RGPD & norme ISO 27001

écrit par Marine de la Clergerie | 01/08/2024
L'article 32 du RGPD dispose que

> *Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque*

Selon l'ISO

> *La conformité à ISO/IEC 27001 signifie qu'une organisation ou une entreprise a mis en place un système pour gérer les risques liés à la sécurité de ses données ou des données qu'elle est amenée à traiter, et que ce système est conforme aux bonnes pratiques et principes énoncés dans cette Norme internationale.*

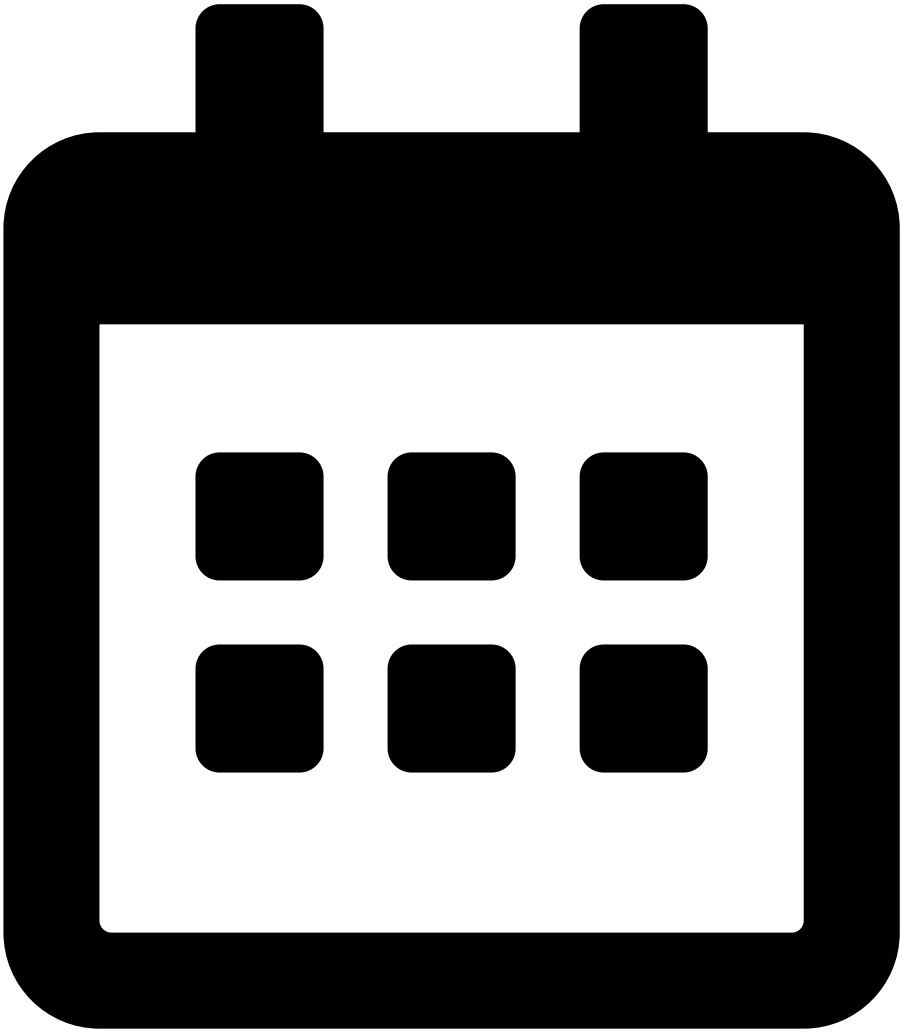
Toutefois, la certification ISO/IEC 27001 ne permet pas en tant que telle de répondre aux exigences du RGPD; en effet selon l'autorité italienne de protection des données:

- Cette certification ne fait pas, pour l'instant, partie de celles prévues par l'art. 42 du Règlement;
- Elle n'implique pas automatiquement le respect du RGPD en matière de mesures de sécurité;
- Elle garantit uniquement l'adoption des contrôles que l'organisation a identifiés et jugés adéquats sur la base de sur sa propre évaluation des risques.

Références:

- La norme: https://www.iso.org/fr/standard/27001
- La décision: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10002324

Marine de la Clergerie (Consultation, LinkedIn, Demande de devis) est avocat au Barreau de Toulouse. Elle intervient partout en France à distance et au sein de ses locaux situés 43 rue Achille Viadieu à Toulouse (métro Saint-Michel). Elle est spécialiste en droit du numérique et des communications, avec la qualification spécifique droit des données à caractère personnel. Elle dispose d'une expertise spécifique dans le domaine du droit des données à caractère personnel et exerce la fonction de DPO externe certifiée pour le compte de plusieurs sociétés.



Prendre RDV avec Me de la Clergerie pour un devis (gratuit)