DSP2, authentification forte : quelle règlementation ? (septembre 2024)

Les associations qui encaissent des cotisations, des dons ou qui réalisent des paiements par carte bancaire sur internet sont concernées.

Quelle est la réglementation en vigueur ?

La DSP2 (Directive sur les services de paiement) impose l'authentification forte à chaque transaction électronique (paiement en ligne). La mise en place de la directive DSP2 doit permettre de sécuriser les paiements et de favoriser l'innovation.

Qu'est-ce que la DSP2 ?

La DPS2 s'applique depuis le 13 janvier 2018.
Elle impose que soient accessibles, gratuitement, les données des comptes de paiement des clients, dans le cadre de deux activités nouvelles :

- **le service d'information sur les comptes** : c'est un service d'agrégation de données fournissant au client titulaire de comptes de paiement, dans un ou plusieurs établissements, des informations consolidées ;
- **le service d'initiation de paiement** : il permet à un prestataire de services de paiement de transmettre un ordre de paiement, au nom et pour le compte du client, à l'établissement teneur de compte.

Depuis le 15 mai 2021, les paiements en ligne font l'objet d'une authentification forte.

Plusieurs services en ligne sont aujourd'hui dans l'obligation d'appliquer la DSP2.
C'est par exemple le cas des banques, des e-commerçants ou encore des prestataires de services de paiement. Cela se traduit par la mise en place du 3DSecure V2, une sécurité qui oblige à confirmer auprès de votre banque que vous êtes bien à l'origine d'un achat réalisé sur Internet.
Les e-commerçants peuvent, s'ils le souhaitent, faire une demande d'exemption pour les transactions inférieures à 30 €. Dans ce cas, l'authentification forte pourra ne pas être demandée.

Qu'est-ce que l'authentification forte ?

L'authentification forte est une procédure de vérification de l'identité de la personne qui réalise l'opération de paiement en ligne.
Elle demande que les opérations de paiement en ligne soit vérifié avec au moins 2 des 3 éléments suivants :

- un élément que seule la personne connaisse (mot de passe, code, etc.) ;
- un élément que seule la personne possède (téléphone mobile, carte à puce, etc.) ;
- une caractéristique personnelle (empreinte digitale, reconnaissance vocale, etc.).

Pour les personnes qui ne possèdent pas de smartphone et qui ne peuvent donc pas installer d'applications mobiles, elles se verront proposer plusieurs solutions comme l'envoi d'un code unique par SMS ou l'utilisation d'un dispositif physique mis à disposition par la banque.

Bon à savoir
Dans le cadre des paiements sur internet, **le protocole 3DSecure doit être utilisé** pour permettre de réaliser cette authentification forte.

Qu'est-ce que le 3DSecure ?

Le système 3D Secure est un système de sécurisation des paiements en ligne, créé par les émetteurs internationaux Visa et MasterCard et mis en place en France en 2008. Il s'agit d'une procédure d'authentification du porteur de la carte, pour s'assurer que c'est bien lui qui effectue un paiement sur internet.
Cette procédure est réalisée en mettant en relation d'une part, le marchand avec son Prestataire de Service de Paiement (PSP), et d'autre part, le PSP avec l'Access Control Server (ACS) de la banque émettrice de la carte du porteur, via le Directory Server du schème d'émission de la carte (Mastercard, Visa, CB, ...).

Ce protocole sécurisé de paiement sur Internet limite les risques de fraude sur Internet, liés à l'utilisation frauduleuse de numéros de carte de paiement et **sécurise** commerçants, associations et consommateurs (particuliers, adhérents, donateurs...)

ATTENTION A défaut de ne pas être authentifiées par le protocole 3DS ou 3DSecure2, les transactions sont refusées.

Rappel des points de vigilances pour les associations

- Si l'association paye par carte bancaire sur internet, le porteur de la carte bancaire de l'association devra s'authentifier.
- Si l'association encaisse des paiements (cotisations, dons...) par carte bancaire, le payeur (adhérents, donateurs...) devra s'authentifier pour que son paiement puisse s'effectuer.
- Si l'association n'a pas mis en place en place de solutions de protocole sécurisé de paiement sur internet, les transactions seront refusées par l'établissement bancaire.

Ce qui n'est pas sans impacts pour les associations : perte de ressources, frais concernant les refus des opérations, temps passé auprès du prestataire informatique ou de la banque, réclamation à gérer de la part des adhérents, donateurs, problème d'image voire de confiance...

Nos conseils

- **Associations, si vous encaissez des dons, des cotisations par internet** :

Rapprochez-vous de votre prestataire informatique afin de vous assurer que votre site internet est conforme au protocole 3DSecure.

- **Adhérents, donateurs...** : si vous payez votre cotisation par carte bancaire sur internet ou si vous faites un don ou un paiement avec votre carte bancaire sur internet :

Rapprochez-vous de votre établissement bancaire pour connaitre les différentes solutions d'Authentification Forte mises à votre disposition.

>> Découvrez les solutions proposées par le Crédit Mutuel pour les associations, pour les particuliers (adhérents, donateurs...).

- *Pour aller plus loin :*
- *Dossier thématique – Collecte de dons*
- *Dossier thématique - RGPD*

Le Crédit Mutuel pour Associathèque