cnil.fr

Fuite de données de santé : sanction de 1,5 million d'euros à l'encontre de la société DEDALUS BIOLOGIE

4–5 minutes

Le 15 avril 2022, la formation restreinte de la CNIL a sanctionné la société DEDALUS BIOLOGIE d'une amende de 1,5 million d'euros, notamment pour des défauts de sécurité ayant conduit à la fuite de données médicales de près de 500 000 personnes.

Le 23 février 2021, une fuite de données massive concernant près de 500 000 personnes a été révélée dans la presse, qui mettait en cause la société DEDALUS. Les nom, prénom, numéro de sécurité sociale, nom du médecin prescripteur, date de l'examen mais aussi et surtout des informations médicales (VIH, cancers, maladies génétiques, grossesses, traitements médicamenteux suivis par le patient, ou encore des données génétiques) de ces personnes ont ainsi été diffusés sur internet.

Dès le 24 février 2021, la CNIL a effectué plusieurs contrôles, notamment auprès de la société DEDALUS BIOLOGIE qui commercialise des solutions logicielles pour des laboratoires d'analyse médicale.

En parallèle, la CNIL a saisi le tribunal judiciaire de Paris qui a bloqué l'accès au site sur lequel étaient publiées les données ayant fuité. Cette décision du 4 mars 2021 a permis de limiter les conséquences pour les personnes.

Sur la base des constatations effectuées lors des contrôles, la formation restreinte – organe de la CNIL chargé de prononcer les sanctions – a considéré que la société avait manqué à plusieurs obligations prévues par le RGPD, en particulier à l'obligation d'assurer la sécurité des données personnelles.

La formation restreinte a ainsi prononcé **une amende de 1,5 million d'euros** et a décidé de rendre publique sa décision. Le montant de cette amende a été décidé au regard de la gravité des manquements retenus mais également en prenant en compte le chiffre d'affaires de la société DEDALUS BIOLOGIE.

Les manquements sanctionnés

Un manquement à l'obligation pour le sous-traitant de respecter les instructions du responsable de traitement (article 29 du RGPD)

Dans le cadre de la migration d'un logiciel vers un autre outil, demandée par deux laboratoires utilisant les services de la société DEDALUS BIOLOGIE, cette dernière a extrait un volume de données plus important que celui requis.

La société a donc traité des données au-delà des instructions données par les responsables de traitement.

Un manquement à l'obligation d'assurer la sécurité des données personnelles (article 32 du RGPD)

De nombreux manquements techniques et organisationnels en matière de sécurité ont été retenus à l'encontre de la société DEDALUS BIOLOGIE dans le cadre des opérations de migration du logiciel vers un autre :

- absence de procédure spécifique pour les opérations de migration de données ;
- absence de chiffrement des données personnelles stockées sur le serveur problématique ;
- absence d'effacement automatique des données après migration vers l'autre logiciel ;
- absence d'authentification requise depuis internet pour accéder à la zone publique du serveur ;
- utilisation de comptes utilisateurs partagés entre plusieurs salariés sur la zone privée du serveur ;
- absence de procédure de supervision et de remontée d'alertes de sécurité sur le serveur.

Cette absence de mesures de sécurité satisfaisantes est l'une des causes de la violation de données qui a compromis les données médico-administratives de près de 500 000 personnes.

Un manquement à l'obligation d'encadrer par un acte juridique formalisé les traitements effectués pour le compte du responsable de traitement (article 28 du RGPD)

Les conditions générales de vente proposées par la société DEDALUS BIOLOGIE et les contrats de maintenance transmis à la CNIL ne contiennent

pas les mentions prévues par l’article 28-3 du RGPD.