Madame, Monsieur,

Nous vous informons que l'incident de sécurité survenu récemment chez notre ancien partenaire tiers payant, Almerys, a concerné certaines de vos données personnelles.

A ce titre, en tant qu'ancien adhérent, certaines de vos données personnelles ainsi que celles de vos éventuels bénéficiaires ont été exposées.

Les investigations réalisées ont permis de confirmer que cet incident résulte de l'utilisation non autorisée d'un compte gestionnaire ayant permis l'accès au portail dédié aux demandes de prises en charge.

Les catégories de données concernées sont :

- Les données d'identification (nom, prénom, date de naissance, rang de naissance) ;
- Le numéro de sécurité sociale ;
- Des informations liées à votre contrat (nom de l'organisme complémentaire, numéro de contrat ainsi que dates de début et de fin de couverture).

Les investigations n'ont pas mis en évidence la compromission de données bancaires, de données de santé, de remboursements, d'adresses postales, de numéros de téléphone ou d'adresses électroniques.

Dès qu'Almerys a pris connaissance de cet acte de violation, une déclaration a été réalisée auprès des autorités compétentes (notamment CNIL).

Plusieurs mesures de sécurisation ont été mises en œuvre afin de contenir l'incident et d'en limiter les conséquences :

- Fermeture du portail dès la connaissance de l'incident ;
- L'ensemble des comptes gestionnaire a été désactivé puis réinitialisé ;
- Une cellule de crise a été activée afin de coordonnées les investigations techniques et les mesures de remédiation.

Depuis, plusieurs mesures de sécurité complémentaires ont été mises en œuvre, notamment :

- Le renforcement des contrôles d'accès aux services concernées ;
- Le déploiement progressif d'un dispositif d'authentification multi facteur ;
- Le renforcement des dispositifs de supervision et de détection des comportements anormaux ;
- L'automatisation des mesures complémentaires de surveillance du trafic et des accès ;
- Renforcement des règles d'accès aux données consultables depuis le portail

Nous attirons votre attention sur le fait que ces données peuvent faire l'objet d'une exploitation sous la forme de campagnes de phishing ou d'usurpation d'identité.

Dans ce contexte, nous vous invitons à redoubler de vigilance dans les prochaines semaines concernant toutes communications que vous pourriez recevoir et d'adopter les bonnes pratiques suivantes :

- Pensez à changer régulièrement le mot de passe de vos espaces clients et boîtes mails ;
- Ne transmettez jamais votre identifiant et votre mot de passe par email, SMS ou par téléphone ;
- Vérifiez bien l'identité de l'expéditeur de mails ou sms avant de cliquer sur une pièce jointe ou un lien ;
- Ne cliquez pas sur les liens directement fournis dans les communications que vous pourriez recevoir et connectez-vous sur les sites web de vos services habituels ;
- Signalez toute anomalie en lien avec vos remboursements ou tentative de contact liée à votre contrat santé.

Pour toute question, vous pouvez contacter notre délégué à la protection des données à l'adresse suivante : info.cnil@klesia.fr

Mutuelle Valeo