

Indicazioni sull'osservanza delle disposizioni di sicurezza PCI DSS per partner contrattuali

In generale

Swisscard AECS GmbH (Swisscard) è impegnata già da diversi anni nella protezione dei dati dei propri titolari di carta onde garantirne la massima sicurezza. L'uso non autorizzato di dati influisce negativamente sui titolari di carta, sui partner contrattuali, sui fornitori di servizi e sull'emittente di carte. L'introduzione degli standard Payment Card Industry Data Security Standards (PCI DSS) in risposta a tale minaccia può contribuire a rafforzare la fiducia dei clienti, ad aumentare la redditività e ad accrescere la reputazione di un'impresa. Da Swisscard sappiamo che i partner contrattuali condividono la nostra preoccupazione. Presupponiamo, quindi, quale parte della Sua responsabilità, che si attenga alle disposizioni in materia di protezione dei dati delle condizioni per l'accettazione di carte American Express e alle presenti indicazioni che di tanto in tanto rielaboriamo.

PCI DSS

I Payment Card Industry Data Security Standards (PCI DSS) sono stati sviluppati già da alcuni anni da Visa International, MasterCard, American Express, JCB e Discover per supportare l'introduzione a livello mondiale di misure consistenti in materia di protezione dei dati e per proteggere in modo preventivo i dati delle carte, accrescendo così la sicurezza nella loro gestione. Vengono pubblicati dal PCI Security Standards Council e disciplinano i requisiti tecnici e operativi per tutte le parti che salvano, elaborano o trasmettono i dati delle carte.

I requisiti dettagliati della versione di volta in volta in vigore possono essere consultati in qualsiasi momento all'indirizzo www.pcisecuritystandards.org

Responsabilità

I PCI DSS sono obbligatori per partner contrattuali, banche, processor e Payment Service Provider che salvano, elaborano o trasmettono i dati dei titolari di carta per finalità proprie o a nome di altre organizzazioni. Rientra nella responsabilità personale dei partner contrattuali attenersi ai PCI DSS. I partner contrattuali sono responsabili anche dell'osservanza dei PCI DSS da parte di terzi a cui abbiano fatto ricorso, p.es. Payment Service Provider che elaborano, salvano o trasmettono dati delle carte a loro nome. I costi per le misure di certificazione sono interamente a carico del partner contrattuale o del terzo a cui abbia fatto ricorso.

Modus operandi del partner contrattuale

Secondo i PCI DSS, il partner contrattuale è tenuto a documentare le misure di sicurezza che ha adottato (misure di certificazione). Nella seguente tabella, i partner contrattuali rilevano, sulla base del numero annuo di transazioni, a quali obblighi siano soggetti e quali documenti debbano essere presentati al fine di dimostrare a Swisscard l'osservanza dei PCI DSS.

I partner contrattuali di livello 3 devono presentare documenti di certificazione solo su richiesta di Swisscard, ma sono comunque soggetti a responsabilità e a tutte le altre disposizioni dei PCI DSS. Swisscard informa tali partner contrattuali designati del livello 3 per iscritto e almeno novanta (90) giorni prima dell'inoltro richiesto dei documenti.

Livello	Volume di transazioni annuo	Prove della certificazione	Requisiti
1	Oltre 2.5 milioni di transazioni annue con carte American Express	<ul style="list-style-type: none"> Rapporto sull'«Annual Onsite Security Assessment» Scansione della rete trimestrale 	Obbligatorio
2	Da 50.000 fino a 2.5 milioni di transazioni annue con carte American Express	<ul style="list-style-type: none"> Questionario «Annual Self Assessment» Scansione della rete trimestrale 	su richiesta di Swisscard
3	Meno di 50.000 transazioni annue con carte American Express	<ul style="list-style-type: none"> Questionario «Annual Self Assessment» Scansione della rete trimestrale 	Raccomandato <i>oppure</i> su richiesta di Swisscard



Settembre 2020

Domande e informazioni

Per richieste riguardanti PCI puoi chiamare lo 044 659 64 44

Modus operandi in caso di violazione di dati

Dovete informare telefonicamente Swisscard **in modo tempestivo o al più tardi, comunque, entro ventiquattro (24) ore** dalla scoperta di una violazione di dati al numero **+41 44 659 64 44** (assistenza telefonica disponibile 24 ore su 24)

Glossario

Annual Onsite Security Assessment: Si tratta di una verifica di sicurezza dettagliata in loco dei Suoi apparecchi, sistemi e reti (e relativi componenti) tramite i quali vengono salvati, elaborati o trasmessi dati relativi ai titolari di carta o dati di autenticazione riservati (o entrambi).

Annual Self Assessment Questionnaire: In occasione dell'autovalutazione annuale, il questionario PCI DSS «Self Assessment Questionnaire» (SAQ) serve all'autocontrollo dei Suoi apparecchi, sistemi e reti (e relativi componenti) tramite i quali vengono salvati, elaborati o trasmessi dati relativi ai titolari di carta o dati di autenticazione riservati (o entrambi).