



VOS ACTIVITÉS • JANVIER 2022

# Quelle est l'autorité de protection des données compétente pour votre entreprise ?

## Ce que vous devez savoir.

L'application du Règlement Général sur la Protection des Données ('RGPD') est assurée par les autorités de contrôle nationales. Bien qu'il ait été initialement proposé de créer une autorité de contrôle européenne, les États membres ne sont pas parvenus à un accord politique à cet égard.

Pour les entreprises actives dans plusieurs États membres de l'Espace économique européen ('EEE'), la question se pose immédiatement de savoir quelle autorité de contrôle nationale est compétente. Ceci doit être vérifié par les entreprises (de manière proactive) afin de (i) pouvoir notifier leur délégué à la protection des données ('DPO') à la ou aux autorité(s) adéquate(s), (ii) pouvoir signaler correctement les violations de données et (iii) être conscient de quelle autorité contacter dans le cadre d'une consultation préalable pour les activités de traitement comportant un risque élevé. La détermination de la ou des autorité(s) de contrôle nationale(s) compétente(s) n'est donc pas quelque chose à remettre à plus tard, mais fait partie intégrante d'une bonne conformité au RGPD.

Lorsqu'il y a des traitements transfrontaliers, et donc que plusieurs autorités de contrôle nationales sont impliquées (article 4, paragraphe 22 du RGPD), le RGPD prévoit un "mécanisme de guichet unique". Sur la base de ce système, une autorité doit être désignée comme "autorité chef de file" qui est en principe seule compétente pour le(s) traitement(s) concerné(s). Le Comité Européen de la Protection des Données ('CEPD') a publié des [lignes directrices](#) pour déterminer cette "autorité chef de file". Il n'en demeure pas moins que cette autorité chef de file doit coopérer avec les différentes autorités de contrôle concernées conformément au mécanisme de coopération prévu à l'article 60 du RGPD.

Le mécanisme de guichet unique ne rentre en jeu que si l'entreprise concernée a au moins un établissement dans l'EEE. Lorsqu'une entreprise n'a pas d'établissement dans l'EEE, mais relève néanmoins du champ d'application territorial du RGPD (par exemple, parce qu'elle offre ses biens et services à des personnes se trouvant dans l'EEE), toutes les autorités de contrôle de tous les États

## • • • contrast

membres où l'entreprise opère, sont compétentes.

## Ce que vous devez faire.

Vous devez d'abord déterminer si votre entreprise a des **activités de traitement transfrontalières**.

C'est le cas lorsque votre entreprise a des établissements dans plusieurs États membres de l'EEE qui traitent des données à caractère personnel. Des activités de traitement transfrontalières existent également lorsque votre entreprise est basée dans un seul État membre de l'EEE, mais que ses activités de traitement concernent des personnes dans plusieurs États membres de l'EEE (par exemple, parce que votre entreprise offre des biens ou des services dans des États membres de l'EEE autres que celui où elle est établie).

Par conséquent, si votre entreprise n'est établie que dans un État membre de l'EEE et que ses activités de traitement ne concernent que des personnes dans cet État membre, seule l'autorité de contrôle de cet État membre est (en principe) compétente. C'est l'autorité de contrôle vers laquelle votre entreprise doit se tourner, par exemple, pour notifier son DPO.

En revanche, si votre entreprise exerce des activités de traitement transfrontalières, vous devez déterminer **l'autorité chef de file** conformément au mécanisme de guichet unique. L'autorité de contrôle de l'EEE où votre entreprise a son établissement principal est l'autorité chef de file.

Si vous êtes un **responsable du traitement**, il s'agit du lieu de votre administration centrale dans l'EEE, à moins que les décisions quant aux finalités et aux moyens du ou des traitements sont prises et mises en œuvre par un autre établissement dans l'EEE. Plus précisément, vous devez donc examiner où les décisions concernant les différentes activités de traitement sont prises. Prenons l'exemple d'un groupe d'entreprises dont l'administration des RH est centralisée au siège de Bruxelles et dont les filiales en Suède et en Espagne sont responsables de tout le marketing au niveau local. Dans cet exemple, l'autorité de contrôle belge sera l'autorité chef de file pour les traitements liés aux RH et les autorités de contrôle suédoises et espagnoles respectivement pour les traitements de marketing effectués par les filiales suédoises et espagnoles.

Il est possible que l'établissement principal de votre entreprise soit situé en dehors de l'EEE, mais qu'elle ait des établissements locaux dans l'EEE. Dans ce cas, le CEPD recommande de désigner comme établissement principal (aux fins du RGPD) l'établissement dans l'EEE qui est chargé de la mise en œuvre des décisions relatives à l'activité de traitement, qui en assume la responsabilité et qui dispose de ressources suffisantes pour le faire. Sans quoi il ne peut y avoir d'autorité chef de file et le mécanisme de guichet unique ne peut pas rentrer en jeu.

Pour les **sous-traitants**, le régime en place est quelque peu différent. Pour les opérations de traitement

## • • • contrast • • • •

effectuées par votre entreprise en tant que sous-traitant, l'établissement principal est le lieu de votre administration centrale dans l'EEE ou, si vous ne disposez pas d'une administration centrale dans l'EEE, l'établissement dans l'EEE où se déroule l'essentiel de vos activités de traitement.

Enfin, dans le cadre d'une **activité de traitement conjointe**, il est important de convenir de l'établissement qui sera considéré comme établissement principal. Il doit s'agir d'un établissement qui exécute la décision à l'égard de tous les responsables conjoints du traitement.