contrast

VOS ACTIVITÉS • FÉVRIER 2021

Est-il temps de réexaminer la désignation de votre DPO ?

Ce que vous devez savoir.

Si votre entreprise a comme activité de base le traitement à grande échelle de données sensibles et/ou judiciaires, ou si elle effectue un suivi de manière régulière et systématique des personnes (par exemple via des cookies), vous devez alors désigner un Délégué à la Protection des Données (en anglais : *Data Protection Officer* ou *DPO*). Tant que celui-ci possède l'expertise nécessaire en ce qui concerne la législation et la pratique, votre DPO peut être tant un membre du personnel interne qu'un conseiller externe. De plus, votre DPO doit exercer ses fonctions en toute indépendance. Cela signifie, entre autres, qu'il ne peut recevoir aucune instruction en ce qui concerne l'exercice des missions, qu'il est protégé contre toute sanction et contre le licenciement et qu'il est soumis au secret professionnel ou a? une obligation de confidentialité?.

La désignation d'un DPO interne présente de nombreux avantages : le DPO connaît l'entreprise et connaît également ses intérêts (commerciaux). Il n'est pas toujours aisé de préserver l'indépendance et d'éviter les conflits d'intérêts entre la fonction de DPO et toute autre fonction. Selon le Groupe de travail « Article 29 » (WP29), votre DPO n'est en effet pas autorisé à exercer une fonction qui l'amène à déterminer les finalités et les moyens du traitement des données à caractère personnel.

Il n'est donc pas possible de cumuler la fonction de DPO avec celle de chef du département que le DPO doit superviser, par exemple le département d'audit, des risques et de la conformité. Une fonction de directeur signifie en effet que l'on détermine inévitablement la finalité et les moyens du traitement des données à caractère personnel au sein du département concerné.

Ce que vous devez faire.

La plupart des entreprises ne sont pas tenues de désigner un DPO. Que vous désigniez un DPO parce que cela est requis par la loi ou sur une base volontaire, vous devez savoir que cette décision n'est pas sans conséquence.

Ainsi, vous devez **documenter** votre choix de désigner (ou non) un DPO. Le suivi de votre processus décisionnel découle, entre autres, du principe de responsabilité imposé par le RGPD. Si cette décision prévoit la désignation d'un DPO, ce document doit également démontrer l'expertise du DPO (APD [*actuellement disponible uniquement en néerlandais*]). Si lors d'une procédure de sélection, un profil ressort comme la personne « la plus apte », cela ne démontre pas *ipso facto* que celle-ci est suffisamment apte (APD). En outre, il est conseillé de préciser également dans ce document (i) les tâches et (ii) l'absence de conflit d'intérêts et de réévaluer régulièrement cette analyse et d'actualiser le document.

De plus, vous devez **fournir toutes les ressources à la disposition de votre DPO** afin qu'il puisse exercer ses missions en toute indépendance. Cela comprend, par exemple, le soutien actif du DPO par la direction, l'accès à certains services, la formation continue, l'octroi de suffisamment de temps pour s'acquitter de ses missions et de moyens financiers suffisants, d'une infrastructure et du personnel. Plus les opérations de traitement sont complexes ou sensibles, plus les ressources octroyées au DPO devront e?tre importantes. (APD). La communication formelle au sein de votre entreprise de la désignation de votre DPO, destinée à s'assurer que l'existence et la fonction du DPO sont connues, relève également de cette obligation.

Afin que votre DPO puisse exercer ses missions, vous devez **l'associer d'une manie?re approprie?e et en temps utile** a? toutes les questions relatives a? la protection des donne?es a? caracte?re personnel. Re?duire l'association du DPO a? sa simple information (*a posteriori*) est insuffisant. En d'autres termes, vous êtes obligé d'associer votre DPO de?s le stade le plus pre?coce possible, afin qu'il puisse agir en tant que conseiller (WP29 et APD).

Vous devez également permettre à votre DPO de **faire directement rapport** au niveau le plus e?leve? de la direction de votre entreprise. Cela ne peut pas se limiter à un rapport annuel, car cette obligation de rapportage s'applique également aux activités d'informations et de conseils *ad hoc* du DPO quant aux obligations découlant de traitements de données à caractère personnel envisagés (APD).

Enfin, vous devez également **divulguer les coordonnées** de votre DPO à la fois à l'autorité de protection des données compétente et aux personnes concernées. Le DPO est le premier point de contact tant pour l'autorité que pour les personnes concernées. S'ils s'adressent à votre entreprise, le DPO doit répondre.

Ces obligations garantissent que votre DPO puissent s'acquitter correctement de ses missions (c'est-à-dire, le cas échéant, informer et conseiller sur les obligations en matière de protection des données, contrôler le respect du RGPD, dispenser - sur demande - des conseils en ce qui concerne l'analyse d'impact relative a? la protection des données, coopérer avec les autorités et faire office de point de contact).

Il est clair que la désignation (volontaire) d'un DPO est une décision qui ne doit pas être prise à la légère. Avez-vous désigné un DPO suffisamment qualifié lorsque le RGPD est entré en vigueur, mais qui dirige également un département ? Ou qui ne participe pas à l'analyse d'une éventuelle violation de données a? caractère personnel ? Ou qui ne fait pas rapport au conseil d'administration ? Votre entreprise est alors en violation du RGPD et risque d’être sanctionnée par l'autorité. Est-il temps de réexaminer la désignation de votre DPO ?