

DPO : en faut-il un, et l'externaliser ?

Délégué à la protection des données obligatoire ou pas, interne ou mutualisé : trancher pour une PME, sans sur-dimensionner.

7 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/dpo-externalise

Le DPO (délégué à la protection des données) est le chef d'orchestre RGPD d'une organisation — obligatoire dans certains cas, précieux dans d'autres, superflu ailleurs. Les PME oscillent entre deux erreurs : s'en croire dispensées de tout pilotage RGPD (non), ou nommer DPO « officiel » un salarié sans temps ni indépendance (pire que rien, car le statut engage). Le point pour trancher — et le mode d'emploi de l'externalisation, souvent la bonne réponse à cette échelle.

1. Obligatoire ou pas : les trois cas

- DPO obligatoire si : vous êtes un organisme public ; votre cœur d'activité exige un suivi régulier et systématique de personnes à grande échelle (profilage, géolocalisation, surveillance) ; ou vous traitez à grande échelle des données sensibles (santé, biométrie, condamnations)
- La PME classique (clients, salariés, prospection ordinaire) n'y est PAS tenue — le critère est le cœur d'activité et l'échelle, pas la simple détention de données
- Cas frontières fréquents : santé et médico-social, marketing intensif, applications qui tracent — dans le doute, une analyse ponctuelle par un conseil tranche pour toujours
- Non obligatoire ne veut pas dire rien : les obligations RGPD demeurent — il faut bien que quelqu'un les pilote

2. Ce qu'un DPO fait (et n'est pas)

- Il informe et conseille, contrôle la conformité, pilote registre et analyses d'impact, forme, et sert de point de contact CNIL et personnes concernées
- Il est indépendant et protégé : pas d'instructions sur ses missions, pas de sanction pour ses avis, rattachement au plus haut niveau — c'est pour cela que le dirigeant, le DSI ou le responsable marketing sont en conflit d'intérêts pour le rôle
- Il n'est PAS le responsable à la place de l'entreprise : la conformité reste portée par la direction — le DPO éclaire et alerte, il ne décharge pas
- À distinguer du référent numérique : le référent est une organisation interne libre ; le DPO, un statut réglementé, déclaré à la CNIL

3. L'externalisation : le format PME

- Le DPO externe mutualisé (avocat, cabinet, prestataire spécialisé) apporte l'expertise et l'indépendance sans créer de poste — de quelques centaines à ~1 500 €/mois selon la complexité
- Le format type : audit initial et registre, puis un forfait de suivi (questions courantes, mises à jour, veille) + interventions ponctuelles (violation, contrôle, nouveau traitement)
- Les critères de choix : références dans VOTRE taille et secteur, réactivité contractuelle en cas de

violation (72 h !), livrables concrets — et un binôme interne désigné (le référent) car le DPO externe sans relais interne ne voit rien

- Alternative sans nomination formelle : les mêmes prestations en « conseil RGPD » récurrent — la valeur sans le statut, pertinent hors obligation

ATTENTION

Le piège du DPO « de papier » : nommer un salarié pour cocher la case, sans temps, formation ni indépendance. Le statut déclaré à la CNIL crée des attentes (missions effectives, moyens) — un DPO nominal défaillant se retourne contre l'entreprise en contrôle, là où l'absence assumée de DPO (hors obligation) avec un pilotage réel se défend très bien. Mieux vaut un vrai pilotage sans titre qu'un titre sans pilotage.

4. Décider en pratique

- Étape 1 : vérifier l'obligation (les trois cas) — 30 minutes avec les critères CNIL, ou une consultation si frontière
- Étape 2 : si obligatoire !' externalisé mutualisé dans 90 % des cas de PME ; interne seulement si la taille et l'activité justifient un mi-temps réel
- Étape 3 : si non obligatoire !' référent interne outillé + conseil ponctuel, et réévaluation quand l'activité évolue (nouveau produit qui trace, données de santé, croissance)
- Dans tous les cas : le socle documenté d'abord — aucun DPO ne compense un registre inexistant

L'essentiel à retenir

- 01 Vérifier si l'un des trois cas d'obligation s'applique
- 02 Ne jamais nommer un DPO sans temps, formation et indépendance
- 03 Privilégier l'externalisation mutualisée à l'échelle PME
- 04 Contractualiser la réactivité (violations, contrôles)
- 05 Désigner le binôme interne du DPO externe
- 06 Réévaluer à chaque évolution significative de l'activité

Questions fréquentes

Le DPO externe peut-il être notre prestataire informatique ?

Prudence : le DPO contrôle notamment... la sécurité que ce prestataire opère — être juge et partie fragilise l'indépendance exigée. La CNIL admet le cumul avec des garde-fous, mais la séparation est plus saine : l'IT chez l'un, le DPO chez un autre, qui se parlent. Même logique que l'audit indépendant de l'exploitant.

Que risque-t-on à ne pas nommer de DPO alors qu'il était obligatoire ?

C'est un manquement sanctionnable en soi (mises en demeure et amendes régulières sur ce motif), et surtout un très mauvais signal en contrôle : l'obligation ignorée suggère le reste à l'avenant. Le test des trois cas prend une demi-heure — faites-le, documentez la conclusion, et elle vous protège dans les deux sens.

Un DPO doit-il être juriste ou informaticien ?

Les deux cultures servent : le droit pour les fondements, la technique pour juger les mesures réelles. Les textes exigent des « connaissances spécialisées » sans imposer de diplôme — en externalisé, cherchez l'équipe qui combine, ou le profil qui sait s'entourer. Le critère décisif reste la pratique de VOTRE taille d'entreprise : le DPO de groupe industriel appliquera des recettes inadaptées à une PME de 20 personnes.

Pour aller plus loin

CNIL — le délégué à la protection des données — www.cnil.fr/fr/le-delegue-la-protection-des-donnees-dpo

CNIL — désigner un DPO — www.cnil.fr/fr/designation-dpo

Structurer sans vous noyer dans la paperasse ?

Audit, mise en conformité, chartes et sensibilisation des équipes : un accompagnement à la taille de votre entreprise.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr