efcse.eu

OUTIL / RGPD - Délégué à la protection des données personnelles [DPO]

Auteur : Olivier de Maison Rouge, Vice-President EFCSE, Avocat
Mai 2018

Contexte

Afin d'assurer l'effectivité de ses dispositions, le Règlement européen à la protection des données à caractère personnel (RGPD), appliqué depuis le 25 mai 2018, a créé la fonction de délégué à la protection des données (DPD) (ou data protection officer - DPO - en anglais), une fonction proche de celle de l'actuel correspondant informatique et libertés (CIL).

Si le DPD apparaît, à première vue, comme le simple successeur du CIL, ses fonctions sont plus étendues et les conditions de sa désignation diffèrent. Alors que la désignation du CIL était toujours optionnelle, la désignation du DPD est, dans certains cas, obligatoire.

Présentation du DPO

Il est présenté comme un élément clé du nouveau système de protection des données personnelles.

Il assiste les entités dans leur mise en conformité au RGPD et joue un rôle d'intermédiaire entre l'entité à laquelle il appartient, les autorités de contrôle et les personnes concernées.

Il doit veiller au respect du droit de la protection des données personnelles dans un cadre réglementaire devenu plus strict.

Pour mener à bien ses missions, il doit savoir convaincre et diffuser une culture d'entreprise intégrant l'impératif de protection des données et sensibiliser les différents acteurs aux rôles et responsabilités de chacun.

Le DPD doit être associé à chaque projet susceptible d'impacter la vie privée des personnes et la protection de leurs données. Une telle fonction implique des compétences particulières et un choix entre externalisation et désignation interne.

Désignation obligatoire du DPO

Pour les traitements de données à caractère personnel mis en œuvre par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle.

Lorsque les activités de base du responsable du traitement ou du sous-traitant nécessitent un suivi régulier et systématique à grande échelle des personnes concernées.

Lorsque les activités de base du responsable de traitement ou du sous-traitant consistent à traiter à grande échelle des données sensibles.

Désignation : définition du traitement à grande échelle

Le règlement indique qu'il s'agit d'actions « 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 » ((§91 du préambule du règlement).

Le G29[1] précise que les facteurs ci-dessous doivent être pris en compte :

- Nombre d'individus
- Volume de données et/ou différentes catégories de données traitées
- Durée et permanence du traitement
- Etendue géographique du traitement.

Le G29 donne des exemples de ce qui constitue un traitement à grande échelle :

- le traitement par un hôpital des données de ses patients ;
- le traitement des données de personnes utilisant les services de transport public ;
- le traitement des données de géolocalisation en temps réel des clients d'une chaîne de fast food internationale dans un but statistique ;
- le traitement des données clients par une compagnie d'assurance ou une banque ;
- le traitement de données à caractère personnel pour de la publicité ciblée par un moteur de recherche ;
- le traitement de données par des fournisseurs de services internet ou de téléphonie.

Modalités de désignation du DPO

Le DPO peut être interne (un membre du personnel) ou externe (lié par un contrat de service prévoyant une répartition des tâches précise) à l'entité.

Il peut être désigné par un groupe d'entreprises à la condition qu'il soit facilement joignable à partir de chaque lieu d'établissement.

Le groupe peut également désigner un DPO « Relai » dans chaque établissement pour diffuser la politique de protection des données personnelles et faciliter les échanges au niveau local. Le règlement n'exclut en outre pas qu'une entreprise puisse désigner plusieurs DPO internes et externes et leur attribuer des champs de compétences propres à chacun, sous la coordination d'un DPO « chef de groupe ».

[1] G29 : correspond au groupe de travail Article 29 sur la protection des données, c'est un organe consultatif européen indépendant dont l'organisation et les missions ont été définies par les articles 29 et 30 de la directive 95 :46/CE et par l'article 14 de la directive 97/66/CE.

Il est envisageable de prévoir, au sein d'une même entreprise, la mise en place de plusieurs DPO avec, selon les caractéristiques de l'entreprise, un périmètre bien défini pour chacun, par exemple un DPO RH, un DPO business et Marketing, etc.

En France par exemple, la désignation officielle du délégué à la protection des données pourra s'effectuer en ligne auprès de la CNIL[2] par un formulaire dédié.

Compétences du DPO

PRINCIPE : le délégué 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, [tant au niveau national qu'européen] et de sa capacité à accomplir [ses] missions » (article 35).

Le délégué à la protection des données doit avoir une bonne connaissance de l'organisation qui l'aura désigné ainsi que de son secteur d'activité. Une compréhension et une connaissance approfondies du RGPD sont requises. A ce titre, il doit avoir des connaissances juridiques ou se faire accompagner par son service juridique et/ou un avocat, ce dernier pouvant par ailleurs exercer la fonction de DPO.

De même, si le Responsable de la Sécurité des Systèmes d'Information (RSSI) peut éventuellement se voir confier la fonction de DPO, ce dernier ne doit pas être vu comme le candidat naturel. Alors que le RSSI veille à la mise en place des solutions techniques de sécurité adéquates, le DPO doit disposer de solides compétences juridiques.

Le niveau d'expertise exigé n'est pas défini mais doit être proportionné à la complexité et à la quantité des traitements mis en œuvre par l'entité.

Indépendance du DPO

Il est également important de veiller à ce que le délégué à la protection des données ne se trouve pas en situation de conflit d'intérêts dans l'exercice de ses fonctions. Par exemple, il ne pourrait pas exercer en parallèle un poste pour lequel il serait amené à déterminer les finalités et les moyens d'un traitement de données à caractère personnel (tel que directeur marketing, DRH, DSI).

Le DPO ne peut exercer d'autres missions dans l'entreprise que s'il n'est pas en situation de conflit d'intérêts, à ce titre, la désignation d'un DPO externe permettrait d'écarter tout risque de conflit d'intérêts.

S'agissant du cas de l'avocat qui serait désigné DPO, il lui est conseillé d'endosser ce rôle pour un client extérieur uniquement s'il n'a pas agi en tant qu'avocat dans des matières qui relèvent de la responsabilité du DPO ou si, au cours de son mandat de DPO, il n'agit pas dans des matières dans lesquelles il était ou est impliqué comme DPO.

Aux termes de l'article 38 du RGPD, le délégué à la protection des données organise la conformité à la réglementation en matière de protection des données personnelles de l'entité l'ayant désigné.

[2] CNIL : Commission Nationale de l'Informatique et des Liberté, autorité administrative indépendante française dont la devise est « protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles ».

Il devra directement faire rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant.

Il incombe à l'entité de veiller à l'indépendance du DPO dans l'exercice de sa fonction.

L'entité doit notamment veiller à ce qu'il ne reçoive pas d'instruction en ce qui concerne l'accomplissement de ses missions. En interne, les règles de hiérarchie et les sanctions éventuelles en cas de mauvaise exécution des missions confiées par l'entité devront être revues.

L'indépendance du DPO est également garantie par l'impossibilité pour le responsable du traitement ou le sous-traitant de le relever de ses fonctions ou de le pénaliser en raison de l'exercice de sa fonction.

Le contrat de services liant l'entité à un DPO externe ne pourra être résilié sans motif légitime.

Missions du DPO

1. Il informe et conseille les responsables de traitement et sous-traitants, ainsi que leurs employés.
2. Il contrôle le respect de la réglementation sur la protection des données à caractère personnel (en particulier à l'occasion d'audits).
3. Il dispense des conseils pour la mise en œuvre d'analyses d'impact et s'assure de leur réalisation.
4. Il coopère avec l'autorité de contrôle (CNIL).
5. Il interagit avec les personnes concernées au sein de l'entité.

Exercice de la mission du DPO

Le règlement précise que le DPO tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement eu égard à la nature, à la portée, au contexte et aux finalités du traitement.

En collaboration étroite avec le directeur des systèmes d'information et le RSSI, il orientera les choix technologiques vers des solutions offrant de solides capacités de gouvernance et respectant les principes posés par le RGPD (notamment le Privacy by design[3]).

Des compétences juridiques seront mobilisées lorsqu'il s'agira de contrôler la conformité de l'organisme au regard du règlement européen, des règles internes de l'organisme ainsi que des autres dispositions nationales ou européennes applicables.

Le délégué à la protection des données doit être impliqué dans la mise en œuvre d'un traitement dès sa conception ce qui suppose de l'associer aux stratégies de développement.

[3] Privacy by Design : concept qui impose que toute nouvelle technologie destinée à traiter des données personnelles soit conçue pour offrir un haut niveau de protection desdites données.

Le DPO devra être consulté en cas de violation de données à caractère personnel ou tout autre incident relatif aux données à caractère personnel.

En cas de décisions contraires aux recommandations du délégué à la protection des données, il sera opportun de documenter les raisons pour lesquelles son avis n'a pas été suivi.

Le DPO doit être lié par le secret ou la confidentialité en ce qui concerne l'accomplissement de ses tâches, conformément au droit de l'Union ou au droit d'un Etat membre.

Moyens et ressources du DPO

Le responsable du traitement et le sous-traitant doivent fournir au délégué à la protection des données les ressources – notamment financières, matérielles et humaines - en vue de la réalisation de sa mission :

- Soutien actif de la part de la direction
- Temps suffisant accordé à la fonction de DPO lorsque ce dernier exercer d'autres fonctions. Il est recommandé de déterminer le temps nécessaire à consacrer à la fonction, le niveau de priorité à accorder à ses missions.
- Budget suffisant
- Matériel approprié
- Locaux dédiés
- Equipe support si la taille de l'entité le permet
- Temps prévu pour la formation continue

Responsabilité du DPO

Si le délégué à la protection des données ne pourra bénéficier du statut de salarié protégé, il ne saura en revanche être personnellement tenu pour responsable en cas de non-conformité au règlement.

Même s'il ne saurait à proprement parler être responsable des manquements à la règlementation, le DPO a vocation à se placer comme le maillon déterminant de l'accountability.

En France par exemple, il existe des situations où le délégué pourrait, au même titre qu'un autre salarié ou agent, voir sa responsabilité pénale engagée. La responsabilité pénale d'un DPO pourrait ainsi être retenue s'il enfreint intentionnellement les dispositions pénales en matière de protection des données personnelles ou en tant que complice s'il aide le responsable du traitement ou le sous-traitant à enfreindre ces dispositions pénales.