Bookassist®

# Extranet-Richtlinie von Bookassist

Letzte Aktualisierung: 25. Mai 2018

Diese Richtlinie enthält:

1) **Allgemeine Geschäftsbedingungen für die Nutzung des Bookassist Administration System („System“)**
2) **Datenschutzinformationen für Mitarbeiter/autorisierte Personen, die auf das System und/oder das Bookassist Content Management System („CMS“) zugreifen**
3) **Erläuterungen zur Passwortrichtlinie für die Nutzung des Systems**

Beachten Sie, dass Sie mit der Verwendung des Bookassist Administration System („System“) Ihre Zustimmung zu den hier beschriebenen Allgemeinen Geschäftsbedingungen bestätigen.

Das System bietet Zugang zu personenbezogenen Daten auf der Grundlage der vertraglichen Verpflichtungen, die im Bookassist-Vertrag mit dem Beherbergungsanbieter und entsprechend den Bookassist-Bedingungen für Datenschutz- und Datenverarbeitung festgelegt sind (https://bookassist.org/dp).

## 1) Allgemeine Geschäftsbedingungen für die Nutzung des Bookassist Administration System („System“)

### 1. Anforderungen nach PCI DSS (Datensicherheitsstandards für die Zahlungskartenindustrie)

a) Während Bookassist sich bemüht, die in den Datensicherheitsstandards für die Zahlungskartenindustrie (PCI DSS) festgelegten Bedingungen für die Verarbeitung von Online-Zahlungen vollständig zu erfüllen, ist der Beherbergungsanbieter voll verantwortlich für die ordnungsgemäße Verwendung der auf dem System bereitgestellten personenbezogenen Daten in Übereinstimmung mit den einschlägigen Datenschutzgesetzen.

b) Der Beherbergungsanbieter muss einen Administrator für das System benennen, der für die Kontrolle des Zugriffs durch andere Mitarbeiter und/oder autorisierte Mitarbeiter auf das System („Benutzer“) verantwortlich ist.

c) Der Beherbergungsanbieter voll verantwortlich ist für die ordnungsgemäße Ausführung der von Bookassist umgesetzten PCI-DSS-Anforderungen in Bezug auf die Verwaltung von Benutzern mit Zugriff auf das System, den Schutz von Benutzernamen und Passwörtern für das System und insbesondere die Kontrolle über Benutzer mit Zugriff auf Kreditkartendaten des Karteninhabers. Insbesondere garantiert der Beherbergungsanbieter, dass

- er die PCI-DSS-Sicherheitsanforderungen einhalten wird;
- er seine Verantwortung für die Sicherung der Karteninhaberdaten bestätigt;
- er bestätigt, dass die Daten des Karteninhabers nur zur Unterstützung der Abwicklung einer Transaktion, zur Unterstützung eines Treueprogramms, zur Bereitstellung eines Betrugsbekämpfungsdienstes oder für gesetzlich vorgeschriebene Verwendungen genutzt werden dürfen;

- er nach einem Sicherheitseingriff bei einem Vertreter der Zahlungskartenindustrie oder einer von der Zahlungskartenindustrie zugelassenen Drittpartei eine vollständige Kooperation und den Zugang für eine gründliche Sicherheitsüberprüfung bietet;
- er bestätigt, dass diese Verpflichtungen zur Wahrung der Vertraulichkeit der Daten des Karteninhabers auch nach Beendigung sonstiger vertraglicher Vereinbarungen mit Bookassist bestehen bleiben.

d) Jeder Verstoß gegen Standards, Verfahren oder Richtlinien, die gemäß dieser Richtlinie festgelegt werden, müssen dem Management des Beherbergungsanbieters vorgelegt werden, damit er entsprechende Maßnahmen ergreifen kann. Dies könnte zu Disziplinarmaßnahmen führen, einschließlich der Entlassung oder Einstellung des Dienstes und/oder einer Strafverfolgung.

**2. Zugriff auf Notwendigkeitsbasis**

Der Zugriff auf das System auf einer bestimmten Ebene sollte nur denjenigen Benutzern gewährt werden, die speziell auf dieser Ebene Zugriff benötigen, um ihre Arbeit auszuführen.

**3. Zugriffs- und Datenbeschränkungen**

a) Der Zugang sollte nur gewährt werden, wenn dies vom Beherbergungsanbieter genehmigt wurde.

b) Kundenkreditkartendaten können nur bis zu einem Monat nach dem Abreisedatum der Buchung angezeigt werden. Danach werden die Daten automatisch aus dem Bookassist-System gelöscht und können nicht mehr abgerufen werden.

c) Alle anderen personenbezogenen Daten werden 12 Monate nach dem Abreisedatum anonymisiert.

**4. Individuelle Logins**

Logins müssen für jeden Benutzer einzeln erfolgen und eindeutig sein. Benutzer dürfen ihre Logins nicht mit anderen teilen.

**5. Inaktive Benutzer**

Logins sollten für die Benutzer sofort gelöscht werden, die sie nicht mehr benötigen oder das Hotel verlassen haben.

**6. Neue Benutzer**

Wenn Logins für das System eingerichtet werden, ist der Benutzer verpflichtet, die oben aufgeführten Bedingungen zu lesen, zu verstehen und zu akzeptieren.

## 2) Datenschutzinformationen für Mitarbeiter/autorisierte Personen, die auf das System und/oder das Bookassist Content Management System („CMS“) zugreifen

**1. Erfasste Informationen über Mitarbeiter/autorisiertes Personal („Benutzer“), die auf das System oder das CMS zugreifen, und warum diese erfasst und verarbeitet wird**

a) Benutzer, die auf das System oder das CMS zugreifen, müssen den Namen, die E-Mail-Adresse und die Telefonnummer angeben. Darüber hinaus protokollieren das System und das CMS Informationen über alle Zugriffe und Aktivitäten.

b) Eine derartige Erfassung und Verarbeitung von Daten ist notwendig für die Funktionalität des Systems und des CMS sowie um Probleme zu analysieren, damit wir auf Anliegen reagieren können.

**2. Wie können die Benutzerdaten verwendet werden und wer hat Zugriff darauf?**

Die Benutzerdaten sollen verwendet werden, um die Funktion des Systems und des CMS zu unterstützen. Der Beherbergungsanbieter kann Zugriff auf Benutzerdaten anfordern. Bitte wenden Sie sich an den jeweiligen Beherbergungsanbieter, um zu erfahren, wie er diese Benutzerdaten möglicherweise verwendet. Bitte beachten Sie, dass, wenn der Beherbergungsanbieter die Benutzerdaten anfordert, der Beherbergungsanbieter den Zugriff für eine andere Aufbewahrungsfrist beibehalten kann.

**3. Rechte des Benutzers**

Benutzer haben das Recht, Zugang zu ihren Daten zu verlangen, sie zu berichtigen und zu löschen, sowie das Recht auf Datenübertragbarkeit und das Recht, bei der zuständigen Aufsichtsbehörde eine Beschwerde einzureichen, die den Datenschutzanforderungen entspricht.

**4. Aufbewahrung**

Alle in Abschnitt 1 aufgeführten Daten werden von Bookassist für zwei Jahre nach dem Benutzer-Ablaufdatum aufbewahrt.

**5. Kontakt**

Sie können den Bookassist-Datenschutz unter dpo@bookassist.com per E-Mail kontaktieren, wenn Sie weitere Informationen benötigen oder Ihre Rechte ausüben möchten.

## 3) Erläuterungen zur Passwortrichtlinie für die Nutzung des Systems

PCI-Standards bedeuten, dass für Passwörter, die Sie auf dem System verwenden, bestimmte Regeln erfüllt werden müssen. Die Anmeldeprozedur auf dem System stellt sicher, dass die PCI-Standards eingehalten werden. Die Login-Prüfung von Bookassist überprüft den Benutzernamen und das Passwort, und bei Fehlern werden auf dem Bildschirm eindeutige Meldungen angezeigt, die erklären, was nicht in Ordnung ist und wie die Fehler korrigiert werden können.

**1. Starke Passwörter**

Wählen Sie starke Passwörter mit den folgenden Eigenschaften:

- Verwenden Sie Groß- und Kleinbuchstaben sowie Ziffern oder Interpunktionszeichen.
- Verwenden Sie keine persönlichen Informationen oder Wörter, die häufig verwendet oder in einem Wörterbuch gefunden werden.
- Teilen Sie ein Passwort nicht mit einer anderen Person.
- Schreiben Sie kein Passwort auf und speichern Sie es nicht online.

**2. Geltungsdauer des Passworts**

Alle 90 Tage werden Sie vom System aufgefordert, Ihr Passwort zu ändern. Klare Anweisungen führen Sie durch diesen Prozess.

**3. Passwortformat**

Das Passwort muss mindestens 7 Zeichen lang sein und mindestens 1 Ziffer und 1 Buchstaben enthalten. Wenn Sie Ihr Passwort ändern und es diesen Anforderungen nicht entspricht, wird eine Bildschirmmeldung angezeigt, in der Sie darüber informiert werden, was zu tun ist, um das Passwort gültig zu machen.

**4. Passworthistorie**

Wenn Sie Ihr Passwort ändern, überprüft das System, ob es mit einem Ihrer letzten 4 Passwörter übereinstimmt.

**5. Login-Versuche**

Wenn Sie sich anmelden und ein falsches Passwort eingeben, haben Sie insgesamt 6 Versuche, bevor Sie gesperrt werden. In diesem Fall sollten Sie Ihren Administrator bitten, das Passwort zurückzusetzen und 30 Minuten warten, bevor Sie sich erneut anmelden.

**6. Sperrzeit**

Wenn Sie vom System gesperrt wurden, weil Sie sechsmal ein falsches Passwort eingegeben haben, müssen Sie 30 Minuten warten, bevor Sie sich wieder anmelden können, auch nachdem der Administrator Ihr Passwort zurückgesetzt hat.

**7. Sitzungs-Timeout**

PCI fordert von uns, dass wir eine Anmeldesitzung auf 15 Minuten Nichtaktivität begrenzen. Wenn Ihr Computer länger als 15 Minuten nicht benutzt wurde, müssen Sie sich erneut im System anmelden.

**8. Benutzer abgelaufen**

Wenn Sie sich nicht innerhalb von 90 Tagen beim System angemeldet haben, läuft Ihr Benutzer ab und Sie müssen Ihren Administrator bitten, ihn zurückzusetzen.

**9. Neuer Benutzer oder Passwort-Zurücksetzung**

Für einen neuen Benutzer, dem ein temporäres Passwort gesendet wurde, oder für einen Benutzer, der ein Zurücksetzen des Passworts angefordert hat und dem ein neues temporäres Passwort gesendet wurde, muss sich der Benutzer innerhalb von 24 Stunden mit dem temporären Passwort anmelden. Danach ist es abgelaufen und der Administrator muss es zurücksetzen.