ANNEXE WP 243 – QUESTIONS FRÉQUEMMENT POSÉES

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 organisations au sujet des nouvelles exigences au titre du règlement général sur la protection des données (RGPD) pour désigner un délégué à la protection des données (DPD).

Désignation du DPD (article 37)

1 Quelles organisations sont tenues de désigner un DPD (article 37, paragraphe 1)?

Le RGPD requiert la désignation d'un DPD dans trois cas spécifiques:

- lorsque le traitement est effectué par une autorité publique ou un organisme public, quelles que soient les données qui sont traitées;
- 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; et
- 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 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, si le RGPD n'exige pas spécifiquement la désignation d'un DPD, les organisations peuvent parfois juger utile d'en désigner un sur une base volontaire. Le groupe de travail «Article 29» sur la protection des données («GT 29») encourage ces efforts déployés sur une base volontaire.

Pour de plus amples informations, voir le point 2.1 des lignes directrices.

2 Que signifie l'expression «activités de base» [article 37, paragraphe 1, points b) et c)]?

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 principales des hôpitaux, et ces derniers doivent donc désigner un DPD.

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

Pour de plus amples informations, voir la section 2.1.2 des lignes directrices.

3 Que signifie l'expression «à grande échelle» [article 37, paragraphe 1, points b) et c)]?

Le RGPD ne définit pas la notion de «grande échelle». Le GT 29 recommande que les facteurs suivants, en particulier, soient pris en considération pour déterminer si le traitement s'opère 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 sur les 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 sur les 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 aux 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 sur ses patients;
- traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions par un avocat exerçant à titre individuel.

Pour de plus amples informations, voir la section 2.1.3 des lignes directrices.

4 Que signifie l'expression «suivi régulier et systématique» [article 37, paragraphe 1, point b)]?

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.

Le GT 29 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 GT 29 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.

Exemples: exploitation d'un réseau de télécommunications; fourniture de services de télécommunications; reciblage par courrier électronique; 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.

Pour de plus amples informations, voir la section 2.1.4 des lignes directrices.

5 Des organisations peuvent-elles désigner un DPD conjointement? Dans l'affirmative, à quelles conditions? (article 37, paragraphes 2 et 3)

Le RGPD prévoit qu'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'organisation. 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 au RGPD. Le DPD 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 personnelle 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.

Pour de plus amples informations, voir le point 2.3 des lignes directrices.

6 Est-il possible de désigner un DPD externe (article 37, paragraphe 6)?

Oui. En vertu de l'article 37, paragraphe 6, 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 une organisation.

Si le DPD est un DPD externe, toutes les exigences visées aux articles 37 à 39 s'appliquent à celui-ci. Comme indiqué dans les lignes directrices, 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'organisation 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, 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.

Pour de plus amples informations, voir les sections 2.3, 2.4 et 3.5 des lignes directrices.

7 Quelles sont les qualités professionnelles que le DPD doit posséder (article 37, paragraphe 5)?

Conformément au RGPD, 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 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 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'organisation;
- capacité à promouvoir une culture de protection des données au sein de l'organisation.

Pour de plus amples informations, voir le point 2.4 des lignes directrices.

Fonction du DPD (article 38)

8 Quelles ressources devraient être fournies au DPD pour l'exercice de ses missions?

L'article 38, paragraphe 2, du RGPD exige que l'organisation 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*.

En fonction de la nature des opérations et activités de traitement et de la taille de l'organisation, 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 tâches;
- 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'organisation de manière à ce que les DPD puissent recevoir le soutien, les contributions et les informations essentiels de ces autres services;
- formation continue.

Pour de plus amples informations, voir le point 3.2 des lignes directrices.

9 Quelles sont les garanties permettant au DPD d'exercer ses missions en toute indépendance (article 38, paragraphe 3)?

Il existe plusieurs garanties permettant au DPD d'agir en toute indépendance comme indiqué au considérant 97:

- 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.

Pour de plus amples informations, voir les points 3.3 à 3.5 des lignes directrices.

10 Quelles sont les «autres missions et tâches» d'un DPD susceptibles de donner lieu à un conflit d'intérêts (article 38, paragraphe 6)?

Le DPD ne peut exercer au sein de l'organisation 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 organisation, cet aspect doit être étudié au cas par cas.

En règle générale, parmi les fonctions susceptibles de donner lieu à un conflit d'intérêts 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.

Pour de plus amples informations, voir le point 3.5 des lignes directrices.

Missions du DPD (article 39)

11 Que comprend la notion de «contrôler le respect» du RGPD (article 39, paragraphe 1)?

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; et
- informer et conseiller le responsable du traitement ou le sous-traitant et formuler des recommandations à son intention.

Pour de plus amples informations, voir le point 4.1 des lignes directrices.

12 Le DPD est-il personnellement responsable en cas de non-respect du RGPD?

Non, le DPD n'est pas personnellement responsable 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 doit être en mesure de démontrer que le traitement est effectué conformément à ce règlement (article 24, paragraphe 1). 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 [article 37, paragraphe 1, point c)] et le registre des activités de traitement (article 30)?

En ce qui concerne l'analyse d'impact relative à la protection des données, le responsable du traitement ou le sous-traitant devrait demander conseil au 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 au RGPD.

Pour de plus amples informations, voir le point 4.2 des lignes directrices.

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. 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.

Pour de plus amples informations, voir le point 4.4 des lignes directrices.