J&Actualités

RGPD – Avril 2022

J&A JOFFE & ASSOCIÉS

Sanction CNIL : Un sous-traitant condamné à une amende de 1,5 million d'euros à la suite d'une fuite massive de données.

Dans une décision remarquée du 15 avril 2022, la Commission Nationale de l'Informatique et des Libertés (CNIL) a infligé à l'éditeur de logiciel Dedalus Biologie **une amende d'1,5 million d'euros** pour manquement à plusieurs dispositions du Règlement général pour la protection des données (« RGPD »). L'autorité administrative a également prononcé **la publication de la sanction sur son site et sur le site de Légifrance**.

Cette condamnation s'inscrit à la suite de la fuite massive de données personnelles, dont des données de santé, qui a concerné plusieurs laboratoires français ayant eu recours aux services du sous-traitant Dedalus. Le journal Libération, qui avait révélé l'affaire le 21 avril 2021, indiquait que les données personnelles de 500 000 patients avaient été rendues accessibles gratuitement sur le darknet.

Les manquements reprochés à la société Dedalus étaient les suivants :

i. Manquement à l'obligation d'assurer la sécurité des données personnelles (article 32 du RGPD) ;
ii. Manquement à l'obligation de suivre les instructions de ses clients, responsables de traitement (article 28 du RGPD) ;
iii. Absence d'accords sur la protection des données (article 28 du RGPD).

Cette décision est inédite dans la mesure où c'est la première fois que la CNIL condamne uniquement un sous-traitant – et non le responsable de traitement – en raison d'un manquement à son obligation de sécurité. En effet, conformément à l'article 32 de RGPD, l'obligation de sécurité incombe tant au responsable de traitement qu'au sous-traitant. Dans une décision du 27 janvier 2021 , la CNIL avait condamné le responsable de traitement et son sous-traitant au paiement de sanctions administratives pour des montants différents selon leur niveau de responsabilité.

Que retenir de cette sanction ?

La sécurité des données est au cœur du RGPD et concerne tant le responsable de traitement que le sous-traitant, qui est exposé à des risques de sanctions CNIL au même titre que son donner d'ordre. La CNIL publie régulièrement les sanctions sur son site internet. Les risques en termes de e-reputation – en plus des risques juridiques et financiers – sont donc bien réels et peuvent être plus néfastes que les sanctions financières.

[1] Délibération de la formation restreinte n° SAN-2022-009 du 15 avril 2022 concernant la société DEDALUS BIOLOGIE
[2] https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant#:~:text=La%20formation%20restreinte%20de%20la,web%20du%20responsable%20de%20traitement

JOFFE & ASSOCIÉS

Sanction CNIL : Un sous-traitant condamné à une amende de 1,5 million d'euros à la suite d'une fuite massive de données.

Le responsable de traitement de traitement doit :

- vérifier que des accords sur la protection des données conformes aux dispositions de l'article 28 du RGPD ont été signés avec chacun de ses sous-traitants et que ces accords détaillent suffisamment les mesures de sécurité mises en place ;

- évaluer le caractère suffisant des garanties fournies par le sous-traitant avant d'entrer en relation contractuelle avec celui-ci. A ce titre, il est recommandé d'auditer le sous-traitant et de lui demander a minima de fournir une documentation de sécurité.

Le sous-traitant doit quant à lui :

- vérifier que des mesures de sécurité technique et organisationnelle adaptées aux risques encourus (notamment en cas de traitement de données sensibles) ont été mises en place ;

- documenter les procédures de sécurité mises en place (création d'un plan d'assurance sécurité, politique de gestion des incidents, etc.).

Le département IT/RGPD du cabinet Joffe & Associés se tient à votre disposition pour vous accompagner dans votre mise en conformité RGPD.

Emilie DE VAUCRESSON
Associée
edevaucresson@joffeassocies.com

Amanda DUBARRY
Avocate
adubarry@joffeassocies.com