racine AVOCATS

Décryptage

Janvier 2024

Condamnation de la commune de Kourou par la CNIL : L'arbre qui cache la forêt

Un rappel du contexte permettra de mieux comprendre cette décision.

En 2021, la CNIL a procédé à des vérifications concernant la désignation ou non de DPO, au sein des communes de plus de 20 000 habitants. Pour mémoire, on compte, d'après le calculateur du site de l'AMF, 502 communes de plus de 20 000 habitants en France métropolitaine et outre-mer.

Suite à cette vérification, la CNIL a alerté les communes qui n'avaient pas désigné de DPO.

En mai 2022, soit un an après cette « alerte », la CNIL, constatant que certaines communes n'avaient toujours pas satisfait à cette obligation, rendit publique une mise en demeure de désigner sous 4 mois un DPO, adressée à 22 communes parmi lesquelles celle de Kourou.

Le cas particulier de la commune de Kourou

La commune de Kourou, n'ayant pas satisfait à sa mise en demeure et ne lui ayant pas répondu, la CNIL est donc entrée en voie de condamnation par le biais d'une sanction simplifiée à hauteur de 5 000 € et injonction de désigner un DPO dans un délai de 3 mois.

Passé ce délai, la commune de Kourou n'ayant toujours pas satisfait à cette exigence ni répondu à la CNIL, cette dernière a à nouveau condamné la ville, dans le cadre d'une procédure ordinaire, à une amende de 5 000 € et une injonction de désigner un DPO dans les 2 mois, affectée d'une astreinte de 150 € par jour de retard.

Les enseignements à tirer de cette décision

On peut tirer 3 enseignements de cette décision :

1. **La CNIL réaffirme ainsi l'impérieuse nécessité pour les « autorités publiques » ou les « organismes publics » (à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle) de désigner un DPO (article 37 du RGPD).**

Mais qui sont ces « autorités publiques » ou « organismes publiques » ?

Il est difficile de trouver une définition précise de ces termes en droit français et les considérants du RGPD ne donnent aucune réponse.

La CNIL précise dans son guide pratique relatif au DPO que sont visés par ces termes : « les autorités nationales, régionales et locales mais également des organismes tels que les structures de l'enseignement supérieur, hôpitaux, agences sanitaires, autorités administratives indépendantes (AAI), établissements publics à caractère administratif (EPA), etc. ».

La CNIL précise également, et ce point est très important, que « les organismes privés chargés d'une mission de service public conservent leur statut de droit privé et ne sont donc pas tenus de désigner un DPO ».

2. **Le chemin est encore long vers la conformité**

Il n'est pas nécessaire de se prêter à de longs calculs pour constater que nombre d'acteurs publics n'ont toujours pas désigné de DPO, 6 ans après son entrée en vigueur.

On compte plus de 96 000 DPO désignés auprès des services de la CNIL. Si beaucoup d'acteurs publics de grande taille (ministères, établissements publics nationaux) ou de taille intermédiaire (collectivités territoriales, établissements publics locaux) ont désigné un DPO, tel n'est pas le cas des plus petites structures.

Combien, parmi les 34 527 communes de moins de 20 000 habitants, ou parmi les acteurs publics locaux tels que les CCAS, lycées, collèges ou écoles, ont-ils désigné un DPO ? La réponse se trouve dans la liste des DPO accessible en open data.

3. **La désignation d'un DPO est une exigence du RGPD, mais il en est une autre toute aussi importante : le DPO doit disposer des compétences nécessaires pour assurer et contrôler la mise en œuvre du RGPD.**

Or là encore, si de nombreux acteurs publics ont désigné un DPO, nombreux sont ceux qui ont été désignés par obligation et sans les moyens associés.

Le CEPD a d'ailleurs publié le 17 janvier son second rapport sur les DPO en pointant un certain nombre de manquements et en émettant des recommandations.

Le plan d'actions : un exercice imposé pour les autorités et organismes publics

- **Action 1 – Désigner un DPO en répondant aux questions de l'annexe 1 du guide de la CNIL relatif au délégué à la protection des données**

Il faut rappeler qu'au besoin les autorités publiques ou organismes publics « de même type, contenu de leur structure organisationnelle et de leur taille » peuvent désigner un seul et même DPO. Il leur est également possible de désigner un DPO externalisé si les compétences internes font défaut.

- **Action 2 – Rédiger une lettre de mission**

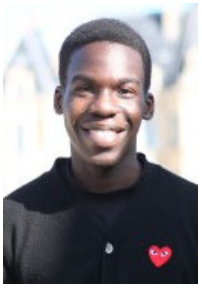
Même si une lettre de mission n'est pas imposée par le RGPD (sauf dans le cas d'une externalisation où la rédaction d'une convention s'impose) la CNIL propose toujours dans son guide, un modèle de lettre de mission. Cette lettre s'avère importante aussi bien pour cadrer la mission du DPO que pour rappeler les obligations de celui qui l'a désigné.

- **Action 3 – Procéder à un audit de conformité**

Désigner un DPO est une exigence légale, mais il importe que celui-ci sache précisément quel est le niveau de maturité de l'établissement dont il est supposé assurer et contrôler la conformité. Seul un audit est de nature à permettre d'identifier les éventuelles non conformités et le plan de remédiation associé.

Vos experts IP/IT

Eric Barbry
Avocat associé
ebarbry@racine.eu



Neldé Kossadoum
Juriste