Reset

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 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 Worldline, con particolare riferimento allo standard PCI DSS.

Se nel contratto la risposta ad almeno una delle tre domande PCI è stata «falso», è necessario fornire i dati pertinenti per l'azienda.

DATI PARTNER CONTRATTUALE/ESERCENTE

Ragione Sociale .....

Via e nr. civico ..... Paese .....

CAP/Località .... Prov. ..... No 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 ..... No di serie .....

Software (numero di versione) ..... ☐ certificato PCI ☐ non certificato PCI

Integratore di cassa

Ragione Sociale .....

Via e nr. civico ..... Paese .....

CAP/Località .... Prov. ..... Telefono .....

Terminale/apparecchi POS

Produttore/marca .....

Tipo ..... No di serie .....

Terminal ID .....

Software (numero di versione) ..... ☐ certificato PCI ☐ non certificato PCI

Altre soluzioni

Produttore/marca .....

Tipo ..... No di serie .....

Software (numero di versione) ..... ☐ certificato PCI ☐ non certificato PCI

Altri integratori

Produttore/marca .....

Tipo ..... No di serie .....

Software (numero di versione) ..... ☐ certificato PCI ☐ 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 PCI DSS (Payment Card Industry Data Security Standard), gli operatori delle carte (Visa, Mastercard, American Express, JCB e Discover Card) intendono migliorare ulteriormente la sicurezza dei pagamenti tramite carta e, di conseguenza, proteggere in maniera ancora più efficace gli esercenti, i titolari delle carte e l'intero settore dai furti e dall'uso improprio 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, Worldline 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, Worldline – 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 di effettuare la certificazione tramite uno strumento online fornito o con documenti di validazione ufficiali, nella misura in cui ciò venga richiesto per iscritto da Worldline. Inoltre, il partner contrattuale si impegna a rispettare le scadenze fissate al riguardo.

Luogo /data	**Ragione Sociale**
.....	.....
Nome/i e cognome/i dei firmatari (in stampatello)	Firma giuridicamente valida del partner contrattuale
.....	.....

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

110.0114.04 CHE_IT/10.2021