

Des fiches pratiques sur le chiffrement et la sécurité des données en cloud



© 2024 Les Echos Publishing

Les entreprises doivent obligatoirement sécuriser la gestion des données personnelles qu'elles récupèrent, sous peine de sanctions prononcées par la CNIL. En 2022, près d'un tiers des sanctions visaient des manquements à cette obligation. Or, de plus en plus d'entreprises font appel à des fournisseurs de solutions informatique en nuage (cloud), ce qui ne les exonère pas de cette obligation. Elles sont donc amenées à s'interroger face aux nombreuses offres sur le marché avec des prestations différentes. Pour les aider dans leur choix et leur permettre de trouver l'approche en matière de sécurité la plus adaptée à leurs besoins, la CNIL vient de publier des fiches de conseils.

Des outils pour sécuriser le cloud

La [première fiche](#) est consacrée au chiffrement des données sur le cloud. Elle détaille les différents types de chiffrement (chiffrement au repos, chiffrement en transit, chiffrement en traitement, chiffrement de bout en bout...) et indique pour chacun les enjeux et problématiques spécifiques. La [deuxième fiche](#) s'intéresse aux outils pour sécuriser un service cloud. Sont ainsi passés en revue les différents produits de sécurité nécessaires pour sécuriser un service cloud, avec les points

de vigilance pour ces différents produits. D'autres fiches devraient suivre, toujours dans l'objectif de donner des clés de compréhension aux entreprises pour mieux choisir leurs solutions numériques.

www.cnil.fr/

© 2024 Les Echos Publishing