

## Informativa sull'Extranet di Bookassist

Ultimo aggiornamento: 25 maggio 2018

Quest'informativa include:

- 1) Termini e condizioni per l'utilizzo del Sistema di amministrazione di Bookassist ("Sistema")**
- 2) Informazioni sulla protezione dei dati per i dipendenti/per il personale autorizzato che accede al Sistema e/o al Sistema di gestione dei contenuti di Bookassist ("CMS")**
- 3) Note esplicative sulla politica relativa alle password, per l'utilizzo del sistema**

Tieni presente che, utilizzando il Sistema di amministrazione di Bookassist ("Sistema"), riconosci di accettare i Termini e le condizioni ivi descritti.

Il Sistema fornisce l'accesso ai dati personali in base agli obblighi contrattuali stabiliti nel Contratto di Bookassist con il Fornitore di alloggio, e in conformità con i Termini di elaborazione dei dati e di sicurezza di Bookassist (<https://bookassist.org/dp>).

### **1) Termini e condizioni per l'utilizzo del Sistema di amministrazione di Bookassist ("Sistema")**

#### **1. Requisiti PCI DSS (Standard di sicurezza dei dati del settore delle carte di pagamento)**

- a) Mentre Bookassist si impegna a soddisfare pienamente le condizioni stabilite dagli Standard di sicurezza dei dati (PCI DSS) facenti parte del settore delle carte di pagamento e volti all'elaborazione dei pagamenti online, il Fornitore di alloggio è pienamente responsabile per il corretto uso dei dati personali inseriti nel Sistema, in conformità con la relativa legislazione sulla protezione dei dati.
- b) Il Fornitore di alloggio deve nominare un amministratore del sistema, che sarà responsabile del controllo dell'accesso degli altri dipendenti e del personale autorizzato al sistema ("Utenti").
- c) Il Fornitore di alloggio è pienamente responsabile per il corretto funzionamento dei requisiti PCI DSS, implementati da Bookassist, in relazione all'amministrazione degli Utenti aventi accesso al sistema, alla protezione dei nomi utente e delle password per il sistema, e in particolare al controllo degli utenti a cui è concesso l'accesso ai dati della carta di credito del titolare della carta. In particolare, il Fornitore di alloggio garantisce
  - o che aderirà ai requisiti di sicurezza PCI DSS;
  - o di riconoscere la propria responsabilità nel proteggere i dati del Titolare della carta;
  - o di riconoscere che i dati del Titolare della carta devono essere utilizzati solo per coadiuvare il completamento di una transazione, supportare un programma di fidelizzazione, fornire un servizio di controllo antifrode, o per usi specificamente richiesti dalla legge;
  - o di fornire piena collaborazione e accesso, ai fini della conduzione di un'accurata revisione della sicurezza dopo un'intrusione di sicurezza, al rappresentante del settore delle carte di pagamento o a terzi autorizzati dal settore delle carte di pagamento;

- o di riconoscere che questi obblighi, volti alla salvaguardia della riservatezza dei dati del Titolare della carta, persisteranno successivamente alla cessazione di qualsiasi altro accordo contrattuale con Bookassist.

- d) Qualsiasi violazione delle norme, delle procedure o delle linee guida stabilite in base a questa informativa deve essere resa nota alla direzione del Fornitore di alloggio, al fine di definire un'adeguata azione in merito. Ciò potrebbe comportare un'azione disciplinare, incluso il licenziamento o la cessazione del servizio e/o l'azione giudiziaria.

## **2. Accesso sulla base di necessità di conoscenza**

L'accesso al sistema a un determinato livello dovrebbe essere consentito solo a quegli Utenti che necessitano specificamente di accedere a tale livello per svolgere il proprio lavoro.

## **3. Accesso e limitazioni dei dati**

- a) L'accesso deve essere consentito solo previa autorizzazione del Fornitore di alloggio.
- b) I dati della carta di credito del cliente potranno essere visualizzati solo fino a un mese dopo la data di partenza presente sulla prenotazione. Successivamente, i dati verranno automaticamente eliminati dal sistema Bookassist e non potranno essere recuperati
- c) Tutti gli altri dati personali del cliente saranno resi anonimi 12 mesi dopo la data di partenza.

## **4. Accessi individuali**

Gli accessi devono essere unici per ciascun Utente. Gli Utenti non possono condividere i propri dati di accesso con altre persone.

## **5. Utenti inattivi**

Gli accessi relativi agli Utenti che non ne necessitano oltre, o che hanno lasciato l'hotel, devono essere immediatamente eliminati

## **6. Nuovi Utenti**

Quando vengono impostati gli accessi per il sistema, l'Utente è obbligato a leggere, comprendere e accettare le condizioni sopra elencate.

## **2) Informazioni sulla protezione dei dati per i dipendenti/per il personale autorizzato che accede al Sistema e/o al Sistema di gestione dei contenuti ("CMS")**

### **1. Informazioni raccolte sui dipendenti/sul personale autorizzato ("Utenti") che accede al Sistema o al CMS, e perché vengono raccolte ed elaborate tali informazioni**

- a) Gli Utenti che accedono al sistema o al CMS sono tenuti a fornire nome, indirizzo e-mail e numero di telefono. Inoltre, il Sistema e il CMS registrano le informazioni di log di tutti gli accessi e di tutte le attività.
- b) La raccolta e l'elaborazione dei dati sono necessarie per la funzionalità del Sistema e del CMS, nonché per analizzare i problemi, così da consentirci di rispondere alle richieste di assistenza.

## **2. Modalità con cui possono essere utilizzati i dati dell'Utente, e chi ha accesso ad essi**

I dati dell'Utente devono essere utilizzati al fine di coadiuvare il funzionamento del Sistema e del CMS. Il Fornitore di alloggio potrebbe richiedere l'accesso ai dati dell'Utente. Si prega di contattare il Fornitore di alloggi pertinente per ricevere informazioni in merito alla modalità con le quali potrebbe utilizzare tali dati Utente. Si noti che se il Fornitore di alloggi ha richiesto i dati dell'Utente, lo stesso potrebbe conservarne l'accesso per un diverso periodo di conservazione.

## **3. Diritti dell'Utente**

Gli Utenti hanno il diritto di richiedere l'accesso, la rettifica e la cancellazione dei propri dati, nonché il diritto alla portabilità dei dati e il diritto di presentare un reclamo all'autorità di vigilanza pertinente, in linea con i requisiti di protezione dei dati pertinenti.

## **4. Conservazione**

Tutti i dati elencati nella sezione 1 saranno conservati da Bookassist per due anni dopo la data di scadenza dell'Utente.

## **5. Contatti**

Per maggiori informazioni, o nel caso desiderassi esercitare i tuoi diritti, puoi inviare un'e-mail alla sezione Protezione dati di Bookassist, all'indirizzo [dpo@bookassist.com](mailto:dpo@bookassist.com).

## **3) Note esplicative sulla politica relativa alle password, per l'utilizzo del sistema**

Gli standard PCI indicano che le password utilizzate nel Sistema devono soddisfare un determinato insieme di regole. La procedura di accesso al Sistema garantisce il rispetto degli standard PCI. La verifica dell'accesso di Bookassist convalida il nome utente e la password e, in caso di errori, mostrerà sullo schermo messaggi chiari, volti a spiegare cosa sia sbagliato e come correggere l'azione eseguita.

### **1. Password sicure**

Seleziona password sicure, aventi le seguenti caratteristiche:

- utilizza sia caratteri maiuscoli che minuscoli, e cifre o segni di punteggiatura
- non utilizzare dati personali o parole di uso comune o reperibili in un dizionario
- non comunicare a nessuno la tua password
- non annotare la tua password e non memorizzarla online.

### **2. Durata della password**

Ogni 90 giorni, il Sistema richiederà il cambio della password. Le chiare istruzioni ti guideranno lungo questo processo.

### **3. Formato della password**

La lunghezza della password deve essere di almeno 7 caratteri, con un minimo di 1 numero e di 1 carattere alfabetico. Nel caso modificassi la password, e questa non soddisfacesse tali requisiti, verrà visualizzato un messaggio sullo schermo, indicante le istruzioni volte a rendere valida la password.

### **4. Cronologia delle password**

Quando modifichi la password, il Sistema verifica che questa non corrisponda ad alcuna delle ultime 4 password.

#### **5. Tentativi di accesso**

Nel caso in cui, effettuando l'accesso, inserissi una password errata, disporrai di un totale di 6 tentativi prima di essere bloccato. In tal caso, si renderà necessario chiedere all'amministratore di reimpostare la password, e attendere 30 minuti prima di poter accedere nuovamente.

#### **6. Periodo di blocco**

Se il Sistema ti ha bloccato perché hai inserito la password errata per sei volte, dovrai attendere 30 minuti prima di poter accedere nuovamente, anche dopo il ripristino della password da parte dell'amministratore.

#### **7. Timeout della sessione**

Lo standard PCI ci impone di limitare una sessione di accesso a 15 minuti di inattività. Se il tuo computer rimarrà inattivo per più di 15 minuti, sarà necessario accedere nuovamente al Sistema.

#### **8. Utente scaduto**

Se non effettuerai l'accesso al Sistema per 90 giorni consecutivi, il tuo nome Utente scadrà e si renderà necessario chiedere all'amministratore di ripristinarlo.

#### **9. Nuovo Utente o Reimpostazione della password**

Nel caso in cui ad un nuovo utente sia stata inviata una password temporanea, o ad un utente che ha richiesto una reimpostazione della password sia stata inviata una nuova password temporanea, tale utente dovrà accedere utilizzando la password temporanea entro 24 ore, termine successivamente al quale l'utente risulterà scaduto e si renderà necessario un ripristino dello stesso da parte dell'amministratore.