

Est-il obligatoire d'avoir un DPO?

écrit par Marine de la Clergerie | 08/06/2017

Dois-je nommer un Data Protection Officer (DPO)/ Délégué à la Protection des Données (DPD) ?

La nomination d'un DPO (interne ou externe, mutualisé ou non) est recommandée dans tous les cas, mais elle **est obligatoire dans les 3 cas suivants** (article 37, §1 du RGPD et guidelines du G29) :

Le traitement est effectué par une autorité publique ou un organisme public ;

Exemples : les autorités nationales, régionales et locales ; les organismes du secteur public (État, collectivités territoriales, associations formées par ces collectivités ou organismes) ; les organismes de droit public.

Les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ;

Exemples : Hôpitaux ; sociétés de sécurité privée assurant la surveillance d'un certain nombre de centres commerciaux ; les sociétés traitant les données de voyage des passagers utilisant un moyen de transport public urbain ; les sociétés internationales de restauration géolocalisant leurs clients ; les compagnies d'assurances ; les banques ; les moteurs de recherche ; les fournisseurs de services de téléphone ou internet ; exploitation d'un réseau de télécommunication ; fourniture de services de télécommunications ; ciblage par courrier électronique ; activités de marketing fondées sur les données ; profilage et notation à des fins d'évaluation des risques ; géolocalisation par exemple par des applications mobiles ; programmes de fidélité ; publicité comportementale ; surveillance des données sur le bien-être, la santé et la condition physique au moyen de dispositifs portables ; système de télévision en circuit fermé ; dispositifs

connectés.

Les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

Il sera toutefois nécessaire de vérifier si la législation de l'État membre n'impose pas la nomination d'un DPO, dans la mesure où cette faculté est prévue au §4 du même article.

Dans tous les cas, la décision de nommer ou non un DPO doit être documentée (principe d'accountability).

Pour rappel, les violations des dispositions relatives au DPO peuvent entraîner des amendes pouvant s'élever jusqu'à 10 000 000 d'euros ou 2% du chiffre d'affaires mondial (art.83.4.a du RGPD)

Références : article 37, §1 du RGPD ; Guidelines/Lignes directrices concernant [les délégués à la protection des données](#), adoptées le 13.12.2016 et révisées le 5.04.2017 ; [Devenir délégué à la protection des données](#), CNIL 23.05.2017