BKN301 S.p.A.
Sede Legale e Amministrativa
Via Tre Settembre 99 - 47891 Dogana - San Marino
T +378 (0549) 943891 F +378 (0549) 943899
C.O.E SM26597

Capitale Sociale 3.450.000,00 euro i.v.
Iscritta nel Pubblico Registro delle Società
della Repubblica di San Marino il 26/11/2015 al n.7382
Iscritta al Registro dei Soggetti Autorizzati al n.73
Iscritta al Registro dei Prestatori di Servizi di Pagamento al n.07

AVVISO ALLA CLIENTELA
– VARIAZIONE UNILATERALE GENERALIZZATA –

Proposta di modifica unilaterale Regolamento Commercio Elettronico Esercenti BKN301 S.p.A. – ai sensi dell'Art. XIV.I.4 del Regolamento BCSM 2020/04 "Regolamento dei servizi di pagamento e di emissione di moneta elettronica (istituti di pagamento e IMEL)"

Gentile Cliente,
La informiamo che gli sviluppi relativi al mercato dei servizi di pagamento, hanno portato la Commissione Europea alla revisione della normativa di settore (Direttiva 2007/64/CE nota come Payment Services Directive -PSD) attraverso la pubblicazione della nuova Direttiva Europea 2015/2366 (cosiddetta PSD2) recepita nella Repubblica di San Marino con il Decreto Delegato 28 dicembre 2018 n. 177 "Disposizioni in materia di servizi di pagamento in recepimento della Direttiva (UE) 2015/2366" e dalla normativa secondaria di settore con il Reg. BCSM 2020/04 "Regolamento dei servizi di pagamento e di emissione di moneta elettronica (istituti di pagamento e IMEL)".
Per quanto attiene nello specifico i servizi di pagamento La informiamo che la PSD2 introduce importanti novità quali:

- obblighi di trasparenza: vengono rafforzati i diritti della clientela e la trasparenza in relazione agli obblighi di informazione, esecuzione e condizioni economiche;
- nuove misure di sicurezza: viene introdotta l'autenticazione forte del cliente (Strong Customer Authentication - SCA) per accedere ai conti, disporre ordini di pagamento sui canali on line e per effettuare operazioni che implichino rischi di abuso o frode.

Poiché le nuove norme si applicano anche ai contratti in essere, le inviamo la proposta di modifica unilaterale del Suo contratto, resasi necessaria dall' entrata in vigore del suddetto Regolamento.
Le modifiche sono evidenziate in grassetto.
Nessuna modifica è apportata alle condizioni economiche applicate.

Art. 1 – Definizioni

I termini e le espressioni utilizzati in maiuscolo nel presente regolamento **e nel Contratto** ove non altrimenti definiti all'interno del medesimo, avranno il significato di seguito indicato:

- **"Acquirer": società che presta i servizi di accettazione e negoziazione delle carte di pagamento (acquiring).**
- **"Applicazione Mobile (APP)": strumento applicativo software da installare su dispositivi mobili, utilizzati dall'Esercente per consentire a questi di accettare ed eseguire Transazioni a mezzo di terminale Mobile Pos.**
- **"Autenticazione Forte" o "SCA" o "Strong Customer Authentication": un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione.**
- **•"Autorizzazione": il processo tramite il quale l'Esercente ottiene l'approvazione creditizia dalla Banca o altra istituzione che ha emesso la Carta prima del perfezionamento di ogni transazione.**
- **"Canale Online": canale utilizzato dall'Esercente per la vendita dei propri beni e/o servizi (APP, sito internet, link diretto ad un gateway di pagamento, etc.).**
- **"Carta/e di Credito, Debito e Prepagata/e": la/e Carta/e che abilita/no il Titolare, in base a un rapporto contrattuale con l'emittente, a effettuare acquisti di beni o servizi presso gli Esercenti, con pagamento differito.**
- **"Carta/e Co-Badged": la/e di pagamento che includono due o più marchi di pagamento o due o più applicazioni di pagamento dello stesso marchio.**
- **Emittente della Carta o Emittente: qualunque banca o altra istituzione autorizzata da un Circuito di pagamento ad emettere Carte.**
- **"Pay-by-Mail": il Sistema elettronico utilizzato dagli Esercenti che consente di concludere Transazioni Elettroniche online, senza l'impiego di un Gateway di Pagamento, mediante utilizzo delle Carte previo rilascio elettronico della relativa autorizzazione.**
- **"PCI-DSS" (Payment Card Industry-Data Security Standard): è l'insieme dei requisiti informatici, tecnologici ed organizzativi previsti dai Circuiti di Carte di pagamento cui ''Esercente è tenuto a conformarsi per garantire la sicurezza dei dati delle Carte.**
- "**Regolamento BCSM n. 2020/04**": Regolamento emanato da Banca Centrale della Repubblica di San Marino n**. 2020/04** e successive modifiche ed integrazioni "Regolamento dei servizi di pagamento e di emissione di moneta elettronica (istituti di pagamento e imel)".

- **"Servizio Clienti": il servizio di assistenza della Società (i cui riferimenti sono riportati sul Foglio Informativo Esercenti BKN301 S.p.A.), messo a disposizione dell'Esercente, che consente di usufruire dei servizi, automatici e con operatore, inclusi quelli regolamentati dal Contratto, di volta in volta disponibili e resi noti all'Esercente e tramite il quale l'Esercente stesso può ricevere assistenza.**
- **"Sito Internet dell'Esercente": il sito internet utilizzato dall'Esercente per l'accettazione delle Transazioni nell'ambito del Funzionalità Pagamenti E-Commerce.**
- **Verifica PCI-DSS: Certificazione PCI-DSS fornita annualmente dall'Esercente a BKN301 S.p.A.**

Art. 2 - Oggetto del Contratto

2.1 Il contratto ha per oggetto il convenzionamento dell'Esercente all'utilizzo del Servizio nell'ambito dell'attività di commercio elettronico. Il Regolamento Commercio Elettronico Esercenti BKN301 S.p.A. contiene le condizioni applicabili alle Transazioni via Internet e costituisce un'appendice del Contratto di Convenzionamento. Esso integra e modifica parzialmente le condizioni generali del Contratto di Convenzionamento., limitatamente alle condizioni applicabili alle Transazioni online. In particolare, tutte le disposizioni contenute nel Contratto di Convenzionamento riguardanti le modalità di accettazione delle Carte devono intendersi derogate e quindi non applicabili alle Transazioni online.

2.2 Al Regolamento Commercio Elettronico Esercenti BKN301 S.p.A. sono allegati i seguenti documenti, che ne costituiscono parte integrante e sostanziale: **a) il Documento di Condizioni economiche Commercio Elettronico Esercenti BKN301 S.p.A., che ne costituisce il frontespizio; b) il modulo denominato "Domanda di Adesione Commercio Elettronico Esercenti BKN301 S.p.A.", comprensivo dell'informativa in materia di trattamento dei dati personali; c) il documento denominato "Foglio Informativo Commercio Elettronico Esercenti BKN301 S.p.A ; d) documento "Standard di Sicurezza sui Dati Previsti dai Circuiti Internazionali (PCI-DSS)" consultabile sul Sito Internet;**

2.3 Per quanto non espressamente disciplinato dal Regolamento Commercio Elettronico Esercenti BKN301 S.p.A., si rinvia alle disposizioni, ivi comprese le definizioni, contenute nel Regolamento Esercenti BKN301 S.p.A., tempo per tempo vigenti da considerarsi qui espressamente richiamato.

Art. 4 - Richiesta di autorizzazione e modalità di negoziazione delle Transazioni E-Commerce

4.1 Per ogni Transazione E-Commerce, l'Esercente deve ottenere, quale che ne sia l'importo, l'autorizzazione dalla Società.

4.2 Al fine di non incorrere in responsabilità dell'Esercente nei confronti dei Circuiti, la Transazione E-Commerce dovrà riportare la stessa data dell'autorizzazione concessa.

4.3: al fine di non incorrere in responsabilità dell'Esercente nei confronti dei Circuiti, la Transazione E-commerce dovrà riportare la stessa data dell'autorizzazione concessa.

4.4: l'Esercente si impegna ad adottare soluzioni che permettano alla Società di eseguire l'Autenticazione Forte (SCA) dei Titolari. La Società si riserva la possibilità di valutare caso per caso misure di autenticazione alternative per categorie di operazione considerate a basso rischio.

4.5 L'Esercente si impegna, se non diversamente comunicato da BKN301 S.p.A. secondo le modalità previste nel Regolamento Esercenti BKN301 S.p.A., a richiedere sempre al Titolare della Carta il codice di sicurezza CVV2 o CVC2 (codice di tre cifre riportato sul retro della Carta) e ad inoltrarlo alla Società unitamente alla richiesta di autorizzazione. L'Esercente si impegna inoltre a rendere accessibile il codice CVV2 o CVC2 solo al personale addetto alla richiesta di autorizzazione e a distruggerlo subito dopo l'effettuazione della medesima, adeguando in tal senso le proprie procedure (modulistica, processi organizzativi, ecc.). Qualora l'Esercente, per modalità tecnico-operative proprie debba conservare anche per un breve periodo tale codice, è obbligato ad attenersi a quanto indicato nel documento **"Standard di Sicurezza sui Dati Previsti dai Circuiti Internazionali (PCI-DSS)", consultabile sul Sito Internet della Società.** Inoltre, l'Esercente dovrà comunque adottare nella propria infrastruttura tecnologica/informatica, misure di sicurezza idonee ad evitare il furto dei dati sensibili relativi ai pagamenti. In caso di inosservanza degli obblighi previsti nel presente par. 4.5 relativi al trattamento dei dati dei Titolari, l'Esercente dovrà corrispondere le sanzioni previste all'art. 18 del Regolamento Esercenti BKN301 S.p.A..

4.6 È fatto assoluto divieto all'Esercente di accettare le Carte per la vendita dei beni e/o servizi espressamente indicati dai Circuiti e consultabili nel Sito Internet della Società.

4.7 L'autorizzazione inviata dall'Esercente senza codice CVV2 o CVC2 viene automaticamente respinta.

Art. 7 - Obblighi dell'Esercente in relazione alle Transazioni E-Commerce

7.1 L'Esercente dovrà conservare, per il tempo previsto dalle vigenti disposizioni di legge e, comunque, per almeno 13 (tredici) mesi dalla data della Transazione E-Commerce, i seguenti dati e/o documenti relativi a ciascuna Transazione: a) dati del Titolare: nome e cognome (ovvero azienda cui fa capo il Titolare per le Carte di tipo aziendale), indirizzo completo di CAP, telefono, fax, e-mail, codice fiscale; b) importo, data e ora della Transazione; c) numero e data di scadenza della Carta, ove presenti; d) numero e data dell'autorizzazione; e) copia della conferma relativa alla Transazione E-Commerce inviata al Titolare; f) fattura relativa alla merce e/o al servizio reso, ovvero documentazione attestante la mancata consegna della merce e/o mancata prestazione del servizio.

7.2 Qualora i beni e/o servizi ordinati debbano essere spediti e/o prestati ad una persona diversa dal Titolare e/o ad un indirizzo diverso da quello indicato nella Transazione quale residenza e/o domicilio del Titolare stesso, l'Esercente dovrà conservare, in aggiunta a quanto indicato al precedente par. 7.1, anche i seguenti dati relativi al destinatario di detti beni e/o servizi: a) nome e cognome; b) indirizzo completo di CAP; c) e-mail (per servizi on-line).

7.3 Nel caso di spedizioni di merci tramite posta o corriere l'Esercente dovrà conservare per almeno 13 (tredici) mesi la prova dell'avvenuta consegna della merce al Titolare della Carta.

In ogni caso, l'Esercente è obbligato a conservare tali dati/documenti nel rispetto degli Standard di Sicurezza sui Dati previsti dai Circuiti, e consultabili nel Sito Internet della Società.

7.4 Nel caso in cui l'Esercente conservi, elabori o trasmetta i dati sensibili relativi ai pagamenti, lo stesso è tenuto a cooperare con la Società e con i competenti organismi di esecuzione della legge qualora si verificassero gravi incidenti relativi alla sicurezza dei pagamenti, comprese le violazioni dei dati.

7.5 Nel caso in cui l'Esercente memorizzi, elabori o trasmetta i dati sensibili relativi ai pagamenti (cd. Dati delle carte), lo stesso è tenuto ad implementare i requisiti richiesti dallo standard PCI-DSS, pubblicato sul Portale BKN301, per la propria categoria di appartenenza. In ogni caso l'Esercente dovrà attuare misure di sicurezza in linea con i seguenti requisiti, al fine di limitare il rischio di furto dei dati sensibili relativi ai pagamenti attraverso i propri sistemi:

- **Prestare particolare attenzione all'adeguata separazione dei compiti e dei ruoli nei diversi ambienti della tecnologia dell'informazione (IT) (ad esempio ambienti di sviluppo, collaudo e produzione) e alla corretta applicazione del principio del "privilegio minimo" quale base per una sana gestione delle identità digitali e degli accessi;**
- **Disporre di soluzioni di sicurezza adeguate per proteggere reti, siti web, sistemi, basi dati e canali di comunicazione contro attacchi o abusi, come, a titolo esemplificativo, software antivirus aggiornati, firewall, principi di sviluppo sicuro, meccanismi di cifratura etc.; disabilitare ogni funzionalità superflua all'interno dei sistemi informatici ed eliminare le vulnerabilità riscontrate attraverso specifiche attività di test;**
- **Garantire l'adozione di meccanismi di cifratura, mascheramento o tokenizzazione per i dati sensibili relativi ai pagamenti che vengono trasmessi attraverso reti non-private o memorizzati all'interno di basi dati;**
- **Avvalersi di processi idonei per monitorare, tenere traccia e limitare l'accesso a: i) dati sensibili relativi ai pagamenti e ii) risorse critiche, logiche e fisiche, quali reti, sistemi, basi dati, moduli di sicurezza etc. e creare, manutenere ed analizzare registri e procedimenti di tracciabilità dei dati;**
- **Assicurare che il principio di "data minimization" sia una componente essenziale delle funzionalità di base: la raccolta, la trasmissione, l'elaborazione, la memorizzazione e/o l'archiviazione e la visualizzazione dei dati sensibili relativi ai pagamenti dovrebbero essere manutenute ad un livello minimo;**
- **Sottoporre i servizi di pagamento via internet a test periodici al fine di garantire la loro sicurezza. Tutte le modifiche devono essere oggetto di un processo formale di gestione dei cambiamenti che garantisca che i cambiamenti stessi siano correttamente pianificati, sottoposti a test, documentati e autorizzati. Sulla base dei cambiamenti effettuati e delle minacce riscontrate, i test devono essere ripetuti regolarmente e comprendere scenari di attacco pertinenti e noti;**
- **Sottoporre a verifica interna periodica le misure di sicurezza e il funzionamento dei servizi di pagamento via internet per garantire la loro robustezza ed efficacia. La frequenza e l'oggetto di tali controlli devono essere attinenti e proporzionali ai rischi per la sicurezza implicati. I controlli in questione devono essere svolti da soggetti terzi certificati e riconosciuti dal Council PCI;**
- **Mantenere regolamenti e documentazione specifica in merito alle regole di gestione dei dati sensibili relativi ai pagamenti.**

Qualora l'Esercente esternalizzi funzioni relative al trattamento dei dati sensibili delle carte, il relativo contratto dovrà includere disposizioni che prevedano il rispetto di misure di sicurezza in linea con i requisiti sopra riportati.

7.6 In caso di richiesta, l'Esercente dovrà trasmettere alla Società le informazioni e i dati di cui al presente articolo, nonché la relativa documentazione, entro e non oltre 7 (sette) giorni dalla data di ricezione della richiesta stessa, utilizzando il Portale Esercenti sul Sito Internet della Società.

7.7 L'esercente si impegna ad inserire sul proprio sito internet il logo della Società, nonché eventuali link al Sito Internet della Società, secondo le specifiche tecniche che verranno indicate dalla Società medesima.

7.8 L'Esercente si impegna altresì a pubblicare sul proprio sito internet un contatto di assistenza e-mail o telefonico.

Le ricordiamo che il termine entro cui lei ha diritto di recedere senza spese e con effetto in qualunque momento fino alla data in cui le modifiche sarebbero applicate, è di (60) sessanta giorni dal ricevimento della presente comunicazione.

Ove non receda entro il suddetto termine, la modifica si intenderà approvata.

Cordiali Saluti.