cnil.fr

# Violation de données : sanction de 180 000 euros à l'encontre de la société SLIMPAY

4–5 minutes

---

Le 28 décembre 2021, la formation restreinte de la CNIL a sanctionné la société SLIMPAY d'une amende de 180 000 euros notamment pour avoir insuffisamment protégé les données personnelles des utilisateurs et ne pas les avoir informés d'une violation de données.

## Le contrôle et la sanction de la CNIL

La société SLIMPAY est un établissement de paiement agréé qui propose notamment des solutions de paiements récurrents à ses clients. Courant 2015, elle a effectué un projet de recherche interne, lors duquel elle a utilisé les données personnelles contenues dans ses bases de données. Lorsque le projet de recherche s'est terminé en juillet 2016, les données sont restées stockées sur un serveur, qui ne faisait pas l'objet d'une procédure de sécurité particulière et qui était librement accessible depuis Internet. Ce n'est qu'en février 2020 que la société SLIMPAY s'est aperçue de la violation de données, qui a concerné environ 12 millions de personnes.

La CNIL a effectué un contrôle auprès de la société SLIMPAY en 2020. Elle a constaté plusieurs manquements concernant le traitement de données personnelles des clients.

Sur la base de ces éléments, la formation restreinte – organe de la CNIL chargé de prononcer les sanctions – a effectivement considéré que la société avait manqué à plusieurs obligations prévues par le RGPD.

Les personnes concernées par la violation de données se trouvant dans plusieurs pays de l'Union européenne, la formation restreinte a coopéré avec les autorités de contrôle de quatre pays (Allemagne, Espagne, Italie et Pays-Bas).

À l'issue de ce processus, la formation restreinte a prononcé **une amende de 180 000 euros** et a décidé de rendre publique sa décision.

## Les manquements constatés

**Un manquement à l’obligation d’encadrer, par un acte juridique formalisé, les traitements effectués par un sous-traitant (article 28 du RGPD)**

Certains des contrats conclus par la société SLIMPAY avec ses prestataires ne contiennent pas toutes les clauses permettant de s’assurer que ces sous-traitants s’engagent à traiter les données personnelles en conformité avec le RGPD (l’article 28-3 du RGPD liste plusieurs obligations devant figurer dans les contrats). Certains des contrats ne contiennent même aucune de ces mentions.

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

La formation restreinte a relevé que l’accès au serveur en question ne faisait l’objet d’aucune mesure de sécurité : il était possible d’y accéder à partir d’Internet entre novembre 2015 et février 2020. Les données d’état civil (civilité, nom, prénom), les adresses postales et électroniques, les numéros de téléphone et des informations bancaires (BIC/IBAN) de plus de 12 millions de personnes ont ainsi été compromises.

Si la société s’est défendue en indiquant que les données n’ont probablement pas été utilisées frauduleusement, la CNIL a tout de même retenu un manquement à l’article 32 du RGPD, considérant que l’absence de préjudice avéré pour les personnes concernées n’a pas d’incidence sur l’existence du défaut de sécurité.

**Un manquement à l’obligation d’information d’une violation de données personnelles aux personnes concernées (article 34 du RGPD)**

La CNIL a considéré que, compte tenu de la nature des données personnelles (comportant notamment des informations bancaires), du volume de personnes concernées (plus de 12 millions), de la possibilité d’identifier les personnes touchées par la violation à partir des données accessibles et des conséquences possibles pour les personnes concernées (risques d’hameçonnage ou d’usurpation d’identité), le risque associé à la violation devait être considéré comme élevé. La société aurait donc dû informer toutes les personnes concernées, ce qu’elle n’a pas fait.