WORLDLINE

Payments to grow your world

Directives pour la certification de sécurité PCI DSS des partenaires affiliés.

Au niveau mondial, tous les partenaires affiliés qui transmettent, traitent ou stockent des données de carte sont tenus de respecter les directives de sécurité spécifiées dans la norme Payment Card Industry Data Security Standard (PCI DSS). En cas de non-respect de ces directives, Worldline est en droit de terminer avec effet immédiat la relation contractuelle en vigueur et de faire valoir d'éventuelles prétentions en dommages-intérêts.

Les présentes directives, qui ont une portée à la fois technique et liée à l'organisation des entreprises, sont contractuellement contraignantes pour tous les partenaires affiliés de Worldline.

Que recouvre PCI DSS ?

La norme PCI DSS comprend 12 exigences contraignantes visant à protéger les données de carte durant leur traitement, leur stockage et leur transmission. La mise en œuvre de PCI DSS est gérée au travers des programmes de sécurisation des organisations de cartes : en l'occurrence les programmes AIS de Visa, SDP de Mastercard, ainsi que les programmes correspondants d'American Express, Discover (Diners Club) et JCB.

Pour quelle raison la norme PCI DSS a-t-elle été éditée ?

Les vols de données de carte ont augmenté de manière continue au cours de ces dernières années. L'usage frauduleux des données volées cause des préjudices considérables à toutes les parties concernées.

Quel est le but précis de PCI DSS ?

Avec la norme PCI DSS, les organisations de cartes souhaitent encore renforcer la sécurité des paiements par carte et, par conséquent, protéger encore plus efficacement les commerçants et les titulaires de cartes, ainsi que l'ensemble de la branche contre le vol et l'utilisation abusive de données.

Qui est tenu de respecter la norme PCI DSS ?

La norme PCI DSS contraint tous les partenaires affiliés dans le monde qui transmettent, traitent ou stockent des données de carte à prendre et à appliquer des mesures efficaces en matière de sécurité.
La responsabilité des partenaires affiliés implique par ailleurs de veiller à ce que des sociétés tierces qui sont mandatées par eux et qui pourraient avoir un impact sur la sécurité des titulaires de cartes ou exercer des activités pour le compte des partenaires affiliés, telles que des sociétés d'hébergement web ou des « Payment Service Providers » (PSP – fournisseurs de service de paiement), se conforment à la norme PCI DSS.

Veuillez vous référer également aux points relatifs à la « protection des données » et à la « responsabilité » contenus dans les conditions générales applicables à l'acceptation des cartes.

Qui est responsable du respect de la norme PCI DSS ?

Il incombe à chaque partenaire affilié de respecter les directives de sécurité de la norme PCI DSS. Par ailleurs, les organisations de cartes leur demandent de fournir une déclaration (certification) relative aux mesures qu'ils ont prises en matière de sécurité. La portée de cette déclaration (certification) dépend du nombre de transactions.

Quels sont les types de mesures de certification ?

- **Self-Assessment Questionnaire (SAQ)**
  Il s'agit d'un questionnaire d'auto-évaluation à remplir.
- **On-Site Audit**
  Les partenaires contractuels avec de gros volumes de transactions et probablement ceux qui ont été victimes d'un vol de données de cartes ont l'obligation de compléter un ROC (Report on Compliance). Le rapport et l'attestation doivent être établis par un QSA (Qualified Security Assessor) ou par un auditeur dûment formé (ISA – Internal Security Assessor).
- **Network Scan**
  D'entente avec le partenaire affilié, une entreprise de certification accréditée (Approved Scanning Vendor) effectue chaque trimestre une analyse ciblée, afin de déceler d'éventuelles failles de sécurité.

Si le partenaire affilié ne remplit pas tous les critères de certification, il est tenu de remédier immédiatement à la situation dans les secteurs concernés et peut être soumis à des sanctions financières jusqu'à ce qu'il se mette en conformité.

Qui doit prendre à sa charge les frais de certification ?

Tous les frais de certification incombent au partenaire affilié ; de même en ce qui concerne les dépenses visant à remédier aux lacunes constatées lors de l'examen.

Que se passe-t-il si un partenaire affilié omet de se faire certifier ?

Si, malgré ses obligations, un partenaire affilié omet de se faire certifier, Worldline est en droit de terminer avec effet immédiat la relation contractuelle et d'exiger des dommages-intérêts pour d'éventuels préjudices subis par les organisations de cartes, ainsi que pour toutes revendications émanant des sociétés émettrices de cartes.

Qui a le droit de consulter les données de certification ?

Seuls le partenaire affilié et l'entreprise de certification ont un droit de regard sur les données recueillies lors de la certification. Le partenaire affilié est cependant tenu d'envoyer à Worldline le résumé des résultats de la certification. Worldline a également le droit de consulter les Self-Assessment Questionnaires. Les organisations de cartes ne reçoivent, par contre, que des analyses statistiques.

À quels intervalles convient-il de renouveler la certification ?

Toutes les entités doivent faire l'objet d'une évaluation annuelle et les entités disposant d'adresses IP orientées vers l'internet (e-commerce, etc.) doivent également faire l'objet d'une analyse trimestrielle des vulnérabilités (ASV).
Toute modification importante de l'environnement du partenaire affilié doit être immédiatement signalée à Worldline afin de déterminer si elle a un impact sur les exigences commerciales ou de conformité.

Par quelles entreprises les mesures de certification doivent-elles être réalisées ?

Vous trouverez sur Internet un répertoire des entreprises de certification accréditées :
- pour l'exécution des On-Site Audits : **pcisecuritystandards.org/pdfs/pci_qsa_list.pdf**
- pour l'exécution des Network Scans : **pcisecuritystandards.org/pdfs/asv_report.html**

Où trouver davantage d'informations sur PCI DSS ?

Vous trouverez de plus amples informations concernant la norme PCI DSS sur les sites web suivants :
- Worldline : **worldline.com/merchant-services/pci**
- PCI Security Standards Council : **pcisecuritystandards.org**

Les coordonnées de votre interlocuteur local sont disponibles sous : **worldline.com/merchant-services/contacts**

110.00110.03 INT_FR/08.2023