MINISTÈRE
DES TRANSPORTS
Liberté
Égalité
Fraternité

dgac
DSAC

Madame, Monsieur,

Nous vous informons que le site internet de paiement des redevances de la DSAC a été victime d'une cyberattaque du 5 au 9 novembre 2026.

Cet accès non-autorisé aux données collectées dans le cadre du paiement des redevances de la DSAC a conduit à la fuite des données relatives à l'ensemble des comptes ainsi qu'à toutes les personnes ayant passé une commande sans créer de compte.

La cyberattaque a été stoppée et des mesures ont été prises pour permettre la réouverture du site internet de paiement des redevances en toute sécurité.

Dès que le sous-traitant de la DGAC a eu connaissance de cette cyberattaque, ses serveurs ont été éteints et des mesures ont été prises pour garantir l'efficacité du chiffrement du site internet. Un audit du code a été diligenté.

Les données concernées sont celles :

- **Des titulaires de compte** (civilité, nom, prénom(s), date de naissance, genre, numéro de TVA, mot de passe crypté et date de création du compte, entreprise, adresse postale, numéro de téléphone, numéro de téléphone portable, numéro de fax) ;
- **Des personnes abonnées à la newsletter** (adresse mail) ;
- **Des personnes ayant consulté la plateforme** (produits indiqués en favoris, date de dernière connexion, informations liées à un panier en cours – nom et adresse saisis) ;
- **Des personnes ayant effectué des achats sur la plateforme** (adresse mail, nom, prénom, date de naissance, adresse IP utilisée pour la commande, numéro, date, montant et contenu des commandes, coordonnées de commande).

  En outre, cela concerne également certaines données de paiement (type de carte bancaire, numéro partiel de la carte bancaire, date d'expiration de la carte, identifiant de transaction SystèmPay, cryptogramme, titulaire de la carte, résultat du paiement – contrôle de sécurité lié à la carte).

Toutefois, nous souhaitons vous assurer qu'aucune donnée bancaire complète n'a été concernée par cette fuite de données. Les informations liées à la carte bancaire sont partielles et ne peuvent donc être utilisées, six des seize chiffres de la carte bancaire n'étant pas enregistrés.

Quand bien même la clé de chiffrement des mots de passe a été renouvelée, nous vous invitons à modifier votre mot de passe sur le site internet de paiement des redevances.

En cas de suspicion d'utilisation frauduleuse de vos données (spams par mail et SMS, lien à cliquer, demande de communication de données confidentielles), nous vous conseillons de vérifier l'authenticité de l'expéditeur et de le signaler sur la plateforme : www.cybermalveillance.gouv.fr.