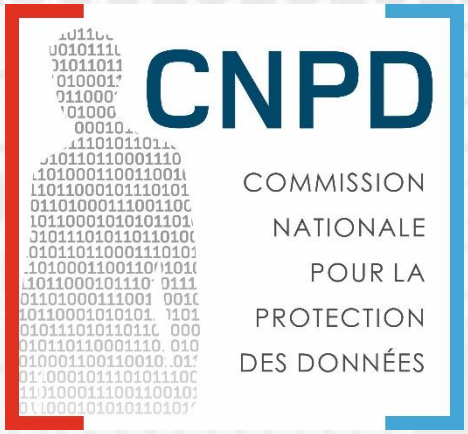
Séances d'information

Règlement général sur la protection des données

Le rôle du futur délégué à la protection des données (DPD)



18 octobre 2017

Esch-sur-Alzette (Belval)

Thierry Lallemang

Membre effectif

I. Les lignes directrices du G29 sur le DPD

1. La designation du DPD

1.1 Désignation obligatoire d'un DPD

1.2 Désignation volontaire d'un DPD dans toutes les autres situations

1.3 DPD mutualisé

1.4 Le profil du DPD: competences et expertise exigées

1.5 DPD interne ou externe

2. La fonction du DPD

3. Les missions du DPD

II. La transition entre le " chargé de la protection des données" sous la loi du 2 août 2002 et le délégué à la protection des données (DPD) sous le RGPD

1. Au niveau de sa designation

2. Au niveau de sa fonction

3. Au niveau de ses missions

I. Les lignes directrices du G29

- Le G29 (regroupe toutes les autorités de contrôle européennes) a adopté en date du 5 avril 2017 des lignes directrices sur le délégué à la protection des données (DPD) dans son document de travail WP 243 .

- Ces lignes directrices se concentrent sur 3 points:

  - **La désignation du DPD (art. 37 RGDP)**

  - **La fonction du DPD (art. 38 RGDP)**

  - **Les tâches du DPD (art. 39 RGDP)**

I. Lignes directrices du G 29
1. La désignation du DPD (art. 37)

1.1 Désignation obligatoire d'un DPD

Désignation obligatoire dans **3 hypothèses** (art. 37(1)) :

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

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

c) les **activités de base** du RT ou du ST consistent en un traitement à **grande échelle** de **catégories particulières de données** visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales ou à des infractions visées à l'article 10;

L'article 37 s'applique aussi bien au responsable du traitement (**RT**) qu'au sous-traitant (**ST**).

1. La désignation du DPD

- **a) autorités ou organismes publics**

  Notion d'autorité publique ou d'organisme public → pas de définition dans RGPD → se référer au droit national.

  Certaines missions de service public peuvent être réalisées par des organismes n'ayant pas un statut public. Il est recommandé que ces organismes désignent aussi un DPD

1. La désignation du DPD

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

Notion **« activités de base »**: L'obligation de désignation d'un DPD est analysée au regard des **traitements de données « clés »**, effectués par le RT ou le ST, **nécessaires pour** réaliser les objectifs de son **activité principale**

→ les **éléments inextricables** de l'activité du RT/ST

*Ex.: Les activités de base d'une banque impliquent des traitements de données financières de ses clients. La banque doit aussi traiter des données RH de ses employés, mais c'est une **activité accessoire**.*

1. La désignation du DPD

Notion de **« grande échelle »** n'est pas non plus définie par le règlement. Il appartient au RT/ST d'effectuer cette analyse sur base de critères tels que:

- Le nombre de personnes concernées (nombre spécifique ou proportion d'une population)
- Le volume des données traitées
- La durée ou permanence des traitements de données
- L'étendue géographique

Ex.:

– *traitement des données des patients par un hôpital (contrairement au traitement de données des patients par un médecin individuel);*

– *traitement de données clients par une assurance ou une banque;*

– *traitement de données (contenu, trafic, localisation) utilisateurs par un fournisseur de services de communications électroniques;*

1. La désignation du DPD

Notion **« suivi systématique et régulier »** n'est pas définie; elle inclut sans aucun doute toutes formes de surveillance, traçage et de profilage sur internet, mais n'est pas limitée à un environnement en ligne.

Une collecte de données est systématique lorsqu'elle est méthodiquement organisée, préétablie ou fait partie d'une stratégie de collecte.

Elle est régulière lorsqu'il y a une certaine répétition, périodicité, constance, permanence dans la mise en œuvre du traitement.

Ex.: Une banque qui doit régulièrement et systématiquement suivre l'évolution des comptes et des transactions de ses clients notamment dans le cadre de ses obligations liées à la prévention de la fraude, du blanchiment d'argent ou du financement du terrorisme.

1. La désignation du DPD

c) les **activités de base** du RT ou du ST consistent en un traitement à **grande échelle** de **catégories particulières de données** visées à l'article 9 ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10;

p.m. catégories particulières de données:

- données qui révèlent l'origine raciale ou ethnique, les convictions religieuses ou philosophiques ou l'appartenance syndicale;
- données concernant la santé ou la vie sexuelle ou l'orientation sexuelle;
- données génétiques;
- données biométriques;
- données relatives aux condamnations pénales ou aux infractions;

Ex.: Un hôpital traitant des données de santé et génétiques

1. La désignation du DPD

- Sauf s'il est évident que la désignation d'un DPD n'est pas nécessaire, il est recommandé que le RT/ST documente son analyse effectuée pour déterminer si un DPD doit ou non être désigné.

- La désignation obligatoire d'un DPD auprès d'un RT n'engendre pas nécessairement une obligation de désigner un DPD auprès du ST et vice versa. Les critères doivent être analysés individuellement au cas par cas pour chaque RT et ST.

Exemple: Une petite entreprise familiale régionale, active dans la distribution d'appareils électroménagers a recours à un ST dont l'activité principale consiste à fournir des services d'analyses de sites internet et d'assistance en matière de marketing et de publicité ciblée. Vu le nombre limité de clients et l'activité relativement limitée de l'entreprises familiale, celle-ci n'effectue pas un traitement de données à grande échelle. Or, le ST, ayant un nombre important de clients, effectue des traitements de données à grande échelle et doit de ce fait désigner un DPD, tandis que l'entreprise familiale n'en est pas obligée.

1. La désignation du DPD

1.2 Désignation volontaire d'un DPD dans toutes les autres situations

Toujours possible de désigner volontairement un DPD. Dans ce cas, les exigences légales (art. 37-39) s'appliquent à sa désignation, sa fonction et ses missions comme si sa désignation avait été obligatoire. Il n'y a donc **aucune différence de statut entre un DPD** désigné de manière **obligatoire ou volontaire**.

1.3 DPD mutualisé

- Un **groupe d'entreprises** ou **plusieurs autorités ou organismes publics** peuvent désigner un **seul DPD** à condition qu'il soit **facilement joignable à partir de chaque lieu d'établissement**. (art. 37(2))

  Cette notion d'**accessibilité** doit être lue en relation avec les missions d'un DPD, dans le sens qu'il est à la fois le point de contact pour les personnes concernées, l'autorité de contrôle, mais aussi en interne, alors qu'il a, entre autres, comme mission d'informer et de conseiller le RT et le ST ainsi que les salariés.

- Pour assurer qu'un DPD interne ou externe, soit effectivement et facilement joignable, il faut que les **coordonnées de contact du DPD** (adresse postale, numéro de téléphone dédié et adresse e-mail dédiée *(dpd@nomdelasociete.lu)*) soient disponibles càd que le RT/ST doit les rendre publiques et les communiquer à l'autorité de contrôle (art. 37(7)).

  - **!!! Il n'est pas obligatoire de publier le nom d'un DPD**

1. La désignation du DPD

1.4 Le profil du DPD: compétences et expertise exigées

- Le DPD doit être désigné sur la base de ses **qualités professionnelles** et, **en particulier**, de ses **connaissances spécialisées du droit et des pratiques en matière de protection des données**, et de sa **capacité à accomplir ses missions** (art. 37(5)).
- Le **niveau de connaissance** n'est pas défini, mais il doit être en rapport avec la sensibilité, la complexité et le volume de données traitées par le RT/ST.
- Les compétences et l'expertise nécessaires devraient notamment inclure:
  - *Connaissances approfondies de la législation nationale et européenne en matière de protection des données*
  - *Connaissance des opérations de traitement effectué par le RT/ST*
  - *Connaissances dans le domaine des systèmes d'information et de la sécurité des données*
  - *Connaissance du secteur d'activité et de l'organisme lui-même*
  - *Capacité à promouvoir une culture de la protection des données au sein de l'organisme*
- **Le DPD ne sera pas agréé par la CNPD**

1. La désignation du DPD

1.5 DPD interne ou externe

- La fonction de DPD peut être exercée par un **salarié** (**DPD interne**) ou par une **personne physique ou morale externe** (**DPD externe**) sur base d'un contrat de service (art. 37(6)). Toutes les exigences des articles 37 à 39 s'appliquent aussi au DPD externe.

- Lorsque la fonction de DPD est exercée par un prestataire externe, une **équipe de personnes** travaillant pour ce dernier, qui doivent toutes remplir les conditions et exigences du RGPD (p.ex. ne pas avoir un conflit d'intérêts), peut accomplir les missions de DPD en équipe. Toutes ces personnes bénéficient bien entendu des dispositions du RGPD qui protègent le DPD.

- Dans un souci de sécurité juridique, il est recommandé que le contrat de service indique clairement la répartition des tâches au sein de l'équipe DPD externe et désigne une personne de contact principale (« lead ») en charge et responsable pour le client.

2. La fonction du DPD (art. 38)

- Le RT/ST doit veiller à ce que le **DPD soit impliqué dès le début** à toutes les questions relatives à la protection des données (art. 38(1)). L'avis du DPD devrait donc être intégré dès la phase de conception des traitements de données (principes de protection des données dès la conception et par défaut) et en particulier pour le DPIA. Pour ce faire le RT/ST devrait garantir p.ex. que:
  - Le DPD est invité à participer régulièrement aux réunions des instances dirigeantes de l'organisation
  - Sa présence est recommandé chaque fois que des décisions en relation avec la protection des données doivent être prises
  - L'avis du DPD soit toujours pris en compte; en cas de désaccord entre le direction et le DPD, il est de bonne pratique de documenter les raisons pour ne pas suivre l'avis du DPD
  - Le DPD soit rapidement consulté en cas de violation de données
- **Bonne pratique**: l'élaboration de lignes directrices internes déterminant quand le DPD doit être consulté

2. La fonction du DPD

- L'article 38(2) exige que le RT/ST aide le DPD en lui fournissant les **ressources nécessaires** pour effectuer ses missions.

- A ce titre, et en fonction de la nature des traitements de données, de l'activité et de la taille du RT/ST, celui-ci devra, notamment, fournir au DPD les ressources suivantes:
  - Appui actif de la fonction de DPD par la direction
  - Soutien adéquat en termes de temps nécessaire, de ressources financières, d'infrastructures et de personnel, au besoin
  - Communication officielle de la désignation du DPD à l'ensemble du personnel (données de contact, y compris le nom)
  - Accès aux données et opérations de traitement de tous les services/départements au sein du RT/ST
  - Formation continue

2. La fonction du DPD

- L'article 38(3) prévoit des garanties pour que le DPD puisse et efficacement exercer sa fonction. Ainsi, il doit pouvoir agir en toute **indépendance** sans recevoir d'instruction par le RT/ST, **ni être licencié ou pénalisé** (directement ou indirectement) à cause de sa fonction ou de son activité. Il fait directement **rapport au niveau le plus élevé de la direction**. Il est soumis au **secret professionnel** ou à une obligation de confidentialité.

  Ex: Licenciement en cas de désaccord entre la direction et le DPD quant à la nécessité d'effectuer un DPIA; absence ou retard dans l'avancement dans sa carrière.

- Corollaire de son indépendance, les autres tâches éventuelles du DPD ne doivent pas engendrer des **conflits d'intérêts** avec la fonction de DPD (art. 38(6)). En particulier, il ne doit pas être dans une position qui lui permet de déterminer les moyens et les finalités des traitements de données (éviter d'être « juge et partie »). Doit être apprécié au cas par cas.

  Ex.: Fonctions qui peuvent être considérées comme incompatibles avec la fonction de DPD: toutes les fonctions dirigeantes telles que directeur général, chef de l'exploitation, chef des finances, médecin-chef, responsable du département marketing, responsable du département informatique, responsable des RH, etc… ou est aussi incompatible l'activité de sous-traitant et de DPD (externe) pour un même RT

3. Les missions du DPD (art. 39)

- Le DPD a comme **tâches principales** de:
  - Informer et conseiller le RT/ST et l'ensemble du personnel sur les questions liées à la protection des données
  - Contrôler le respect des dispositions du RGPD par le RT/ST
  - Conseiller le RT/ST dans le cadre d'un DPIA et en vérifier son exécution
  - Prendre en compte dans ses conseils et analyses les risques plus ou moins élevés liés aux traitements de données
  - Coopérer avec l'autorité de contrôle et faire office de point de contact

    → rôle de facilitateur p.r. à CNPD

- Il appartient au RT/ST de tenir un « registre des activités de traitement » et non au DPD; or, il est évident que ce dernier doit être étroitement associé à ce travail de cartographie des traitements de données.

- En tout état de cause, le **RT/ST reste toujours responsable** de la conformité au règlement. Cette responsabilité **ne peut en aucun cas être transférée** au DPD.

II. La transition entre le **chargé** de la protection des données et le **délégué** à la protection des données (DPD)

- La loi modifiée du 2 août 2002 **permet déjà** au RT de désigner sur une base volontaire un « chargé de la protection des données » (art. 40).

- Le DPD sera le successeur naturel de l'actuel **« chargé de la protection des donéées »**

- Quels sont les **différences et les similitudes** entre le régime actuel et le régime futur au niveau de:

  - **la désignation**

  - **la fonction**

  - **des missions ?**

1. Au niveau de la désignation

- **Ce qui change à partir du 25 mai 2018**:
  - Désignation d'un DPD est **obligatoire** dans les 3 hypothèses pré-décrites.
  - DPD ne sera **plus agréé** par la CNPD. Toutefois, comme évoqué, il est utile de documenter la décision de désigner ou non un DPD.
  - La **fonction** de DPD sera beaucoup **plus accessible** et ne sera plus limitée aux seules personnes justifiant d'une formation universitaire en droit, économie, gestion d'entreprise, sciences de la nature ou informatique ou faisant partie d'une profession réglementée (avocat à la Cour, réviseur, d'entreprise, expert-comptable et médecin).
  - La désignation d'un DPD est aussi étendue aux sous-traitants
- **Similitudes entre l'actuel et le futur régime**:
  - DPD se devra d'avoir une certaine intégrité professionnelle dans l'exercice de sa fonction et il reste soumis au secret professionnel.
  - DPD interne ou externe.

II. La transition vers le DPD

2. Au niveau de la fonction

- Prérogatives et missions du DPD renforcées. Sa **position/fonction est valorisée**, il rapporte directement au niveau le plus élevé de la direction.

- La loi actuelle se focalise principalement sur le temps dont le chargé de la protection des données doit bénéficier pour effectuer correctement sa mission. Le RGPD étend cette exigence; le RT/ST doit fournir au DPD les **ressources** humaines et techniques nécessaires à l'exécution de ses missions ainsi que l'accès aux données et aux opérations de traitement.

- Même si le minimum actuel d'une **formation** annuelle n'est plus prescrite (art. 1(2) du règlement grand-ducal du 27 novembre 2004), le RT/ST doit permettre au DPD de maintenir ses connaissances et compétences régulièrement à jour.

- Comme le chargé de la protection des données, le DPD est **indépendant** et ne doit pas avoir de **conflit d'intérêts** avec d'autres tâches éventuelles.

3. Au niveau des missions

- Les tâches du DPD sont plus exigeantes que celles du chargé de la protection des données.

- Promouvoir et développer au sein du RT/ST la mise en œuvre d'une politique cohérente de gestion de la protection des données par l'ensemble des intervenants est une tâche qui requiert un large panel de compétences professionnelles et personnelles.

- Les chargés de la protection des données déjà actuellement en fonction disposent d'un avantage dans cette transition de par leur intime connaissance de la structure et de l'organisation du RT ainsi que des risques liées aux traitements de données effectués.

- Le RGPD n'impose pas au DPD de communiquer une copie du registre des traitements contrairement au règlement grand-ducal du 27 novembre 2004 (art. 4) qui le requiert de la part du chargé de la protection des données. Toutefois, comme évoqué plus haut, il est recommandé que le DPD soit étroitement associé à la tenue de ce registre, alors que c'est un élément important pour le RT/ST pour démontrer sa conformité au RGPD.

Commission nationale pour la protection des données

Merci pour votre attention!