitant ne possède pas d'établissement dans l'Union européenne, le DPD puisse mener ses activités de manière plus efficace s'il se trouve en dehors de l'Union.

7 Est-il possible de désigner un DPD externe?

Oui. Le DPD peut être un membre du personnel du responsable du traitement ou du sous-traitant (DPD interne) ou exercer ses missions sur la base d'un contrat de service, ce qui signifie que le DPD peut être une personne externe et, dans ce cas, sa fonction peut être exercée sur la base d'un contrat de service conclu avec une personne ou un organisme.

Lorsque la fonction du DPD est exercée par un prestataire de services externe, une équipe de personnes travaillant pour le compte de cette entité peut, dans les faits, exercer les missions du DPD 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'organisme externe exerçant les fonctions de DPD remplisse l'ensemble des exigences applicables établies dans le RGPD.

Dans un souci de clarté juridique et de bonne organisation, et afin de prévenir les conflits d'intérêts pour les membres de l'équipe, les lignes directrices recommandent 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 comme personne de contact principale «responsable» du client.

Sources: article 37, paragraphe 6, du RGPD

8 Quelles sont les qualités professionnelles que le DPD doit posséder?

Le DPD est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir ses missions.

Le niveau de connaissances spécialisées requis devrait être déterminé en fonction des opérations de traitement de données effectuées et de la protection exigée pour les données à caractère personnel traitées. Par exemple, lorsqu'une opération de traitement de données est particulièrement complexe, ou lorsqu'une grande quantité de données sensibles est concernée, il est possible que le DPD doive disposer d'un niveau plus élevé d'expertise et de soutien.

Les compétences et l'expertise nécessaires sont notamment les suivantes:

- expertise relative aux législations nationale et européenne en matière de protection des données, y compris une connaissance approfondie du RGPD;
- compréhension des opérations de traitement effectuées;
- compréhension des technologies de l'information et de la sécurité des données;
- connaissance du secteur d'activité et de l'organisme;
- capacité à promouvoir une culture de protection des données au sein de l'organisme.

Sources: article 37, paragraphe 5, du RGPD

9 Quelles ressources le responsable du traitement ou le sous-traitant doit-il mettre à la disposition du DPD?

Le DPD doit disposer des ressources nécessaires à l'exécution de ses missions.

En fonction de la nature des opérations et activités de traitement et de la taille de l'organisme, les ressources suivantes devraient être fournies au DPD:

- soutien actif de la fonction du DPD par l'encadrement supérieur;
- temps suffisant pour que les DPD puissent accomplir leurs missions;
- soutien adéquat du point de vue des ressources financières, des infrastructures (locaux, installations, équipements) et du personnel, le cas échéant;
- communication officielle de la désignation du DPD à l'ensemble du personnel;
- accès à d'autres services au sein de l'organisme de manière à ce que les DPD puissent recevoir le soutien, les contributions et les informations essentiels de ces autres services;
- formation continue.

Sources: article 38, paragraphe 2, du RGPD

10 Quelles sont les garanties permettant au DPD d'exercer ses missions en toute indépendance? Qu'entend-on par «conflit d'intérêts»?

Il existe plusieurs garanties permettant au DPD d'agir en toute indépendance:

- absence d'instruction de la part des responsables du traitement ou des sous-traitants en ce qui concerne l'exercice des missions du DPD;
- interdiction pour le responsable du traitement de licencier ou de sanctionner le DPD pour l'exercice de ses missions;
- absence de conflit d'intérêts avec d'autres missions et tâches possibles.

Les autres missions et tâches d'un DPD ne doivent pas donner lieu à un conflit d'intérêts. Cela signifie tout d'abord que le DPD ne peut exercer au sein de l'organisme une fonction qui l'amène à déterminer les finalités et les moyens du traitement de données à caractère personnel. En raison de la structure organisationnelle spécifique de chaque organisme, cet aspect doit être étudié au cas par cas.

En règle générale, parmi les fonctions susceptibles de donner lieu à un conflit d'intérêts au sein de l'organisme peuvent figurer les fonctions d'encadrement supérieur (par exemple, directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique), mais aussi d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement. En outre, il peut également y avoir conflit d'intérêts, par exemple, si un DPD externe est appelé à représenter le responsable du traitement ou le sous-traitant devant les tribunaux dans des affaires ayant trait à des questions liées à la protection des données.

Sources: article 38, paragraphes 3 et 6, du RGPD

Missions du DPD

11 Qu'entend-on par «surveillance du respect des règles»?

Dans le cadre de ces tâches de contrôle du respect du RGPD, les DPD peuvent 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.

Sources: article 39, paragraphe 1, point b), du RGPD

12 Le DPD est-il personnellement responsable en cas de non-respect des exigences en matière de protection des données?

Non, le DPD n'est pas personnellement responsable en cas de non-respect des exigences en matière de protection des données. C'est le responsable du traitement ou le sous-traitant qui est tenu de s'assurer et doit être en mesure de démontrer que le traitement est effectué conformément au RGPD. Le respect de la protection des données relève de la responsabilité du responsable du traitement ou du sous-traitant.

13 Quel est le rôle du DPD en ce qui concerne l'analyse d'impact relative à la protection des données et le registre des activités de traitement?

En ce qui concerne l'analyse d'impact relative à la protection des données, le responsable du traitement ou le sous-traitant devrait solliciter l'avis du DPD sur les questions suivantes notamment:

- la question de savoir s'il convient ou non de procéder à une analyse d'impact relative à la protection des données;
- la méthodologie à suivre lors de la réalisation d'une analyse d'impact relative à la protection des données;
- la question de savoir s'il convient d'effectuer l'analyse d'impact relative à la protection des données en interne ou de la sous-traiter;
- les mesures (y compris des mesures techniques et organisationnelles) à appliquer pour atténuer les risques éventuels pesant sur les droits et les intérêts des personnes concernées;
- la question de savoir si l'analyse d'impact relative à la protection des données a été correctement réalisée et si ses conclusions (opportunité ou non de procéder au traitement et garanties à mettre en place) sont conformes aux exigences en matière de protection des données.

En ce qui concerne le registre des activités de traitement, c'est le responsable du traitement ou le sous-traitant, et non le DPD, qui est tenu de tenir un registre de ces opérations. Toutefois, rien ne s'oppose 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 la responsabilité du responsable du traitement ou du sous-traitant. Ce registre doit être considéré comme l'un des outils permettant au DPD d'exercer ses missions de contrôle du respect des règles ainsi que d'information et de conseil du responsable du traitement ou du sous-traitant.

Sources: article 39, paragraphe 1, point c), et article 30 du RGPD

Fait à Bruxelles, le 13 décembre 2016

Pour le groupe de travail,
La présidente

Isabelle FALQUE-PIERROTIN

Version révisée et adoptée le 5 avril 2017

Pour le groupe de travail
La présidente

Isabelle FALQUE-PIERROTIN