WORLDLINE

Payments to grow your world

# Indicazioni sull’osservanza delle disposizioni di sicurezza PCI DSS per i partner contrattuali.

A livello mondiale, i partner contrattuali che trasmettono, elaborano o memorizzano i dati delle carte sono tenuti ad osservare le direttive di sicurezza definite nel Payment Card Industry Data Security Standard (PCI DSS). Qualora queste venissero disattese, Worldline ha la facoltà di recedere dal contratto con effetto immediato e di rivalersi sul partner per eventuali sanzioni e risarcimenti.

Le seguenti indicazioni sono, in qualità di direttive tecniche e organizzative, parte integrante e vincolante di ogni contratto stipulato con Worldline.

### In cosa consiste lo standard PCI DSS?

PCI DSS comprende 12 requisiti vincolanti, che devono garan tire la tutela dei dati delle carte durante l’elaborazione, la memorizzazione e la trasmissione. L’applicazione di PCI DSS è regolata dai programmi di sicurezza delle organizzazioni che emettono le carte. Tra essi AIS di Visa, SDP di Mastercard nonché i corrispondenti programmi di American Express, Discover (Diners Club) e JCB.

### Perché è stato introdotto lo standard PCI DSS?

Negli ultimi anni i furti di dati delle carte sono aumentati in maniera costante. Il successivo impiego abusivo dei dati rubati ha causato danni considerevoli a tutte le parti coinvolte.

### Qual è lo scopo dello standard PCI DSS?

Con lo standard PCI DSS le organizzazioni delle carte vogliono incrementare ulteriormente la sicurezza dei pagamenti con le carte e, quindi, tutelare con maggiore efficacia i commer cianti, i titolari di carte e l’intero settore dal furto e dall’abuso dei dati delle carte.

## Chi è tenuto ad osservare lo standard PCI DSS?

Lo standard PCI DSS obbliga i partner contrattuali che tra smettono, elaborano o memorizzano dati di carte a livello mondiale ad adottare e osservare misure di sicurezza efficaci.

Inoltre, gli esercenti hanno la responsabilità di garantire la conformità agli standard PCI DSS di tutte le terze parti a cui si rivolgono e che potrebbero avere un impatto sulla sicurezza dei dati dei titolari di carta o che svolgono attività per conto dell'esercente, come le società di web hosting o i provider di servizi di pagamento (PSP).

Si vedano al proposito i punti relativi alla «protezione dei dati» e alla «responsabilità» contenuti nelle condizioni generali applicabili all'accettazione delle carte.

## Chi è responsabile dell'osservanza dello standard PCI DSS?

Per principio risiede nella responsabilità propria di ciascun partner contrattuale rispettare le disposizioni di sicurezza. Le organizzazioni delle carte, tuttavia, esigono che i partner contrattuali dichiarino (facciano certificare) le misure di sicurezza adottate. L'entità di una dichiarazione (certificazione), dipende dalla quantità di transazioni effettuate.

## Quali varianti di certificazione esistono?

- **Self-Assessment Questionnaire (SAQ)**
  Richiede la compilazione di un questionario di autovalutazione.
- **On-Site Audit**
  I partner contrattuali con un volume elevato di transazioni e possibilmente coloro che sono stati vittime di un furto di dati delle carte sono tenuti a compilare un ROC (Report on Compliance). Il rapporto e l'attestazione devono essere a cura di un QSA (Qualified Security Assessor) o da un auditor qualificato (ISA – Internal Security Assessor).
- **Network Scan**
  Un'azienda di certificazione accreditata (Approved Scanning Vendor) esegue trimestralmente e previo accordo con il partner contrattuale una scansione mirata al sistema per individuarne eventuali punti deboli.

Se un partner contrattuale non soddisfa tutti i criteri di certi ficazione, è tenuto a perfezionare, senza indugio, le misure di sicurezza nei settori contestati e può essere soggetto a sanzioni finanziarie fino al raggiungimento della conformità.

## Chi sostiene i costi della certificazione?

I costi delle misure di certificazione sono interamente a carico del partner contrattuale; lo stesso vale per i costi inerenti la rimozione delle defezioni riscontrate nei controlli di certificazione.

## Cosa succede se un partner contrattuale non si sottopone alla certificazione?

Se un partner contrattuale che soggiace all'obbligo di certifi cazione non si sottopone alla stessa, Worldline ha facoltà di recedere dal contratto con effetto immediato e di esigere il risarcimento dei danni per eventuali multe comminate dalle organizzazioni delle carte e crediti richiesti dalle emittenti delle carte.

## Chi ha accesso ai dati di certificazione?

Soltanto il partner contrattuale e l'azienda certificatrice inca ricata hanno accesso ai dati rilevati nell'ambito della certifica zione. Tuttavia, il partner contrattuale è tenuto a spedire a Worldline il riassunto degli esiti della certificazione. Allo stesso modo, Worldline ha accesso ai SelfAssessment Questionnaire. Le organizzazioni delle carte ricevono invece soltanto valutazioni statistiche.

## Con quale frequenza occorre rinnovare una certificazione?

Tutte le entità devono essere sottoposte a una valutazione annuale e le entità con indirizzi IP rivolti a Internet (e-commerce, ecc.) devono anche sottoporsi a scansioni ASV (vulnerabilità) trimestrali.
Qualsiasi modifica significativa dell'ambiente commerciale deve essere immediatamente comunicata a Worldline per valutare l'eventuale impatto sui requisiti commerciali o di conformità.

## Da quali aziende devono essere eseguite le misure di certificazione?

L'elenco di tutte le aziende di certificazione accreditate è disponibile in Internet:
- per l'esecuzione degli OnSite Audit: **pcisecuritystandards.org/pdfs/pci_qsa_list.pdf**
- per l'esecuzione dei Network Scans: **pcisecuritystandards.org/pdfs/asv_report.html**

## Dove reperire ulteriori informazioni sullo standard PCI DSS?

Ulteriori informazioni sullo standard PCI DSS sono disponibili sui siti Internet seguenti:
- Worldline: **worldline.com/merchant-services/pci**
- PCI Security Standards Council: **pcisecuritystandards.org**

L'interlocutore locale è indicato su: **worldline.com/merchant-services/contacts**

110.00110.04 INT_IT/08.2023