Sanction de la CNIL à l'encontre de CEGEDIM SANTÉ : une amende de 800 000€ pour des manquements en matière de protection des données de santé

La CNIL considère que les données collectées par CEGEDIM SANTÉ auprès de médecins sur leurs patients, chiffrées et rattachées à un identifiant unique, sont des données pseudonymes et non anonymes, en ce qu'elles sont susceptibles d'être réidentifiées par des moyens raisonnables. En collectant massivement ces données, la CNIL a notamment considéré que CEGEDIM SANTÉ exploitait un entrepôt de données de santé de manière illégale.

CEGEDIM SANTÉ développe et commercialise des logiciels de gestion destinés aux médecins. La CNIL a constaté que l'utilisation de l'un de ces logiciels par des médecins participant à un « observatoire », impliquait la transmission à CEGEDIM SANTÉ de données de santé non anonymisées, sans autorisation de la CNIL et leur fourniture ultérieure à des clients de CEGEDIM SANTÉ dans le but de réaliser des études et des statistiques.

La CNIL a constaté que la société collectait auprès de chaque médecin un grand nombre de données sur ses patients (dont l'année de naissance, le sexe, la catégorie socio-professionnelle, les allergies, les antécédents médicaux, la taille, le poids, le diagnostic, les prescriptions médicales, les arrêts de travail et les résultats d'analyse). Ces données sont chiffrées et rattachées à un identifiant unique pour chaque patient d'un même médecin et transmises à CEGEDIM SANTÉ, ce qui permet d'associer l'ensemble des données transmises concernant un patient et de reconstituer son parcours de soins auprès de ce médecin. La CNIL relève qu'il est possible d'isoler un individu dans la base de données de CEGEDIM SANTÉ puisque l'identifiant unique permet de le suivre au fil du temps et que la richesse des données collectées fait courir un risque encore plus important de levée du pseudonymat.

La CNIL en a conclu que ces données restaient susceptibles d'être réidentifiées par des moyens raisonnables et donc qu'elles ne sont pas anonymes mais pseudonymes. Elle en conclut que leur traitement est soumis au RGPD.

Or, les traitements réalisés CEGEDIM SANTÉ révèlent deux manquements au RGPD :

1. Un entrepôt de données de santé illégal

La CNIL considère que CEGEDIM SANTÉ a constitué un entrepôt de données de santé : elle a collecté de manière massive des données de santé de patients et de médecins, alimenté la base de données au fil de l'eau afin d'obtenir un volume important de données et mis à disposition des données à des clients qui réalisent des études et des statistiques dans le domaine de la santé.

Or, dans la mesure où la société traite des données de santé et qu'elle ne peut se prévaloir d'une des exceptions prévues à l'article 65 de la Loi Informatique et Libertés (notamment le recueil du consentement des personnes concernées), elle devait obtenir une autorisation de la CNIL pour pouvoir réaliser les traitements[1] ou respecter l'un de ses référentiels au regard de l'intérêt publics qu'ils représentent et adresser une déclaration de conformité à la CNIL[2]. CEGEDIM SANTÉ n'ayant pas respecté ces conditions, la CNIL a considéré qu'elle exploitait un entrepôt de données de santé de manière illégale.

2. Des manquements au principe de licéité des traitements

[1] Quelles formalités pour les traitements de données de santé ? | CNIL

[2] Traitements de données dans le domaine de la santé : les référentiels pour simplifier vos démarches | CNIL

Alors que l'assurance maladie a mis en place un téléservice nommé « HRi », permettant aux médecins de consulter l'historique des remboursements de leurs patients sur les douze derniers mois, la société a mis en place un système de collecte automatique des données du téléservice à l'occasion de la simple consultation de ces données par les médecins, sans offrir la possibilité d'empêcher cette collecte. La CNIL a jugé que cette pratique, qui permettait à CEGEDIM SANTÉ d'aspirer automatiquement les données du service contrevenait au principe de licéité prévu à l'article 5.1.a du RGPD, qui impose que les données personnelles soient traitées de manière licite, loyale et transparente.

La CNIL a sanctionné la société CEGEDIM SANTÉ à hauteur de 800 000€, en prenant en compte la gravité des manquements, le caractère sensible des données de santé en cause, et le volume important de données traitées. Cependant, la formation restreinte n'a pas prononcé d'injonction de mise en conformité puisque la société a depuis transféré la responsabilité du traitement des données à une autre entité du groupe.

Lien utile :

- Délibération SAN-2024-013 du 5 septembre 2024