Règlement Général de la Protection des Données
Contexte et Obligations pour le Délégué à la Protection des Données

Sommaire

Le RGPD (« règlement général sur la protection des données ») est le règlement européen qui encadre les règles de protection des données personnelles (règlement UE 2016/679). Il fixe de nouveaux droits pour les personnes physiques dont les données sont collectées et de nouvelles obligations pour les responsables de leur traitement (essentiellement des administrations et des entreprises).

Cette nouvelle réglementation vise à mieux adapter le droit des personnes à l'évolution numérique, et notamment au développement du « big data », du e-commerce, des objets connectés... qui reposent en grande partie sur la collecte et le traitement des données personnelles.

La parution du règlement européen a précédé celle de la loi française sur la protection des données personnelles, afin d'adapter l'ancienne loi Informatique et Libertés aux nouvelles règles européennes (loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles).

En France, le texte de la loi sur la protection des données personnelles a donc été promulgué le 20 juin 2018. Il a ensuite été publié au Journal officiel du 21 juin 2018. Ce texte de loi a été voté au printemps 2018. Il met à jour la loi Informatique et libertés de 1978 en tenant compte des nouvelles normes européennes inscrites dans le règlement européen sur la protection des données personnelles (RGPD 2018), entré en vigueur le 25 mai 2018.

1 - Obligations

Le RGPD impose un nombre d'important de nouvelles obligations pour les responsables d'organismes. En plus des obligations visant à permettre aux personnes d'exercer leurs nouveaux droits, le texte prévoit également des règles en matière de sécurisation des données. Il impose en outre la désignation d'un délégué à la protection des données (DPO), qui sera amené à tenir un rôle de plus en plus important dans les mois et années à venir.

1.1 - Qui est concerné ?

Toutes les entreprises responsables de traitements de données personnelles sont concernées par le RGPD. Les informations permettant d'identifier une personne sont notamment considérées comme des données personnelles : le nom, l'adresse, la date de naissance, la localisation, l'adresse IP... Dès lors que l'entreprise stocke ces données (que cela soit sous la forme de fichier, de tableau, etc.), elle est concernée.

Le texte ne vise donc pas que les réseaux sociaux ou les plateformes internet travaillant massivement sur le « big data » (Google, Facebook...), mais aussi toutes les grandes entreprises, les PME et les TPE qui effectuent des traitements de données. Les nouvelles obligations concernent notamment les sous-traitants des grandes sociétés qui devront démontrer leur mise en conformité au RGPD.

Mais les obligations du règlement ne se limitent pas aux seules entreprises privées puisque les administrations ou les associations sont également concernées.

En revanche, le RGPD ne s'applique pas aux particuliers, c'est-à-dire, selon l'article 18 du règlement, aux personnes physiques qui effectuent des traitements de données à caractère personnel au cours d'activités strictement personnelles ou domestiques. Ces traitements de données doivent être sans lien avec une activité professionnelle ou commerciale.

Plus précisément, les organismes concernés par l'obligation de nommer un DPO sont mentionnés à l'article 37 du RGPD.

Administrations :
Le premier cas concerne les traitements de données personnelles effectués par un organisme public ou une autorité publique (hormis les juridictions). L'obligation concernera donc toutes les structures publiques effectuant des traitements de données personnelles : l'Etat, les collectivités territoriales, etc.

Entreprises :
Mais l'obligation de nommer un DPO concernera aussi un très grand nombre d'entreprises. Le champ d'application posé par l'article 37 du RGPD est en effet très large, puisque seront concernées les entreprises dont les activités de base consistent :

- Soit en des opérations de traitement qui exigent un suivi régulier et systématique à grande échelle des personnes concernées ;
- Soit en un traitement à grande échelle de catégories particulières de données visées à l'article 9 (qui regroupent des données « sensibles » : origines raciales ou ethniques, convictions politiques ou religieuses, etc.) et de données personnelles liées à des condamnations pénales et à des infractions visées à l'article 10.

Il est notamment tenu compte de la nature de l'activité de l'entreprise, du nombre de personnes concernées ainsi que du volume de données traitées. Le règlement ne précise toutefois pas de seuils minimaux à partir desquels l'obligation de recourir à un DPO s'appliquerait : les grands groupes sont bien sûr visés, mais un grand nombre de PME seront également concernées, notamment parmi celles spécialisées dans le e-commerce. L'étendue de l'obligation apparait ainsi très large.

Un groupe d'entreprises peut nommer un seul DPO.

1.2 - Interne ou externe ?

Le recours au DPO représente naturellement un coût supplémentaire pour l'entreprise (en particulier pour les PME).

Si les grandes sociétés recherchent et recrutent des DPO, les entreprises n'ont toutefois pas l'obligation d'embaucher un DPO à temps plein : il n'est pas nécessaire que ce dernier soit un membre du personnel. Il peut ainsi accomplir ses missions sur la base d'un contrat de service. Les entreprises concernées par les nouvelles obligations peuvent donc choisir d'externaliser leur DPO.

1.3 – Le DPO

L'article 37 du RGPD prévoit l'obligation de nommer un délégué à la protection des données, appelé DPO : « Data Protection Officer ». Il est principalement chargé du bon respect, par l'organisme pour lequel il travaille, de la réglementation applicable à la protection des données.

1.4 - Protection et sécurité

Le responsable de l'organisme doit respecter un certain nombre d'obligations en matière de protection et de sécurisation des données qu'il traite. Ses obligations figurent au chapitre IV du RGPD. Dans ce cadre, ses représentants doivent notamment coopérer avec la CNIL.

2 - La Commission nationale de l'informatique et des libertés (CNIL)

La loi Informatique et Libertés, telle que modifiée par la loi du 20 juin 2018, donne à la CNIL une nouvelle compétence en matière de certification de personnes. La CNIL peut désormais adopter des référentiels de certification, et agréer les organismes chargés de délivrer cette certification.

A la suite d'une consultation publique et forte de son expérience dans l'accompagnement des Correspondants Informatique et Libertés (CIL), la CNIL adopte deux référentiels :

- Un référentiel de certification qui fixe notamment les conditions de recevabilité des candidatures et la liste des 17 compétences et savoir-faire attendus pour faire certifier ses compétences de DPO.
- Un référentiel d'agrément qui fixe les critères applicables aux organismes qui souhaitent être habilités par la CNIL à certifier les compétences du DPO sur la base du référentiel de certification élaboré par la CNIL.

2.1 - Synthèse de la consultation publique

La consultation publique sur les projets de référentiels s'est déroulée entre le 23 mai et le 22 juin 2018. Près de 200 contributions ont été reçues provenant :

- De DPO ou de futurs DPO ;
- De responsables de traitement et de sous-traitants (entreprises, fédérations professionnelles, organismes de formation, associations, cabinets d'avocats et cabinets de conseil) ;
- D'organismes de certification.

Les contributeurs représentent des secteurs d'activités très variés (banque, secteur public, santé, éducation, éditeur de logiciels, transport, distribution, enseignement supérieur).

Des réunions de travail ont également été organisées avec les trois associations professionnelles françaises de délégués (ADPO, AFCDP et UDPO) l'IAPP et une dizaine d'organismes de certification.

Cette consultation a permis d'enrichir la réflexion et de trouver le meilleur point d'équilibre entre les connaissances et compétences que doit détenir le DPO et les attentes des professionnels (organismes de certification, DPO, responsables de traitement, sous-traitant).

2.2 - La certification des personnes physiques

La certification n'est pas obligatoire pour exercer les fonctions de délégué à la protection des données. Ce n'est pas non plus un préalable nécessaire à la désignation auprès de la CNIL. Inversement, il n'est pas exigé d'être désigné en tant que délégué pour être candidat à la certification des compétences du DPO.

Il s'agit d'un mécanisme volontaire permettant aux personnes physiques de justifier qu'elles répondent aux exigences de compétences et de savoir-faire du DPO prévues par le règlement. Acteur clé de la conformité au RGPD, le DPO doit en effet disposer de connaissances spécialisées du droit et des pratiques en matière de protection des données. Le certificat constitue un vecteur de confiance à la fois pour l'organisme faisant appel à ces personnes certifiées mais également pour ses clients, fournisseurs, salariés ou agents.

Les conditions préalables pour accéder à la certification sont précisées à l'exigence 1 du référentiel de certification.

2.3 – Organismes certificateurs

La CNIL ne délivrera pas elle-même de certification des compétences du DPO. Ce sont les organismes certificateurs, lorsqu'ils auront été agréés par la CNIL, qui délivreront la certification aux personnes remplissant les conditions préalables et ayant réussi l'épreuve écrite. La certification ne sera donc possible que lorsque les premiers agréments auront été délivrés par la CNIL aux organismes certificateurs. Les personnes intéressées par cette certification pourront alors se rapprocher de ces organismes en vue d'être certifiés.

2.4 - L'agrément des organismes certificateurs par la CNIL

Les organismes certificateurs qui souhaitent délivrer une certification de compétences sur la base du référentiel d'agrément de la CNIL peuvent déposer une demande d'agrément auprès de la CNIL (modalités décrites dans les FAQ). La demande devra respecter les exigences prévues dans le référentiel d'agrément.

Dans l'attente de l'élaboration d'un programme d'accréditation spécifique portant sur la certification des compétences du DPO avec le COFRAC, les organismes certificateurs candidats à l'agrément de la CNIL doivent être agréés par un organisme d'accréditation au regard de la norme ISO/CEI 17024:2012 (Évaluation de la conformité – Exigences générales pour les organismes de certification procédant à la certification de personnes) dans un domaine existant.

Le fonctionnement de ce dispositif fera l'objet, au plus tard dans un délai de deux ans à compter de son entrée en vigueur, d'une évaluation en vue d'adapter, le cas échéant, les exigences des référentiels. Les éventuelles modifications du référentiel d'agrément ou du référentiel de certification seront sans incidence sur les certifications ou les agréments qui auront déjà été délivrés.

Ces référentiels pourront être partagés avec les autres autorités de protection européennes au sein du CEPD (Comité européen de la protection des données).

L'agrément de la CNIL n'est obligatoire que pour les organismes qui souhaitent délivrer une certification des compétences du DPO sur la base du référentiel élaboré par la CNIL. Cela signifie que tout organisme peut néanmoins certifier des compétences du DPO sur la base de son propre référentiel de certification, non approuvé par la CNIL, comme c'est déjà le cas aujourd'hui.