Obblighi di controllo dei Fornitori esterni

Standard di sicurezza dei dati per il settore Carte di Pagamento (Payment Card Industry Data Security Standard - PCI DSS)

Versione 14.0, ottobre 2024

Obblighi PCI DSS	Descrizione	Perché è importante?
1. Ottenere la conformità dei dati della carta	Il Fornitore è tenuto a rispettare le attuali versioni degli Standard di sicurezza dei dati per il settore delle Carte di Pagamento come stabilito dal Consiglio per gli Standard di Sicurezza dei Pagamenti, come ad esempio PCI DSS, PA-DSS, PCI-P2PE, PCI-PTS, PCI Card Production.	Proteggere i dati del titolare della carta: lo standard riconosciuto per raggiungere questo obiettivo è PCI DSS ed è un requisito normativo globale del settore. Gli standard di sicurezza PCI sono requisiti tecnici e operativi stabiliti dal Consiglio per gli Standard di Sicurezza per il settore Carte di Pagamento per proteggere i dati del titolare della carta.
2. Attestato per fornitori e commercianti	Il Fornitore deve esibire, prima del contratto e successivamente una volta all'anno, un Attestato di Conformità per le Valutazioni in loco (AoC) o, laddove applicabile, un Questionario di Autovalutazione (SAQ), applicabili all'ambito dei servizi forniti a Barclays. Tali documenti devono essere conformi ai requisiti PCI DSS - vedi www.pcisecuritystandards.org/ In caso di domande sollevate in sede di revisione dell'attestato AoC, ad esempio in merito all'ambito dei servizi, alla descrizione dell'ambiente o alla conformità PCI del fornitore, il relativo Rapporto sulla conformità (RoC) può essere richiesto ed esaminato per ulteriori informazioni. Un RoC modificato può essere accettabile se conferma che l'ambito della certificazione PCI si applica alla sfera dei servizi forniti o ad altre questioni sollevate da Barclays dopo aver esaminato l'AoC. Il Fornitore deve notificare a Barclays la non conformità, ovvero il più presto possibile e	Prova che un fornitore o un esercente ha raggiunto la conformità ai dati della Carta di Credito per l'ambito dei servizi forniti a Barclays e ha aderito ai requisiti. Prova che l'attestazione del fornitore AoC / RoC o SAQ si riferisce al servizio fornito. Se Barclays utilizza un fornitore o un esercente che non è conforme agli standard PCI DSS, dovrà contattare il team Rischi Terzi di Visa Europe (agentcompliance@visa.com) via e-mail per confermare che il fornitore o l'esercente sta implementando gli standard PCI DSS e ha fornito a Visa Europe un piano di stato PCI DSS (utilizzando il modello di Visa Europe) per la revisione e l'approvazione di Visa Europe.

	comunque non oltre 30 giorni dalla data di scadenza dei documenti di convalida.	
3. Accettazione del Fornitore	Prima della firma del contratto, il Fornitore deve confermare per iscritto a Barclays di essere responsabile, per i servizi oggetto del contratto, per la sicurezza dei dati del titolare della carta che possiede / memorizza / elabora / trasmette, o per i servizi che potrebbero avere un impatto sulla sicurezza dell'ambiente del cliente che ospita i dati del titolare della carta Barclays, ad esempio servizi di sicurezza (come i server di autenticazione), web hosting ecc. Eventuali modifiche al servizio fornito devono essere comunicate per iscritto a Barclays prima dell'implementazione delle modifiche stesse.	**Da PCI DSS v3.2.1** **Procedura di test per 12.8.2:** Rispettare gli accordi scritti e confermare che questi ultimi includono l'accettazione da parte dei fornitori di servizi della responsabilità riferita alla sicurezza dei dati dei titolari di carta che i fornitori di servizi possiedono o comunque memorizzano, elaborano o trasmettono per conto del cliente, o nella misura in cui tali servizi potrebbero avere un impatto sulla sicurezza dell'ambiente del cliente che ospita i dati dei titolari di carta. Nota: Insieme al Requisito 12.9, questo requisito per gli accordi scritti tra organizzazioni e fornitori di servizi è inteso a promuovere un livello coerente di comprensione tra le parti in merito alle rispettive responsabilità PCI DSS applicabili. Ad esempio, l'accordo può includere i requisiti PCI DSS applicabili da mantenere come parte del servizio fornito. **Linee guida per 12.8.2:** L'accettazione da parte dei fornitori di servizi dimostra il loro impegno a mantenere le adeguate misure di sicurezza per i dati del titolare della carta che ottiene dai propri clienti. Le politiche e le procedure interne del fornitore di servizi relative al processo di coinvolgimento dei clienti e gli eventuali modelli utilizzati per gli accordi scritti devono includere un modello per l'accettazione PCI DSS applicabile ai propri clienti. Il metodo con cui il fornitore di servizi invia l'accettazione scritta deve essere concordato tra il fornitore e i propri clienti.

Utilizzo di fornitori di servizi di terze parti / Outsourcing

Un fornitore di servizi o un esercente può utilizzare un fornitore di servizi terzo per memorizzare, elaborare o trasmettere i dati del titolare della carta per proprio conto, oppure per gestire componenti quali router, firewall, database, sicurezza fisica e/o server. In tal caso, ci può essere un impatto sulla sicurezza dell'ambiente che ospita i dati del titolare della carta.

Le parti devono identificare chiaramente i servizi e i componenti del sistema che sono inclusi nell'ambito della valutazione PCI DSS del fornitore di servizi, i requisiti specifici PCI DSS coperti dal fornitore di servizi e qualsiasi requisito che i clienti del fornitore di servizi devono includere nelle proprie revisioni PCI DSS. Ad esempio, un provider di hosting gestito è tenuto a indicare chiaramente quali dei suoi indirizzi IP vengono acquisiti nell'ambito del processo di verifica trimestrale delle vulnerabilità e quali sono gli indirizzi IP che il cliente è tenuto a includere nelle proprie verifiche trimestrali.

I fornitori di servizi sono tenuti a dimostrare la loro conformità agli standard PCI DSS, anche su richiesta dei brand di pagamento. I fornitori di servizi devono contattare il loro acquirente e/o il loro brand di pagamento per stabilire l'idonea convalida della conformità.

I fornitori di servizi di terze parti hanno due possibilità per convalidare la conformità:

1) **Valutazione annuale**: I fornitori di servizi possono sottoporsi a una o più valutazioni annuali PCI DSS per conto proprio e fornire prove ai loro clienti per dimostrare la loro conformità; oppure

2) **Valutazioni multiple, su richiesta:** Se non si sottopongono alle valutazioni annuali PCI DSS per conto proprio, i fornitori di servizi devono sottoporsi a valutazioni su richiesta dei loro clienti e/o partecipare a ciascuna delle revisioni PCI DSS dei loro clienti, fornendo ai rispettivi clienti i risultati di ciascuna revisione.

Se i fornitori terzi si sottopongono alla valutazione PCI DSS per conto proprio, devono fornire ai propri clienti prove sufficienti per verificare che l'ambito della valutazione PCI DSS del fornitore di servizi copra i servizi applicabili al cliente e che i requisiti PCI DSS pertinenti siano stati esaminati e determinati. Il tipo specifico di prova inviata dal fornitore di servizi ai propri clienti dipenderà dagli accordi/contratti in vigore tra le parti. Ad esempio, l'attestato CoA e/o le sezioni pertinenti del rapporto RoC del fornitore di servizi (modificate per proteggere le informazioni riservate) potrebbero contribuire a fornire le informazioni necessarie, tutte o in parte.

Inoltre, gli esercenti e i fornitori di servizi devono gestire e monitorare la conformità PCI DSS di tutti i fornitori di servizi terzi associati con accesso ai dati dei titolari di carta. *Per maggiori dettagli, fare riferimento al Requisito 12.8 del presente documento.*