

Accès illégitime à un espace personnel en ligne : comment réagir ?

19 avril 2023

Régulièrement, la CNIL communique sur des violations de données typiques inspirées d'incidents réels qui lui sont notifiés. Cette publication a pour objectif de permettre à tous les professionnels de comprendre et de prévenir les risques d'accès accidentel à des données par d'autres personnes que les personnes légitimes.

ACCÈS AUX DONNÉES D'AUTRES INDIVIDUS DEPUIS UN ESPACE PERSONNEL, COMMENT RÉAGIR ?

Ce matin, Armand se connecte au portail citoyen de sa commune pour réserver le centre de loisirs.



Mais c'est le dossier et les données personnelles d'une autre famille qui apparaissent !
Après plusieurs reconnections, le problème persiste.

Armand envoie un courriel explicatif de la situation via le formulaire de contact de la mairie.



La réclamation arrive jusqu'à Clémence, la RSSI de la ville.



Clémence démarre son investigation et comprend que l'incident provient d'une anomalie informatique.



Elle contacte l'équipe en charge des développements et documente l'incident en violation de données personnelles.



Découvrir toute l'histoire de Clémence et Armand

Après analyse des traces applicatives il semblerait qu'une trentaine de personnes aient été touchées dans le même cas qu'Armand.

Comment limiter ce risque ?

Pour éviter que votre début de semaine soit comme celui de Clémence et de sa commune, **n'attendez pas qu'un problème soit signalé par un usager** et suivez ces bonnes pratiques :

1. Mettre en œuvre les bonnes pratiques de développements de projet web ou applicatif

✓ Réaliser les développements en conformité avec le RGPD.

✓ Tester vos applications en incluant de vérifier la sécurité des données traitées.

✓ Compte tenu de la présence de données personnelles, notamment financières, la commune informe la CNIL ainsi que les personnes concernées par l'incident.

✓ Mettre en place un dispositif de conservation de données de journalisation des actions d'accès, création, modification et suppression sur un traitement de données personnelles.

3. Désigner un(e) délégué(e) à la protection des données

✓ Désigner un délégué à la protection des données : obligatoire dans certains cas et notamment pour les collectivités et recommandé dans tous les cas.

Pour comprendre tous les enjeux de la cybersécurité sur les données personnelles, la CNIL propose de nombreux conseils sur son site web et dans le guide de la sécurité des données.

Texte référence

*L'anomalie est finalement corrigée.
Après plusieurs tests, l'accès au portail est de nouveau possible.*

Pour approfondir

> Les violations de données personnelles
> Tous les contenus sur la cybersécurité

Texte référence

Les textes de référence

> Articles 33 du RGPD (sécurité du traitement)
> Article 34 du RGPD – Communication d'une violation de données aux personnes





Consciente des enjeux liés aux données personnelles et afin de respecter le RGPD, la commune désigne un délégué à la protection des données auprès de la CNIL. Elle pourra ainsi mieux gérer ce genre d'incident.

CNIL.