



Lista di controllo per la verifica della conformità PCI DSS

Il partner contrattuale s'impegna a proteggere tutti i sistemi e i supporti dati che contengono i dati delle carte (cfr. cifra 13 CG) da un eventuale smarrimento e dall'accesso di terzi non autorizzati. Egli è altresì tenuto a rispettare sempre le disposizioni delle organizzazioni di carte internazionali e di SIX Payment Services, con particolare riferimento allo standard PCI DSS.

Se si è risposto «no» o «non è esatto» ad almeno una delle tre domande PCI nel contratto, occorre fornire di seguito le informazioni rilevanti per l'azienda.

Dati sulla ditta

Ditta	
Via/n°	Paese
NPA/luogo	N° partner contratt.

Indicate quali tipi di dispositivi hardware e software utilizzate e il nome dell'installatore della vostra soluzione di cassa.

Soluzioni integrate nella cassa

Produttore/marca	
Tipo	N° di serie
Software (numero di versione)	
<input type="checkbox"/> certificato PCI	<input type="checkbox"/> non certificato PCI

Integratore di cassa

Ditta	
Via/n°	
NPA/luogo	
Paese	Telefono

Terminale/apparecchi POS

Produttore/marca	
Tipo	N° di serie
Terminal ID	
Software (numero di versione)	
<input type="checkbox"/> certificato PCI	<input type="checkbox"/> non certificato PCI

Altre soluzioni

Produttore/marca	
Tipo	N° di serie
Software (numero di versione)	
<input type="checkbox"/> certificato PCI	<input type="checkbox"/> non certificato PCI

Altri integratori

Produttore/marca	
Tipo	N° di serie
Software (numero di versione)	
<input type="checkbox"/> certificato PCI	<input type="checkbox"/> non certificato PCI

Conferma del raggiungimento della conformità PCI DSS

Negli scorsi anni, gli attacchi hacker contro i sistemi informatici e di conteggio dei pagamenti tramite carta – nel corso dei quali sono stati sottratti illegalmente milioni di dati dei titolari – hanno segnato un netto aumento. Le conseguenze sono state gravi per tutte le parti coinvolte. Con l'introduzione di PCI DSS (Payment Card Industry Data Security Standard), le società di carte – Visa, Mastercard, American Express, JCB e Discover – intendono migliorare la sicurezza dei pagamenti tramite carta e proteggere con misure più efficaci gli esercenti, i titolari di carta e l'intero settore dal furto e dall'abuso dei dati delle carte.

Tutti i partner contrattuali nel mondo intero che trasmettono, elaborano o memorizzano i dati delle carte sono tenuti a rispettare le norme di sicurezza previste da PCI DSS. In caso di violazione delle precitate disposizioni, le organizzazioni di carte possono comminare sanzioni o avanzare richieste di indennizzo. Quale conseguenza diretta, in simili circostanze, SIX Payment Services si vedrebbe costretta a rescindere con effetto immediato il rapporto contrattuale e ad applicare le richieste di indennizzo e le eventuali sanzioni nei confronti del partner contrattuale coinvolto.

Oltre a garantire il rispetto delle disposizioni di sicurezza per quanto riguarda i loro sistemi e le loro applicazioni, i partner contrattuali sono altresì responsabili dell'osservanza delle disposizioni di sicurezza da parte delle aziende terze, come i Payment Service Provider (PSP) o i Data Storage Entities (DSE), da loro incaricate di trasmettere, elaborare o memorizzare dati delle carte.

In linea di principio, è nell'interesse di ogni singolo partner contrattuale garantire l'attuazione e il rispetto delle direttive di sicurezza PCI DSS. Le organizzazioni di carte ritengono che sia il proponente del contratto (l'acquirer) – in questo caso, SIX Payment Services – a dover verificare che tutti i suoi partner contrattuali rispettino PCI DSS. A tal fine, è necessario che i partner contrattuali dichiarino le misure di sicurezza da loro applicate (e ottengano la relativa certificazione). L'entità della dichiarazione (certificazione) dipende dal numero di transazioni elaborate e dalla misura in cui il partner contrattuale viene a contatto con i dati delle carte durante la loro trasmissione, elaborazione o memorizzazione.

Con il presente documento, il partner contrattuale conferma che effettuerà la registrazione sul portale web SAQ* (SAQ-Self Assessment Questionnaire) per procedere alla certificazione, se ciò gli verrà richiesto in forma scritta da SIX Payment Services. Il partner contrattuale s'impegna altresì a rispettare le scadenze previste.

Luogo/data

Ditta

Nome/i e cognome/i dei firmatari (in stampatello)

Firma giuridicamente valida del partner contrattuale

* Il portale web SAQ permette ai partner contrattuali di SIX Payment Services di effettuare la dichiarazione delle misure di sicurezza PCI DSS in tutta comodità online.

L'interlocutore locale è indicato su www.six-payment-services.com/contatto

SIX Payment Services SA
Hardturmstrasse 201
Casella postale
CH-8021 Zurigo

SIX Payment Services (Europe) S.A.
10, rue Gabriel Lippmann
5365 Munsbach
Lussemburgo

SIX Payment Services (Austria) GmbH
Marxergasse 1B
1030 Vienna
Austria

SIX Payment Services (Germany) GmbH
Langenhorner Chaussee 92-94
22415 Amburgo
Germania

