POLITICA SWISSCARD PCI DSS E REQUISITI DI SICUREZZA PER PARTNER CONTRATTUALI

Disposizioni generali
Da molti anni Swisscard AECS GmbH (Swisscard) si impegna a proteggere i dati dei titolari di carta per garantire il massimo livello di sicurezza. L'utilizzo non autorizzato dei dati ha un impatto negativo non solo sui titolari di carta, ma anche su partner contrattuali, fornitori di servizi ed emittenti di carte. L'introduzione dei Payment Card Industry Data Security Standards (PCI DSS), sviluppati in risposta a questa minaccia, contribuisce a rafforzare la fiducia dei clienti, ad aumentare la redditività e a migliorare la reputazione di un'azienda. Noi di Swisscard siamo consapevoli che i nostri partner contrattuali condividono queste preoccupazioni. Nell'ambito della propria responsabilità, è pertanto richiesto il rispetto delle disposizioni in materia di protezione dei dati contenute sia nelle Condizioni generali accettazione American Express che nella presente politica, soggetta a revisioni periodiche.

PCI DSS
I Payment Card Industry Data Security Standards (PCI DSS) sono stati sviluppati diversi anni fa da Visa International, MasterCard, American Express, JCB e Discover per promuovere l'introduzione globale di coerenti misure di sicurezza dei dati e per proteggere preventivamente i dati delle carte, aumentando così la sicurezza nella loro gestione. I PCI DSS, pubblicati dal PCI Security Standards Council, disciplinano i requisiti tecnici e operativi per tutte le parti che conservano, trattano e trasmettono i dati delle carte.
La versione più recente dei requisiti dettagliati può essere consultata in qualsiasi momento all'indirizzo www.pcisecuritystandards.org.

Responsabilità
I PCI DSS sono obbligatori per tutti i nostri partner contrattuali, le banche, i responsabili del trattamento e i fornitori di servizi di pagamento che conservano, trattano o trasmettono i dati dei titolari di carta, per scopi propri o per conto di altre organizzazioni. Il rispetto dei PCI DSS rientra nella responsabilità del partner contrattuale, che risponde inoltre della conformità ai PCI DSS da parte di eventuali terzi coinvolti, ad esempio i fornitori di servizi di pagamento, che conservano, trattano o trasmettono i dati delle carte per suo conto. I costi delle misure di certificazione sono interamente a carico del partner contrattuale o del terzo coinvolto.

Come procedere
Per comprovare la conformità ai PCI DSS, il partner contrattuale è tenuto a documentare le misure di sicurezza adottate (misure di certificazione). La tabella seguente illustra ai partner contrattuali, in base al rispettivo volume annuo di transazioni, i compiti loro spettanti e i documenti da presentare quale prova della conformità ai PCI DSS.
È importante notare che i partner contrattuali di 3° e 4° livello sono tenuti a presentare i documenti di certificazione soltanto su richiesta di Swisscard; restando comunque responsabili e soggetti a tutte le altre disposizioni in materia di PCI DSS. Swisscard informerà tali partner contrattuali per iscritto con un preavviso minimo di novanta (90) giorni dalla presentazione dei documenti richiesti.

Livello/Transazioni annuali con carta American Express	Relazione di valutazione sulla conformità in loco (ROC)	Questionario di autovalutazione (SAQ) e Scansione trimestrale	Attestato STEP per commercianti idonei
Livello 1 **2,5 milioni o più**	Obbligatorio	Non applicabile	Facoltativo (sostituisce il ROC)
Livello 2 **da 50 000 a 2.5 millions**	Facoltativo	SAQ obbligatorio (salvo presentazione di una valutazione in loco): scansione obbligatoria con certi tipi di SAQ	Facoltativo (sostituisce il SAQ e la Scansione di rete o il ROC)
Livello 3 **da 10 000 a 50 000**	Facoltativo	SAQ facoltativo (obbligatorio se richiesto da Swisscard o American Express): scansione obbligatoria con certi tipi di SAQ	Facoltativo (sostituisce il SAQ e la Scansione di rete o il ROC)
Livello 4 **10 000 o meno**	Facoltativo	SAQ facoltativo (obbligatorio se richiesto da Swisscard o American Express): scansione obbligatoria con certi tipi di SAQ	Facoltativo (sostituisce il SAQ e la Scansione di rete o il ROC)

Cosa fare in caso di violazione dei dati?
È necessario notificare immediatamente Swisscard, **comunque entro e non oltre ventiquattro (24 ore)** dalla scoperta della violazione dei dati, telefonando al numero **044 659 64 44** (servizio telefonico attivo 24 ore su 24).

Per domande e ulteriori informazioni
Per domande relative ai PCI DSS, contattare il nostro centro servizi al numero **044 659 64 44** (servizio telefonico attivo 24 ore su 24).
Per informazioni più dettagliate si rimanda alla Politica operativa di sicurezza dei dati di American Express (Data Security Operating Policy, DSOP) disponibile online all'indirizzo www.americanexpress.com. Si ricorda che la documentazione presentata non deve essere inviata direttamente ad American Express, bensì a Swisscard. Per ulteriori dettagli, contattare Swisscard.

Glossario
Valutazione annuale della sicurezza in loco: la valutazione annuale della sicurezza in loco è una verifica dettagliata in loco delle apparecchiature, dei sistemi e delle reti (e relativi componenti) in uso mediante i quali sono conservati, trattati o trasmessi i dati del titolare di carta o i dati confidenziali di autenticazione (o entrambi).

Questionario di autovalutazione annuale: il questionario di autovalutazione PCI DSS (SAQ) consente di autovalutare lo stato delle apparecchiature, dei sistemi e delle reti (e relativi componenti) in uso mediante i quali sono conservati, trattati o trasmessi i dati del titolare di carta o i dati confidenziali di autenticazione (o entrambi).

Versione 2025/01