RGPD et DPO : la liste des compétences est longue et le nombre de profils insuffisant

On sait en revanche que la CNIL, garante de la protection des données des citoyens français, a reçu 13 000 déclarations de DPO, soit seulement 16% des 80 000 estimées nécessaires. Le Délégué à la Protection des Données est pourtant considéré par la CNIL comme la clé de voûte de la conformité au règlement européen.

Pour mémoire, le RGPD est la nouvelle réglementation mise en place le 25 mai 2018 par l'Union Européenne pour contraindre toutes les organisations à garantir leur contrôle sur la collecte, le stockage et l'utilisation des données à caractère personnel des ressortissants européens. Les conséquences peuvent être très lourdes pour les entreprises, avec des amendes pouvant atteindre 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial. Sans compter bien sûr le risque sur la réputation de la société, sa perte de clientèle, les frais de procédures en cas de plaintes, etc.

RGPD et DPO : quelles sont les obligations de l'entreprise ?

Pour être en mesure de tenir leurs engagements, les entreprises doivent donc se doter d'un DPO, dont les missions sont stratégiques : conseils organisationnels, techniques et juridiques sur la bonne sécurité des données, relations avec la CNIL et les autres DPO, gestion des demandes d'exercice des droits, du respect des règles (Accountability) et des risques encourus.

D'après la CNIL, dans le cadre de la mise en application du RGPD, l'entreprise a l'obligation de :

- Choisir son DPO en fonction de son expertise.
- Veiller à ce que son expert reçoive la formation et les moyens matériels, financiers et intellectuels nécessaires pour mener à bien sa mission.
- Veiller à ce que son DPO exerce ses activités sans conflit d'intérêts, en toute indépendance, qu'il puisse rendre compte de son action au plus haut niveau de l'entreprise.

Le choix du DPO doit être pris en fonction de ses compétences, mais aussi de son expérience de la protection des données, selon l'exposition aux risques identifiés de l'entreprise (classement risques EBIOS) :

- Exposition basse : un minimum de 2 ans d'expérience peut être suffisant.
- Exposition très haute : un minimum de 5 à 15 ans d'expérience peut s'avérer nécessaire.

Si l'on considère la pénurie actuelle de DPO et le caractère récent du métier, ces exigences d'expérience peuvent apparaître compliquées à remplir par tous.

Compétences et savoir-faire du DPO

Pour répondre aux nombreux questionnements des entreprises, la CNIL a publié au Journal Officiel le 11 octobre un référentiel listant les 17 critères cumulatifs auxquels un DPO doit pouvoir

répondre pour être certifié par un organisme certificateur. Une démarche d'autant plus attendue que les profils ont été jugés très hétérogènes parmi les 13 000 DPO déclarés à la CNIL.

Les compétences et savoir-faire que les DPO doivent satisfaire peuvent être regroupés en trois catégories, organisationnelle, juridique et technique :

- **Les savoirs organisationnels** : le DPO conseille l'entreprise dans l'élaboration de procédures et politiques, ce qui induit des connaissances en gouvernance des entreprises. Par ailleurs, il est en mesure de mener un audit de conformité et de proposer des mesures de réduction ou gestion des risques, de les évaluer et d'en surveiller la mise en œuvre.

- **Les savoirs techniques et informatiques** : le DPO doit mettre en œuvre les principes de minimisation ou d'exactitude, d'efficacité et d'intégrité des données et pouvoir exécuter les demandes de modification et d'effacement de données, ce qui impacte les systèmes et solutions de l'entreprise. Le DPO doit être ainsi force de conseils et de recommandations pour la mise en œuvre du « Privacy by Design » dans l'entreprise.
- **Les savoirs juridiques** : le DPO est un expert en protection juridique et règlementaire des données à caractère personnel. Outre le RGPD, il peut conseiller l'entreprise en cas de conflit de lois. Il participe à l'élaboration des contrats avec les partenaires, peut négocier avec le DPO du partenaire les clauses de protection de données personnelles. Il a également un rôle essentiel à jouer en matière de contentieux : il est l'interlocuteur de la CNIL et il instruit les plaintes des personnes concernées.

Avec ce référentiel de certification, l'entreprise dispose donc désormais d'éléments pour vérifier l'adéquation des savoirs en place en interne. Et force est de constater que le DPO doit faire figure de super-héros multi-compétences aux expertises transverses dans de nombreux domaines.

Par ailleurs, il s'avère dans la pratique que la seule connaissance du texte de loi publié est insuffisante pour être en mesure de répondre à ces exigences.

La nécessaire montée en expertise du DPO

L'entreprise qui constate ne pas être en capacité à répondre aux critères du référentiel se trouve dans une position potentiellement à risque. Si elle dispose déjà d'un DPO en place, qu'il soit déclaré à la CNIL ou pas encore, il s'agit de mesurer l'écart d'expertise à combler et de l'accompagner en mettant à sa disposition les moyens matériels, financiers et intellectuels pour lui permettre d'atteindre les objectifs fixés.

Selon l'exposition aux risques identifiées par l'entreprise, elle peut faire le choix d'une montée en expertise dans les catégories prioritaires pour elle. Par exemple, si l'organisation a une part importante de son activité gérée par des prestataires externes, elle devra les auditer régulièrement et réviser sa politique contractuelle, et le DPO sera alors très attendu sur les aspects juridiques et audits. Il pourra alors avoir besoin d'un soutien sur des points précis tels que : auditer un traitement ou une conformité, mener un DPIA et gérer les risques, élaborer une procédure…

Le référentiel de la CNIL fixe le plancher des connaissances au suivi d'une formation de 35h sur le RGPD, afin d'en avoir une vision synthétique. Cela pourra s'avérer insuffisant tant la plupart des missions du DPO requiert des expertises fines dans des domaines très divers.

En prenant en compte l'isolement du DPO dans ses fonctions du fait de leur nature, et que la collaboration ou l'émulation avec des profils plus seniors dans l'entreprise est donc rarement possible, il n'est effectivement pas simple d'organiser un accompagnement dans sa montée en compétence. La CNIL encourage donc les DPO à s'organiser en groupes de travail réunis par secteurs d'activité, territoires ou même pour les indépendants à mutualiser leurs fonctions pour plusieurs entreprises. Cette approche ne produira néanmoins des résultats qu'à moyen terme et remplacera difficilement un transfert de savoir-faire par des DPO seniors.

Le choix de l'externalisation

Si l'entreprise ne dispose pas encore de DPO, ou si l'écart d'expertise à combler est trop important, l'externalisation totale ou partielle des fonctions de DPO peut être une option viable. Pour une entreprise de petite ou moyenne taille qui ne souhaite pas disposer d'un DPO en interne, avoir recours à des services extérieurs mutualisés est une des possibilités les plus pertinentes.

Mais une externalisation partielle présente aussi l'avantage d'accompagner le DPO interne dans une partie de ses activités, avec un partage des pratiques professionnelles à l'aune des contraintes de l'entreprise. Une approche qui gagnera en efficacité si elle est envisagée dans le cadre d'un plan global de formation du DPO.