# ARTICLE

## M-9 : LE DPD « CHEF D'ORCHESTRE DE LA CONFORMITÉ »

IT et données personnelles ANNULE - Concurrence, régulation européenne et FDI Contrats commerciaux et internationaux | 01/09/17 | Florence Chafiol

TECH & DIGITAL PROTECTION DES DONNÉES PERSONNELLES

Le Délégué à la Protection des Données (« **DPD** »), qu'il soit facultatif ou obligatoire, constituera un atout majeur pour permettre aux organismes de relever les défis du Règlement Général européen sur la Protection des Données (« **RGPD** »), applicable à compter du 25 mai 2018, et plus généralement des nouvelles réalités numériques.

Les responsables de traitement et les sous-traitants doivent désigner un DPD dans l'un des trois cas suivants :

**1**

Si le traitement est effectué **par une autorité publique ou un organisme public**

> Toute autorité publique ou tout organisme public doit désigner un DPD, quelles que soient les données traitées. Le G29 recommande également aux organismes privés chargés d'une mission de service public de désigner un DPD.

**2**

Si leurs **activités de base** 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

> Sont considérées comme des « **activités de base** » les opérations clés de l'organisme qui sont inextricablement liées à son activité et qui lui sont nécessaires pour atteindre ses objectifs. Ne sont pas considérées comme telles les activités de paye et de support informatique selon le G29.

- *Exemple : Bien que l'activité de base d'un hôpital soit de prodiguer des soins, celui-ci ne peut y parvenir qu'en traitant les données de santé des patients.*
- *Exemple : Bien que l'activité de base d'une société de sécurité privée soit de surveiller un certain nombre de centres commerciaux et d'espaces publics, cette surveillance implique nécessaire le traitement de données personnelles.*

> Il n'y a pas de définition de la notion de « **suivi régulier et systématique** » dans le RGPD. Le G29 adopte l'interprétation suivante :
- Un suivi « **régulier** » doit être compris comme intervenant à des intervalles de temps réguliers sur une période donnée et/ou ayant lieu de manière constante ou périodique.
- Un suivi « **systématique** » doit être compris comme étant mis en œuvre de manière préparée/méthodique et/ou dans le cadre d'une stratégie ou d'un projet prédéfini(e).

- *Exemples d'opérations impliquant un tel suivi : la fourniture de services de télécommunication ; les activités marketing axées sur les données ; la géolocalisation des applications mobiles ; les programmes de fidélité ; la publicité comportementale ; les traitements mis en œuvre via les objets connectés ; le « scoring » et le profilage à des fins d'analyse de risque ; etc.*

**3**

Si leurs **activités de base** consistent en un **traitement à grande échelle** de **catégories particulières de données** ou **de données relatives aux condamnations pénales et aux infractions**

> Il n'y a pas de définition de la notion de traitement à « **grande échelle** » dans le RGPD. Selon le G29, les facteurs suivants doivent être pris en compte pour déterminer si le traitement est à « grande échelle » : le nombre de personnes concernées par le traitement ; le volume de données ou l'éventail des différentes données traitées ; la durée ou le caractère permanent du traitement mis en œuvre ; l'étendue géographique du traitement mis en œuvre.

- *Exemple : Les traitements de données de clients dans le cadre de la vie normale des affaires par une banque ou une société d'assurance et les traitements de données personnelles pour de la publicité comportementale par un moteur de recherche doivent être considérés comme des traitements à grande échelle.*
- *Exemple : Le traitement des antécédents judiciaires par un seul avocat ne constitue en revanche pas un traitement à grande échelle.*

> **Les catégories particulières de données** comprennent les données sur l'origine raciale ou ethnique, les opinions politiques, syndicales, philosophiques ou religieuses, les données génétiques et biométriques, les données sur la santé et la vie sexuelle.

**À NOTER**

- Le DPD **est désigné pour l'ensemble des traitements de données mis en œuvre** par les organismes (alors que la loi Informatique et Libertés prévoyait la possibilité de désignation partielle).
- En dehors des trois cas susmentionnés, la désignation du DPD est une « **bonne pratique** » encouragée par le G29 et la CNIL. Lorsqu'un organisme désigne un DPD de manière volontaire, l'ensemble des dispositions/obligations du RGPD relatives au DPD deviennent applicables.
- Les organismes ne souhaitant pas désigner de DPD devront conserver les éléments leur permettant de **justifier pourquoi elles estiment ne pas relever d'un des trois cas susmentionnés**, ce qui pourrait parfois se révéler plus compliqué ou risqué que de nommer un DPD.
- Les **Etats Membres peuvent également, au moyen de leurs lois locales, rendre la désignation d'un DPD obligatoire dans d'autres cas que ceux visés par le Règlement** (*l'Allemagne a ainsi choisi de rendre la désignation d'un DPD obligatoire quand au moins 10 employés de l'entreprise sont impliqués dans le traitement de données à caractère personnel et ce même si aucune des 3 conditions énoncées par le RGPD n'est remplie*).
- Le DPD **peut être un prestataire de service externe** à l'organisme. **Un groupe peut nommer un seul DPD pour toutes ses filiales** à condition que le DPD soit « *facilement joignable* » à partir de chaque lieu d'établissement (disponibilité, langue(s) parlées(s), coordonnées accessibles, etc.). Le G29 recommande que le DPD soit localisé au sein de l'UE.
- L'organisme doit **communiquer les coordonnées du DPD** aux personnes concernées (publication sur le site web de l'organisme par exemple) et à l'autorité de contrôle. Il n'est pas impératif de communiquer au public et aux employés d'un organisme le nom du DPD mais cela est conseillé par le G29 en tant que bonne pratique.

## 2. QUI PEUT ETRE DPD ?

- Le DPD doit avoir **les « qualités professionnelles » et les « connaissances spécialisées »** requises en matière de protection des données, par exemple :
  - Expertise concernant les lois/réglementations et pratiques applicables en matière de protection des données (niveau d'expertise adapté à la sensibilité, la complexité et le volume de données traitées) ;
  - Compréhension du secteur d'activité et des opérations de traitement effectuées par l'organisme ;
  - Compréhension des questions relatives aux technologies de l'information et à la sécurité des données ;
  - Capacité à promouvoir une culture de la protection des données au sein de l'organisme ;
  - Intégrité et éthique professionnelle.
- Le DPD a la possibilité d'exercer d'autres fonctions au sein de l'entreprise, mais **ne doit pas exercer de fonctions susceptibles d'engendrer des conflits d'intérêt** (cela implique en particulier que le DPD n'exerce pas une fonction au sein de l'organisme qui pourrait l'amener à déterminer les finalités et les moyens des traitements).
  - *Le G29 considère par exemple que les fonctions suivantes peuvent engendrer des situations de conflits d'intérêts : PDG ; Directeur des Ressources Humaines ; Directeur Financier ; Directeur Marketing ; Directeur des Systèmes d'Information, mais également des fonctions moins élevées dans la hiérarchie si la personne participe à la détermination des finalités et moyens des traitements mis en œuvre.*

## 3. QUELLES SONT LES MISSIONS DU DPD ?

- ***« Informer et conseiller »*** l'organisme ainsi que ses employés sur leurs obligations en matière de protection des données ;
- ***« Contrôler le respect » de la législation/réglementation applicable*** en matière de protection des données – pour ce faire le DPD doit identifier les traitements de données mis en œuvre, analyser leur conformité avec les dispositions légales applicables et informer/conseiller l'organisme en conséquence ;
- ***« Faire office de point de contact » auprès de l'autorité de contrôle et « coopérer » avec celle-ci*** – il doit aussi faire office de point de contact au sein de l'entreprise et auprès des personnes concernées pour toute question relative au traitement de leurs données ;
- ***« Dispenser des conseils » concernant la réalisation d'une analyse d'impact*** (DPIA) à savoir notamment sur l'opportunité de réaliser une telle étude, la méthodologie à suivre, les modalités de réalisation (en interne ou de manière externalisée), les garde-fous à mettre en place pour préserver les droits des personnes concernées, etc ;
- ***Tenir, le cas échéant, le registre des traitements de données*** mis en œuvre par l'organisme si le responsable de traitement/sous-traitant souhaite confier cette mission au DPD.

## 4. LES MOYENS DU DPD

- Le DPD doit **être « associé, en temps utile [le plus tôt possible], à toutes les questions relatives à la protection des données »** et ainsi notamment :
  - Assister aux réunions des cadres supérieurs ;
  - Etre consulté lors des prises de décisions ayant des répercussions sur la protection des données ;
  - Etre consulté en cas de violation de données ou autre incident de sécurité.

- Le DPD doit bénéficier des « **ressources nécessaires pour exercer ses missions** », ce qui peut notamment impliquer :
  - Le soutien actif de la direction ;
  - Un temps suffisant à sa disposition pour pouvoir exercer ses missions ;
  - Les ressources financières, l'infrastructure et une équipe dédiée si nécessaire ;
  - Une communication officielle concernant sa désignation à tous les salariés pour s'assurer que son existence et ses fonctions sont connues au sein de l'organisme ;
  - Un accès privilégié aux différentes divisions de l'organisme (RH, IT, sécurité, etc.) afin de pouvoir bénéficier de toute information utile ;
  - Des formations récurrentes afin de permettre au DPD d'entretenir/de mettre à jour ses connaissances.

- Qu'il soit employé de l'organisme ou non, le DPD doit exercer ses fonctions en toute indépendance :
  - Le DPD ne doit « **recevoir aucune instruction en ce qui concerne l'exercice des missions** », notamment sur la manière de traiter les questions qui lui sont soumises, ni sur l'objectif à atteindre ou l'interprétation à faire des dispositions légales ;
  - Le DPD **ne doit « pas être pénalisé »** d'une quelconque manière pour l'exercice de ses missions ;
  - Le DPD **doit « rapporter au niveau le plus élevé de la direction »** de l'organisme.

### ACTIONS DE MISE EN CONFORMITE

- Déterminer si la désignation d'un DPD est obligatoire et, à défaut, si elle présente un intérêt pour l'organisme – documenter la position adoptée afin de pouvoir la justifier ;
- Procéder à la détermination d'un profil adapté et d'un positionnement approprié au sein de l'organisme pour remplir la mission de DPD (absence de conflit d'intérêts, indépendance, etc.) ; et s'assurer que le DPD possède les connaissances adéquates et les ressources nécessaires à l'exercice de ses missions ;
- S'assurer que les missions du DPD sont bien conformes aux dispositions du RGPD ;
- Veiller à ce que le DPD soit associé en temps utile à toutes questions relatives à la protection des données en mettant par exemple en place des procédures de saisine obligatoire du DPD.