Septembre 2020

Directive concernant le respect des prescriptions de sécurité PCI DSS pour les partenaires contractuels

En général

Swisscard AECS GmbH (Swisscard) s'engage depuis des années à la protection des données des titulaires de cartes afin de garantir le niveau de sécurité le plus élevé. L'utilisation abusive de données a un impact négatif sur les titulaires de cartes, les partenaires contractuels, les prestataires de services et les émetteurs de cartes. L'introduction de la norme Payment Card Industry Data Security Standards (PCI DSS) comme réponse à ces menaces peut contribuer à renforcer la confiance du client, augmenter la rentabilité et accroître la réputation d'une entreprise. Chez Swisscard, nous savons que nos partenaires contractuels partagent nos préoccupations. Nous attendons donc de votre part, dans le cadre des responsabilités qui vous incombent, que vous respectiez les dispositions relatives à la protection des données des Conditions d'acceptation des Cartes American Express et de la présente Directive, que nous modifions à l'occasion.

PCI DSS

La norme Payment Card Industry Data Security Standards (PCI DSS) a été établie il y a quelques années déjà par Visa International, MasterCard, American Express, JCB et Discover pour assurer la mise en œuvre au niveau mondial de mesures de protection des données cohérentes et pour protéger préventivement les données de cartes afin d'augmenter la sécurité. Elles sont publiées par le PCI Security Standards Council et définissent les exigences techniques et opérationnelles pour toutes les parties prenantes qui enregistrent, traitent ou transmettent des données de cartes.

Les exigences détaillées dans leur version en vigueur peuvent être consultées à tout moment sous www.pcisecuritystandards.org.

Responsabilités

La norme PCI DSS est obligatoire pour les partenaires contractuels, les banques, les processeurs et les Payment Service Providers qui enregistrent, traitent ou transmettent des données de titulaires de cartes pour leurs propres besoins ou au nom d'autres organisations. Il est de la responsabilité du partenaire contractuel de respecter la norme PCI DSS. Les partenaires contractuels sont également responsables du respect de la norme PCI DSS par les tiers qu'ils ont mandatés, comme par exemple les Payment Service Providers qui enregistrent, traitent ou transmettent des données de cartes en leur nom. Les frais relatifs à la certification sont intégralement à la charge du partenaire contractuel, respectivement des tiers mandatés.

Comment le partenaire contractuel doit-il procéder

En vertu de la norme PCI DSS, le partenaire contractuel a l'obligation de documenter les mesures de sécurité qu'il a prises (certification). Dans le tableau ci-dessous figurent les obligations que les partenaires contractuels doivent respecter et les documents qu'ils doivent soumettre sur la base du nombre annuel de transactions, afin de prouver leur respect de la norme PCI DSS vis-à-vis de Swisscard.

Les partenaires contractuels de la catégorie 3 ne doivent soumettre les documents de certification que si Swisscard les demande, mais ils sont soumis à la clause de responsabilité et aux autres dispositions de la norme PCI DSS. Swisscard informe les partenaires contractuels de la catégorie 3 concernés au moins nonante (90) jours avant l'envoi des documents requis.

Tableau «partenaires contractuels»

Catégorie	Volume annuel de transactions	Preuves de certification	Exigences
1	Plus de 2,5 millions de transactions par cartes American Express par an	• Rapport sur le „Annual Onsite Security Assessment“ • Scan de réseau trimestriel	Obligatoire
2	De 50'000 à 2,5 millions de transactions par cartes American Express par an	• Questionnaire «Annual Self Assessment» • Scan de réseau trimestriel	Recommandé ou à la demande de Swisscard

3	Moins de 50'000 transactions American Express par an	• Questionnaire «Annual Self Assessment» • Scan de réseau trimestriel	Recommandé ou à la demande de Swisscard

Questions et informations

Pour toute demande concernant PCI, vous pouvez appeler le 044 659 64 44

Procédure à suivre en cas d'incident de données

Vous devez aviser Swisscard **immédiatement, mais au plus tard dans les vingt-quatre (24) heures** à compter de la découverte de l'incident de données en téléphonant au **044 659 64 44** (service téléphonique 24 heures sur 24)

Glossaire

Annual Onsite Security Assessment: l'Annual Onsite Security Assessment est un contrôle sur place de sécurité détaillé de vos appareils, systèmes et réseaux (et des composants s'y rapportant) au moyen desquels des données de titulaires de cartes ou d'identification confidentielles (ou les deux) sont enregistrées, traitées ou transmises.

Annual Self Assessment Questionnaire: le questionnaire PCI DSS «Self Assessment Questionnaire» (SAQ) sert, lors de votre auto-évaluation annuelle, à évaluer vos appareils, systèmes et réseaux (et les composants s'y rapportant) au moyen desquels des données de titulaires de cartes ou d'identification confidentielles (ou les deux) sont enregistrées, traitées ou transmises.