RGPD : Dans quel cas devez-vous désigner un DPO (Data Protection Officer) ?

RGPD : Dans quel cas devez-vous désigner un DPO (Data Protection Officer) ?

L'article 37 du RGDP oblige les opérateurs (responsable de traitement et sous-traitant), dans certains cas, à désigner un DPO. Le G29 [1] encourage, par ailleurs, toutes les entreprises à procéder à la désignation d'un DPO, étant précisé qu'en cas de désignation « volontaire » d'un DPO, l'entreprise devra respecter l'ensemble des dispositions du RGDP y afférentes. Dans quel cas est-il obligatoire de désigner un DPO ?

Selon le RGPD (Réglement Général sur la Protection des Données), il est obligatoire de désigner un DPO dans trois différentes hypothèses :
1. Lorsque le traitement des données personnelles est effectué par une autorité publique ou un organisme public ;
2. Lorsque les *« activités de base »* du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui exigent un *« suivi régulier et systématique »* à *« grande échelle »* des personnes concernées ;
3. Lorsque les *« activités de base »* du responsable du traitement ou du sous-traitant consistent en un traitement à *« grande échelle »* des données *« particulières »*, c'est-à-dire sensibles au sens de la réglementation en matière de données personnelles (telles que les données de santé ou relatives à des infractions ou condamnations).

La première hypothèse n'appelle pas de commentaire particulier. En revanche, comment interpréter les notions d'« activités de base », « suivi régulier et systématique » et « grande échelle » des deux autres hypothèses ?

« activités de base »

Le G29 [1] précise qu'il s'agit des activités principales et non accessoires du responsable de traitement ou du sous-traitant. Autrement dit, ce sont les opérations de traitement de données personnelles qui découlent des opérations clés résultant de l'activité du responsable de traitement ou du sous-traitant. Le G29 [1] illustre son propos de plusieurs exemples. Ainsi, par exemple, une société ayant pour activité principale la surveillance d'espaces publics doit nécessairement mettre en œuvre des traitements de données personnelles résultant de cette surveillance, cette société devrait donc désigner un DPO. Au contraire, les opérations de traitement de données personnelles relatives aux salariés de l'entreprise, liées à l'établissement des fiches de paie, des congés, etc., ne seraient que des opérations accessoires.

« grande échelle »

Le G29 [1] ne définit pas plus que le RGDP cette notion et fournit seulement les critères pouvant être pris en compte pour déterminer s'il s'agit d'un traitement à « grande échelle ».
Devront ainsi être pris en compte :
• le nombre de personnes concernées ;
• le volume des données traitées ;
• la durée du traitement ;
• l'étendue géographique du traitement.
Cette notion, dont l'interprétation sera casuistique, place ainsi les entreprises face à une certaine insécurité juridique. Elles devront faire preuve de prudence quant à leur décision de ne pas désigner de DPO.

« suivi régulier et systématique »

Le G29[1] a défini, d'une part, la notion de *« suivi régulier »* comme étant un suivi *« en cours ou se produisant à des intervalles particuliers pour une période donnée »* ou *« récurrent ou répété à des moments fixes »* ou encore *« constant ou périodique »* et, d'autre part, la notion de *« suivi systématique »* comme étant un suivi *« produit selon un système »* ou *« pré-organisé, organisé ou méthodique »* ou *« adopté dans le cadre d'un plan général de collecte de données »* ou encore *« réalisé dans le cadre d'une stratégie globale »*. Cette notion doit nécessairement couvrir toute activité consistant à faire du suivi et du profilage en ligne des personnes.
Exemples d'activités traitant de manière régulière et systématique des données personnelles :
• Recherche et profilage sur Internet ;
• Opérateur de réseau de télécommunication ;
• Fournisseur de services de télécommunication ;
• Publicité comportementale ;
• Géolocalisation ;
• E-mail retargeting ;
• Vidéo surveillance ;
• Appareils connectés ;
• etc.

: Le G29 [1] recommande à toutes les entreprises traitant des données personnelles de désigner un DPO.

[1] : Le G29 est un organe consultatif européen indépendant sur la protection des données et de la vie privée. Son organisation et ses missions sont définies par les articles 29 et 30 de la directive 95/46/CE, dont il tire sa dénomination sur la protection des données

---

Besoin de **vous mettre en conformité avec le RGPD** ?
Besoin d'une **formation pour apprendre à vous mettre en conformité avec le RGPD** ?
Contactez-nous

A Lire aussi :
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

ou suivez nous sur

Réagissez à cet article

Source : *Le statut du délégué à la protection des données personnelles. Par Jean-Baptiste Chanial et Cécile Louwers, Avocats.*