

ARTICLE

ANTICIPER

DIRECTIVE NIS 2 | IA ACT | RGPD

RÈGLEMENTS ET DIRECTIVES (UE)





Calendrier des différentes normes européennes

Alors que le RGPD s'applique depuis plus de 5 ans, la nouvelle directive 2022/2555 « NIS II » sera applicable à partir du **18 octobre 2024**.

Le règlement sur l'intelligence artificielle « IA Act », quant à lui devrait être applicable **24 mois après son entrée en vigueur**.





La directive NIS 2 et le RGPD

Certaines dispositions de la directive NIS II s'imbriquent avec celles du RGPD de sorte que les acteurs concernés doivent **anticiper les obligations et les enjeux croisés** que recouvrent ces textes.

Depuis l'entrée en vigueur du RGPD en 2018, les entités ont l'obligation de prendre des mesures techniques et organisationnelles appropriées pour garantir la sécurité des données personnelles. La directive NIS II prévoit une obligation connexe concernant la cybersécurité des réseaux et des systèmes d'informations, qui inclut la prise de **mesures techniques, opérationnelles et organisationnelles** fondées sur le risque.





La directive NIS 2 et le RGPD

Il faut souligner que les exigences de cybersécurité prévues par NIS II prévoient que : « *La sécurité des réseaux et des systèmes d'information devrait inclure la sécurité des données stockées, transmises et traitées* ».

En effet, ces mesures favoriseront le respect des obligations de sécurité des données personnelles, prévues par l'**article 32 du RGPD**, en renforçant les mesures techniques des entités.





La directive NIS 2 et le RGPD

De plus, la directive prévoit une politique d'**analyse des risques et de sécurité** qui peut s'avérer pertinente à conjuguer avec une **analyse d'impact relative à la protection des données** telle que prévue par l'article 35 RGPD.

En effet, sachant que le PIA contient une partie technique sur les risques sur la sécurité des données et permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données, ces mesures pourraient tout à fait s'intégrer aux autres mesures de cybersécurité.





Le règlement IA Act et le RGPD

L'IA Act s'inscrit dans le **prolongement** du RGPD. Il est intéressant de noter que ces règlements ont une base juridique commune « **protection des données** ».

Ainsi, lorsque les systèmes d'IA devront prendre en compte le droit de la protection des données personnelles et garantir leur efficacité au travers d'outils, comme les analyses d'impact (**PIA**).





Le règlement IA Act et le RGPD

Ce règlement devra permettre de lutter contre les biais et discriminations qui pourra résulter du traitement de **données sensibles** et devra s'imbriquer avec le RGPD sur la question de la **prise de décision automatisée**. En effet, le RGPD prévoit qu'une « *personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé...* » et si ce n'est pas le cas, elle peut disposer du **droit d'obtenir une intervention humaine**.

L'IA Act ira dans ce sens en prévoyant un rôle de supervision par un « **contrôle humain** » explicitement consacré. Cela aura vocation à prévenir ou réduire au minimum les risques liés à l'utilisation d'une IA à haut risque. Enfin, il faut noter que le règlement IA Act se fonde sur une **approche sur les risques**.