Payment Services

Directive concernant le respect des prescriptions de sécurité de la Payment Card Industry («Directive PCI»)

1. Préambule

Les attaques sur les systèmes informatiques se sont répandues dans le monde entier. En particulier, les données des cartes sont une cible attrayante et lucrative pour des agresseurs. En raison de ce constat, les organismes internationaux de cartes, en collaboration avec les spécialistes de la sécurité des données et des représentants du commerce, ont crée ensemble le Payment Card Industry Security Standards Council. Cet organisme définit divers standards de sécurité des données (par ex. Payment Card Industry Data Security Standard [ci-après «PCI DSS»] et Payment Application Data Security Standard [ci-après «PA DSS»]) qui ont force obligatoire pour tous les partenaires commerciaux (ci-après «PC») et pour les acteurs impliqués dans le traitement et le stockage de données de cartes de crédit. En cas de non respect de ces standards, SIX Payment Services SA (ci après «SPS») s'expose à des amendes substantielles et/ou à des prétentions en dommages et intérêts de la part des organismes internationaux de cartes.

2. Champ d'application

La directive concernant le respect des prescriptions de sécurité de la Payment Card Industry a force obligatoire pour tous les PC de SPS et fait partie intégrante du contrat d'acceptation pour les transactions en présence du titulaire et/ou pour les transactions à distance. La directive comprend également d'éventuels mandataires ou fournisseurs du PC, dès le moment où ceux-ci traitent, enregistrent ou enregistrent temporairement des données de paiement importantes pour le PC. Le cas échéant, le PC est tenu de mettre à la charge de tout tiers prestataire de service les obligations résultant de cette directive, ainsi que de veiller à leur respect.

3. Enregistrement des données

3.1 Interdiction de l'enregistrement des données

Toute forme d'enregistrement (conservation de données sous forme électronique ou physique de courte et de longue durée) de données de cartes sensibles est – exception faite de l'obtention immédiate de l'autorisation – interdite dans tous les cas. Les données de la bande magnétique de la carte (Track2-données), le code de sécurité de la carte (CVC2/CW2) ainsi que toutes les données en relation avec le numéro d'identification personnel (NIP) du titulaire de la carte font partie de la catégorie des données de cartes sensibles.

3.2 Restrictions à l'enregistrement des données

Le numéro de la carte (en règle générale à 16 chiffres) ne peut être enregistré que sous forme cryptée et particulièrement sécurisée. Cela vaut également pour la date d'expiration et pour le nom du titulaire, si ceux-ci sont enregistrés avec le numéro de la carte. Des documents physiques qui contiennent les informations susmentionnées ne doivent être conservés que d'une manière spécialement sécurisée. L'enregistrement des données doit se limiter au minimum nécessaire pour l'exploitation.

3.3 Autres données

Toutes les autres données enregistrées du titulaire de la carte doivent être protégées contre les accès non autorisés de l'intérieur et de l'extérieur au moyen de mesures logiques et physiques appropriées.

4. Certification Payment Card Industry Data Security Standard

Les Payment Card Industry Data Security Standards comprennent une série de règles obligatoires pour toutes les parties qui travaillent, enregistrent ou traitent les données de cartes. Le PCI DSS est défini et régulièrement actualisé par le PCI Security Standards Council. De plus amples informations peuvent être consultées sur le site web officiel: https://www.pcisecuritystandards.org.

En principe, tous les PC de SPS sont tenus de se certifier vis-à-vis du PCI DSS au moyen des mesures de certification imposées. SPS est habilitée à demander une certification PCI DSS à la conclusion du contrat ou à tout moment pendant la durée du contrat. La non-certification du PC malgré une invitation écrite de SPS ou l'absence d'une certification correspondante constitue un motif de résiliation immédiate du contrat.

Les conditions pour l'obtention d'un certificat sont échelonnées selon le volume des transactions (voire chiffre 4.2).

4.1 Obligation de certification

Tous les PC avec un contrat d'acceptation pour des transactions à distance et plus de 20 000 transactions annuelles avec MasterCard (incl. Maestro) et/ou les cartes Visa sont tenus d'obtenir et de maintenir une certification PCI DSS.

Tous les PC avec un contrat d'acceptation pour les transactions en présence du titulaire de la carte et plus de 1 000 000 transactions annuelles avec MasterCard (incl. Maestro) et/ou les cartes Visa sont tenus d'obtenir et de maintenir une certification PCI DSS.

Tous les partenaires contractuels avec un contrat d'acceptation pour les transactions à distance sont tenus, pour autant qu'ils traitent totalement ou partiellement des données de cartes dans leurs propres systèmes, d'acquérir une certification PCI DSS et de la conserver.

4.2 Acquisition et obtention à bon droit de la certification PCI DSS
La certification PCI DSS dépend du nombre des transactions annuellement traitées. Des mesures de certification différenciées doivent être prises régulièrement en fonction du nombre des transactions. Ces mesures sont les suivantes:

Niveau	Description	Mesures de certification	Obligation de certification
1	- PC avec plus de 6 mios de transactions annuelles avec MasterCard (incl. Maestro) ou Visa sur tous les canaux de distribution - PC avec pertes de données attaques de hackers réussies	- On-Site Audit annuel par QSA - Network-Scan trimestriel par ASV	Obligation
2	- PC avec 1 mio jusqu'à 6 mios de transactions annuelles avec MasterCard (incl. Maestro) ou Visa sur tous les canaux de distribution (transactions en présence du titulaire/ou à distance)	- On-Site Audit annuel par QSA ou questionnaire Self Assessment annuel par un collaborateur accrédité ISA - Network-Scan trimestriel par ASV	Obligation
3	- PC avec 20 000 jusqu'à 1 mio de transactions E-commerce par an avec MasterCard ou Visa	- questionnaire Self Assessment annuel - Network-Scan trimestriel par ASV	Obligation
4	- PC avec transactions e-commerce qui traitent des données de cartes dans leurs propres systèmes	- questionnaire Self Assessment annuel - Scan trimestriel du réseau par ASV	Obligation
5	- Tous les autres PC	- questionnaire Self Assessment annuel - Network-Scan trimestriel par ASV	A la demande de SIX Payment Services SA

Pour les définitions des principes, voir le chiffre 8

4.3 Obligation d'information
Le PC doit informer SPS régulièrement et spontanément des résultats des mesures de certification. Cela comprend la mise à disposition du Report on Compliance (ROC), si un tel rapport est prévu comme mesure de certification, et les résultats du Network-Scan ainsi que du questionnaire Self-Assessment.

Le PC doit informer SPS immédiatement et spontanément si le degré de certification ne peut pas être maintenu (pour cause d'ajustement du système, de résultats négatifs lors de la certification ou similaires).

Les changements relatifs à l'engagement de tiers prestataires de services doivent immédiatement être communiqués à SPS.

Si, dans le modèle de licence, des applications de tiers prestataires de services sont impliquées dans le traitement ou dans l'enregistrement des données des cartes, ces applications doivent être communiquées à SPS.

Le PC habilite SPS à demander des informations concernant le degré de certification directement auprès des organismes de certification.

5. Payment Application Data Security Standard (PA DSS)

Les applications (par ex. les applications Webshop, systèmes de Customer Relationship Management, systèmes de Hotel Property Management), vendues, transmises ou faisant l'objet de licence à des tiers, sont soumises, sauf exceptions, aux exigences du PA DSS. Les applications de paiement propre à l'entreprise, qui ont été développées par le PC ou par des tiers prestataires de services et qui n'ont pas été vendues ou fait l'objet de licence à des tiers, ne sont pas soumises aux exigences du PA DSS.

A partir du **01.07.2012**, toutes les applications standard achetées ou utilisées dans le cadre d'un modèle de licence d'un tiers prestataire de services, qui traitent ou enregistrent des données de carte, doivent disposer d'une certification selon le PA DSS. Toutes les applications certifiées PA DSS sont publiées sur le site web du PCI Security Standard Council.

6. Tiers prestataires de services

Les tiers prestataires de services sont des entreprises externes mandatées par le PC pour traiter, travailler, enregistrer ou transférer des données des cartes (par ex. Payment Service Provider, Webhosting-Provider, portails de réservation).

Tous les tiers prestataires de services auxquels le PC a recours doivent à tout moment être certifiés PCI DSS et avoir été acceptés formellement et enregistrés par les organismes internationaux de cartes. SPS peut à tout moment interdire le recours à un tiers prestataire de services ou le soumettre à des restrictions individuelles. En principe, seuls peuvent être utilisés les tiers prestataires de service qui figurent sur la liste des tiers prestataires de services autorisés publiée par SPS.

7. Terminaux POS

Tous les terminaux POS utilisés doivent disposer de certificats PCI PTS valides.

8. Définitions

Enregistrement des données
L'enregistrement des données comprend la conservation des données sous forme électronique ou physique, aussi bien de longue que de courte durée (enregistrement temporaire).

Qualified Security Assessor (QSA)
Un Qualified Security Assessor est une personne physique, accréditée par le PCI Security Standards Council, qui est habilitée à procéder à des vérifications dans les locaux du PC ou d'un tiers et à établir un Report of Compliance (ROC).

Approved Scanning Vendor (ASV)
Un Approved Scanning Vendor est une entreprise de sécurité qui a été accréditée par le PCI Security Standards Council et qui conduit les Network-Scans.

Network-Scan
Un Network-Scan est une attaque de hacking périodique, faite en accord avec le PC pour déceler des possibles faiblesses dans le système du PC. Un Network-Scan ne peut être effectué que par un Approved Scanning Vendor.

On-Site Audit
Un On-Site Audit est un contrôle effectué auprès du PC ou d'un tiers par le Qualified Security Assessor concernant la vérification du respect des PCI DSS. Le résultat sera communiqué dans un Report on Compliance.

Self Assessment Questionnaire (SAQ)
Un Self Assessment Questionnaire est une auto-déclaration concernant le respect des PCI DSS. A cet effet, il s'agit de remplir un questionnaire de sécurité. Celui qui répond à toutes les questions par «oui» respectivement par «pas pertinent» est certifié.

Report on Compliance (ROC)
Un Report on Compliance est établi après un On-Site Audit réussi mené par un Qualified Security Assessor et confirme le respect intégral des PCI DSS.

Internal Security Assessor Program (ISA)
L'Internal Security Assessor Program mis à disposition par le PCI Security Standards Council s'adresse au personnel technique interne du PC et propose un programme de formation complet concernant les exigences des PCI DSS. Ledit programme se termine par un examen d'accréditation. L'accréditation doit être répétée annuellement.

110.0901.03 CHE_FR/06.2018

SIX Payment Services SA
HHardturmstrasse 201, Case postale
8021 Zurich

www.six-payment-services.com/welcome