LES FICHES RÉGLEMENTAIRES CLOUD TEMPLE

Le RGPD, en clair

LES FAITS

Le RGPD est un règlement européen adopté le 27 avril 2016 et entré en application le 25 mai 2018. Il fait l'objet de clarifications via des lignes directrices interprétatives et de décisions de la Cour de justice de l'Union européenne.

Il poursuit trois objectifs principaux : renforcer les droits des personnes sur leurs données à caractère personnel, responsabiliser les responsables de traitements et leurs sous-traitants, et harmoniser les règles pour favoriser un marché numérique unique des données.

CHAMPS D'APPLICATION

Le RGPD s'applique au traitement de données à caractère personnel, c'est-à-dire à toute opération portant sur des informations concernant une personne physique identifiée ou identifiable.

Il concerne les acteurs établis dans l'Union européenne, quel que soit le lieu du traitement, ainsi que les acteurs non établis dans l'UE lorsqu'ils ciblent des personnes se trouvant sur le territoire de l'Union européenne.

COMMENT SE METTRE EN CONFORMITÉ

Licéité, loyauté, transparence	Toute traitement doit être justifiée par une base légale claire (ex. consentement, contrat, obligation légale, intérêt légitime). Les personnes concernées doivent être informées de manière claire, complète et compréhensible.
Responsabilisation accrue des acteurs	Les responsables de traitement et leurs sous-traitants doivent mettre en œuvre une démarche de conformité proactive (« accountability ») par exemple : tenir un registre des traitements, réaliser d'analyses d'impact sur la vie privée (AIPD) dans les cas à risque, désigner un DPO dans certains cas, mettre en œuvre des mesures techniques et organisationnelles appropriées pour assurer la confidentialité, l'intégrité et la disponibilité des données.
Droits des personnes renforcés	Droit d'accès, de rectification, d'effacement, d'opposition, de portabilité, limitation du traitement, et droit à ne pas faire l'objet d'une décision automatisée.
Autorité de protection des données (APD)	En France, c'est la Commission nationale de l'informatique et des libertés (CNIL). Elle doit contrôler la conformité, informer, sensibiliser, accompagner les organismes dans la mise en conformité, recevoir et traiter les plaintes, sanctionner les manquements au RGPD et participer à la coopération européenne.
Notification des violations	Obligation de notifier la CNIL dans les 72h en cas de violation de données personnelles, et les personnes concernées si le risque est élevé.

L'ANALYSE

Giuliano Ippoliti,
directeur cybersécurité de Cloud Temple

« Le RGPD a constitué un tournant majeur pour la protection des données en instaurant un principe de responsabilisation. Désormais, chaque traitement doit être justifié, documenté et maîtrisé. Cette exigence de rigueur a érigé le règlement en standard de référence à l'échelle internationale. »

UNE POSSIBLE SIMPLIFICATION ?

La proposition de règlement "Digital Omnibus" pourrait entraîner des ajustements du RGPD, notamment en clarifiant certaines définitions, en réduisant les obligations pour les petits acteurs, et en facilitant l'utilisation des données pour l'intelligence artificielle et la recherche scientifique. Il ne s'agit toutefois que de pistes potentielles, dans l'attente d'une adoption formelle par les institutions de l'UE.

CLOUD TEMPLE
Innovative by design