

La fuite de données de l'application Kooma

Le mardi 3 mars 2026 à 9 h, l'équipe technique de Kooma constate qu'un accès non autorisé a permis de copier une partie de la base des utilisateurs de l'application de covoiturage (nom, adresse électronique, trajets habituels). Mme Diallo, cofondatrice, vous demande, en tant qu'assistant(e) de direction, de chiffrer l'ampleur de l'incident, les délais à respecter et le coût de sa gestion (documents 1 et 2).

Une semaine plus tard, le 10 mars, un utilisateur demande par courriel la copie de toutes les données que Kooma détient sur lui.

Document 1 : données de l'incident

Élément	Contenu
Base de données	48 000 comptes utilisateurs
Comptes copiés	15 % de la base
Détection	mardi 3 mars 2026 à 9 h
Chiffre d'affaires 2026 de Kooma	2 400 000 €
Comptes inactifs depuis plus de trois ans	3 100 (non supprimés malgré la politique de conservation de trois ans)

Document 2 : coûts de gestion et rappels

Élément	Contenu
Courriel d'information	0,02 € par personne concernée
Expert en sécurité	3 jours à 950 € par jour
Temps interne	40 h à 32 € de l'heure

Élément	Contenu
Notification à la CNIL	dans les 72 heures suivant la découverte
Réponse à une demande d'accès	dans le mois suivant la réception
Amende administrative	jusqu'à 20 M€ ou 4 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu

Annexe 1 (arrondir les montants à deux décimales, les pourcentages à une décimale)

Question	Réponse
Nombre de personnes concernées par la violation	_____
Délai maximal de notification de la violation à la CNIL (heures)	_____

Montant de 4 % du chiffre d'affaires annuel de Kooma (€)	_____
Plafond de l'amende administrative encourue par Kooma (€)	_____
Coût de l'information individuelle des personnes concernées (€)	_____
Coût total de la gestion de l'incident (€)	_____
Part des comptes inactifs depuis plus de trois ans dans la base (%)	_____
Nombre de jours dont dispose Kooma pour répondre à la demande d'accès reçue le 10 mars	_____

Questions d'analyse

- Les personnes concernées doivent être informées directement de la violation :
- ☐ Jamais : seule la CNIL est informée
 - ☐ Lorsque la violation présente un risque élevé pour leurs droits et libertés, ce qui est le cas ici (adresses et trajets habituels)
 - ☐ Uniquement si elles en font la demande

L'hébergeur des serveurs de Kooma, qui stocke les données pour son compte, est :

- ☐ Le responsable du traitement
- ☐ Un tiers sans obligation
- ☐ Un sous-traitant, lié par un contrat qui fixe ses obligations de sécurité

Pour envoyer des offres commerciales par courriel aux utilisateurs, la base légale la plus sûre est :

- ☐ Le consentement préalable, libre et spécifique de l'utilisateur
- ☐ L'intérêt légitime de Kooma, sans information
- ☐ L'obligation légale