LA DÉSIGNATION D'UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES : **DRH, ÊTES-VOUS PRÊTS ?**

LA CHRONIQUE JURIDIQUE D'AVOSIAL

Le syndicat des avocats d'entreprise en droit social

CLAIRE LE TOUZÉ
SIMMONS & SIMMONS

LE RÈGLEMENT EUROPÉEN GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD) entre en vigueur le 25 mai 2018. Faisons un zoom sur l'une des nouveautés majeures : l'obligation pour certaines entreprises de désigner un délégué à la protection des données, également appelé en anglais, Data Protection Officer (DPO), terme retenu par la pratique.

QU'EST-CE QU'UN DPO ?

C'est une sorte de vigie des données personnelles, une évolution du correspondant informatique et libertés (CIL) avec davantage de responsabilités. Le DPO a pour mission principale d'informer et de conseiller les entreprises sur le traitement des données ; de contrôler le respect des dispositions du RGPD et d'être l'interface entre l'entreprise et l'autorité de contrôle (la CNIL).

DANS QUELLE ENTREPRISE DOIT-IL ÊTRE DÉSIGNÉ ?

Le Règlement prévoit la désignation obligatoire d'un DPO, notamment par les entreprises dont l'activité de base les amène à réaliser un suivi régulier et systématique des personnes à grande échelle ou consiste en un traitement à grande échelle de données sensibles.

Est-ce à dire que cette obligation concerne toutes les entreprises en raison du traitement des données personnelles relatives aux salariés (établissement des bulletins de paie par exemple) ? Bien heureusement non, le G29 (organisation qui réunit l'ensemble des CNIL européennes) précise que l'activité de base doit être entendue comme l'activité principale de l'entreprise, or, le traitement des données des salariés n'est qu'une activité accessoire.

Par conséquent, l'obligation ne concerne que les entreprises dont l'activité principale les amène à traiter des données à caractère personnel de grande ampleur (ex : une société de surveillance d'espace public) ou portant sur des données sensibles.

COMMENT CHOISIR VOTRE DPO ?

Une liberté de choix est laissée aux entreprises : le délégué peut être désigné parmi les membres du personnel ou être un prestataire externe. Une mutualisation entre plusieurs entreprises est possible.

En revanche, le DPO doit impérativement être désigné sur la base de ses connaissances spécialisées du droit et des pratiques en matière de protection des données (ce qui suppose une expérience significative dans le domaine ainsi qu'une formation adaptée). Ainsi, les DPO seront d'anciens CIL, des professionnels de la sécurité informatique, du droit ou de la conformité à condition qu'ils aient reçu une formation complémentaire. Il conviendra néanmoins de s'assurer que le DPO n'exerce pas, par ailleurs, des fonctions qui peuvent l'amener à déterminer les finalités et moyens de traitement. Ainsi, certaines fonctions sont susceptibles de donner lieu à un conflit d'intérêts avec la mission de DPO : le directeur informatique, le DRH, le responsable marketing ou encore les fonctions d'encadrement général.

LE DPO ET LES RH, EN PRATIQUE ?

Les actions à mettre en œuvre entre DPO et RH sont multiples. En effet, de nombreuses actions RH visent à collecter, traiter et stocker des données personnelles, tel le recrutement (données personnelles des candidats), la paie et la politique de rémunération et les avantages sociaux, la sécurité et la gestion des accès, le temps de travail… RH et DPO devront œuvrer pour s'assurer que les données collectées soient adéquates, pertinents et strictement nécessaires à la finalité du traitement.

QUEL STATUT POUR LE DPO ?

Le DPO doit disposer d'une autonomie et de ressources suffisantes pour s'acquitter de ses missions. À ce titre, il devra être associé à toutes les questions relatives à la protection des données dans l'entreprise et son indépendance devra être garantie. Bénéficiera-t-il du statut de salarié protégé ? La loi est muette sur le sujet mais précise que celui-ci ne sera pas personnellement responsable en cas de non-conformité avec le Règlement.

QUELLE SANCTION ?

Le non-respect des dispositions du RGPD (parmi lesquelles figure l'obligation de nommer un DPO pour certaines entreprises) peut donner lieu à une amende pouvant s'élever jusqu'à 10 millions d'euros ou jusqu'à 2 % de son chiffre d'affaires annuel mondial total de l'exercice précédent.

Il est donc urgent de vous mettre en conformité avec la désignation de ce nouvel acteur !