Données de santé : sanction de 800 000 euros à l'encontre de la société CEGEDIM SANTÉ

12 septembre 2024

Le 5 septembre 2024, la CNIL a sanctionné la société CEGEDIM SANTÉ d'une amende de 800 000 euros, pour avoir notamment traité des données de santé sans autorisation.

Le contexte

La société CEGEDIM SANTÉ édite et vend des logiciels de gestion aux médecins de ville exerçant en cabinet et en centre de santé. Environ 25 000 cabinets médicaux et 500 centres de santé utilisent ces logiciels. Ils permettent aux médecins de gérer leur agenda, les dossiers de leurs patients et leurs prescriptions.

Les contrôles réalisés par la CNIL en 2021 ont notamment permis de révéler que, dans le cadre de l'utilisation de l'un de ses logiciels, la société avait traité sans autorisation des données de santé non anonymes, transmises à ses clients en vue de produire des études et des statistiques dans le domaine de la santé.

En conséquence, la formation restreinte – organe de la CNIL chargé de prononcer les sanctions – **a prononcé une amende de 800 000 euros à l'encontre de la société CEGEDIM SANTÉ**, au regard des capacités financières de la société, de la gravité des manquements retenus, du caractère massif du traitement et du fait que les données concernées sont des données de santé, donc des données sensibles.

Des données pseudonymes et non anonymes

Dans le cadre de son activité, la société propose à un panel de médecins utilisant l'un de ces logiciels d'adhérer à un « observatoire », les données alors collectées sont ensuite utilisées par des clients de la société CEGEDIM SANTÉ, notamment pour mener des études.

Les investigations menées par la CNIL ont permis d'établir que ces données n'étaient pas anonymes, mais uniquement pseudonymes, la réidentification des personnes concernées étant techniquement possible.

S'agissant d'un traitement de données personnelles, la société aurait dû disposer d'une autorisation de la CNIL pour les utiliser (article 66.III de la loi Informatique et Libertés).

Pour apprécier le caractère anonyme ou non des données traitées, la formation restreinte s'est attachée à déterminer **si les personnes concernées pouvaient être réidentifiées par des moyens raisonnables**, comme le prévoient notamment la jurisprudence de la Cour de justice de l'Union européenne et les travaux conduits par les autorités de protection des données au niveau européen (avis

05/2014 sur les techniques d'anonymisation du 10 avril 2014).

En pratique, la formation restreinte a relevé que la société CEGEDIM SANTÉ collectait de très nombreuses données sur les personnes concernées, telles que 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 étaient reliées à un identifiant unique pour chaque patient d'un même médecin, permettant de relier entre elles les données transmises successivement par un même médecin concernant ce même patient et de reconstituer ainsi son parcours de soins. Au vu de ces éléments, la formation restreinte a considéré qu'**il est possible d'isoler un individu au sein de la base de données** de la société et que la société **dispose de nombreuses informations particulièrement riches** le concernant, ce qui induit un **risque de réidentification.**

Dans ces conditions, compte tenu de l'existence de l'identifiant unique et de la profondeur des données collectées par la société – et en tenant également compte de la possibilité de combiner les données détenues par la société CEGEDIM SANTÉ avec des données détenues par des tiers – la formation restreinte a considéré que le risque que l'identité d'une personne puisse être retrouvée était trop élevé pour que les données traitées par la société soient considérées comme anonymes.

Dès lors, la formation restreinte a considéré que **les données traitées par la société CEGEDIM SANTÉ au moins jusqu'en 2022 (date de la fin des contrôles) étaient pseudonymes et non anonymes.**

Rappel

Si les données sont anonymes, alors elles ne sont pas des données personnelles : dans ce cas, la règlementation sur la protection des données n'est pas applicable.

À l'inverse, **si les données sont pseudonymes, alors la réglementation est applicable.**

Les manquements sanctionnés

Un manquement à l'obligation d'effectuer les formalités préalables dans le domaine de la santé (article 66 de la loi Informatique et Libertés)

La loi Informatique et Libertés (article 66.III) prévoit que les traitements de données personnelles dans le domaine de la santé ne peuvent être mis en œuvre qu'après autorisation de la CNIL ou à la condition d'être conformes à un référentiel mentionné (article 66.II).

La formation restreinte a considéré que la société ne s'est pas conformée à ces exigences alors qu'elle constituait un entrepôt de données de santé :

- **elle n'a formulé aucune demande d'autorisation auprès de la CNIL** permettant d'évaluer si le traitement en cause était nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique ou nécessaire à des fins de recherche scientifique ;
- **elle n'a pas adressé à la CNIL une déclaration de conformité à l'un de ses référentiels.**

Un manquement à l'obligation de traiter les données de manière licite (article 5.1.a du RGPD)

La formation restreinte a considéré que la société avait commis un manquement à l'article 5.1.a du RGPD concernant son utilisation du téléservice « HRi » mis en place par l'assurance maladie, qui permet d'accéder à l'historique des remboursements de santé effectués par l'assurance maladie pour un patient sur les douze derniers mois.

La formation restreinte a en effet constaté que la consultation des données issues de ce téléservice par un médecin membre de « l'observatoire » entraînait automatiquement leur téléchargement dans le dossier informatisé du patient, permettant dans le même temps leur aspiration par la société. La formation restreinte a considéré qu'**en ne prévoyant pas la possibilité que les données soient simplement consultées par les médecins sans entraîner une collecte automatique, la société n'avait pas traité les données de manière licite.**

Pour ces deux manquements, la formation restreinte a prononcé **une amende de 800 000 euros** à l'encontre de la société CEGEDIM SANTÉ.

La formation restreinte n'a pas prononcé d'injonction de mise en conformité dans la mesure où, depuis le mois de juillet 2024, la société n'est plus responsable du traitement, mais uniquement éditrice du logiciel en cause. Les données recueillies par les médecins ne transitent ainsi plus via la société CEGEDIM SANTÉ, mais alimentent désormais directement une base détenue par une autre société du groupe, qui est devenue responsable de ce traitement.

Pour approfondir

- La procédure de sanction
- Qu'est-ce ce qu'une donnée de santé ?
- Quelles formalités pour les traitements de données de santé ?
- Traitements de données de santé : comment faire la distinction entre un entrepôt et une recherche et quelles conséquences ?
- L'anonymisation des données personnelles

Textes de référence

- Article 66 de la loi Informatique et Libertés (autorisations en matière de santé)
- Article 5-1-a du RGPD (licéité du traitement)

Délibération

- Délibération de la formation restreinte n°SAN-2024-013 du 5 septembre 2024 concernant la société CEGEDIM SANTÉ - Légifrance