„Der digitale Hotelmeldeschein“

Häufig gestellte Fragen und Antworten (FAQ)

Stand: 28. Januar 2021, 14:00 Uhr

„Der digitale Hotelmeldeschein“

Häufig gestellte Fragen und Antworten (FAQ)

Stand: 28. Januar 2021

Mit dem Dritten Bürokratieentlastungsgesetz (BEG III) novellierte der Gesetzgeber Ende 2019 auch das Bundesmeldegesetz (BMG) und ebnete den Weg zu einer digitalen Erfüllung der Hotelmeldepflicht. Mit Inkrafttreten des novellierten Bundesmeldegesetzes am 1. Januar 2020 wurde der Weg für den – so nicht ganz zutreffend benannten – „digitalen Hotelmeldeschein“ rechtlich frei, den der Hotelverband mehr als zwei Jahrzehnte lang von der Politik gefordert hatte.

Neben dem „digitalen“ Check-in bleibt die altbewährte „analoge“ Variante eine gleichberechtigte Alternative, die entweder weiterhin ausschließlich oder ergänzend zum Einsatz kommen wird. Hieraus ergeben sich eine ganze Reihe von Fragen, auf die wir mit dieser Veröffentlichung bestmöglich – aber ohne rechtliche Gewähr – Antworten geben wollen, um das Umstellen auf ein digitales Hotelmeldeverfahren zu erleichtern und Fehlinvestitionen zu vermeiden.

A. Grundsätzliches

I. Welche Möglichkeiten des elektronischen Check-ins sieht das Bundesmeldegesetz überhaupt vor?

Das Bundesmeldegesetz sieht zwei voneinander unabhängige Alternativen für einen digitalen Check-in im Hotel vor: Zum einen kann die Identifizierung des Gastes bei einem kartengebundenen Zahlungsvorgang mittels Starker Kundenauthentifizierung erfolgen. Zum anderen ist der elektronische Identitätsnachweis mit dem Online-Ausweis des Personalausweises, des elektronischen Aufenthaltstitels oder der eID-Karte für EU/EWR-Bürger möglich.

1. Kartengebundener Zahlungsvorgang mit Starker Kundenauthentifizierung

Mit den neuen Regelungen im Bundesmeldegesetz wird eine ausschließlich elektronische Speicherung der melderechtlich zu erhebenden Daten zugelassen, wenn die Speicherung mit einem elektronischen, kartengebundenen Zahlungs- oder Reservierungsvorgang des Hotelgastes am Tag

der Ankunft unter Anwendung einer Starken Kundenauthentifizierung (auch Strong Customer Authentication, SCA) verknüpft wird.

Die Starke Kundenauthentifizierung ist Bestandteil der Anforderungen der europäischen Zahlungsdienste-Richtlinie und eine EU-weite Anforderung an die Art der Authentifizierung elektronischer Zahlungen. Neben Deutschland sind auch alle anderen EU-Mitglieder, aber auch Länder des Europäischen Wirtschaftsraumes (EWR) davon betroffen, die eine richtlinienkonforme Umsetzung gewährleisten müssen.

Wer über eine Debit- oder Kreditkarte verfügt, hat sich bereits gegenüber seiner Bank authentifiziert und seine Identität persönlich und unter Vorlage eines gültigen Ausweisdokuments bestätigt. Durch den mit der Hotelanmeldung verknüpften kartengebundenen Zahlungsvorgang können im Bedarfsfall die hierzu berechtigten Behörden die Identität des im Hotel einchecken den Gastes im Nachhinein über den Bankensektor überprüfen.

2. Identifizierung mit Personaldokumenten

Eine elektronische Speicherung der Daten ist auch zulässig, wenn der Hotelgast einer Erfassung seiner melderechtlich vom Hotel zu erhebenden Daten mithilfe seines deutschen Personalausweises, seines in Deutschland ausgegebenen elektronischen Aufenthaltstitels oder mithilfe seiner eID-Karte für EU/EWR-Bürger zustimmt.

Der Identitätsnachweis und die Datenerhebung können dabei auf zwei Wegen erfolgen:

- Durch Identifizierung des Gastes mit einem eingeschalteten Online-Ausweis (das heißt aktivierter Funktion zum elektronischen Identitätsnachweis) seines Personalausweises, seines elektronischen Aufenthaltstitels oder seiner eID-Karte für EU/EWR-Bürger, Eingabe seiner Geheimnummer (PIN) an einem Terminal mit Kartenlesegerät oder mittels NFC-fähigen Mobilgerät und anschließender Datenübermittlung aus dem elektronischen Speichermedium des Personalausweises, des elektronischen Aufenthaltstitels beziehungsweise der eID-Karte für EU/EWR-Bürger am Tag der Ankunft;

- Durch Identifizierung des Gastes durch die/den Rezeptionistin/en mittels eines Lichtbildabgleichs mit dem vorgelegten Personalausweis, elektronischen Aufenthaltstitel, oder einem Reisepass beziehungsweise anderen amtlichen Personendokument eines anderen Mitglieds-

staates der EU oder EWR am Tag der Ankunft. Die Datenübermittlung geschieht dabei im Anschluss nach erfolgter Einwilligung des Gastes im Wege des sogenannten Vor-Ort-Auslesens der Daten vom elektronischen Speichermedium der Ausweiskarte nach Eingabe der Zugangsnummer (sog. Card Access Number, CAN) durch die/den Rezeptionistin/en am Terminal mit einer Kartenleseeinheit. Die sechsstellige CAN befindet sich auf den genannten Ausweiskarten auf der Vorderseite rechts unten über oder neben der Unterschrift.

II. Können Hotelgäste alternativ auch auf einem Unterschriftenpad, Smartphone oder Tablet unterschreiben und dadurch die melderechtlich zu erhebenden Daten bestätigen?

Die Bestätigung der melderechtlich zu erhebenden Daten mittels Unterschrift auf einem Eingabefeld, wie sie unter anderem bei Paketzustellern oder Mietwagenfirmen mittlerweile üblich ist, ist beim Check-in im Hotel weiterhin gesetzlich nicht zulässig. Die Aufzählung der elektronischen Identifikationsverfahren ist im Bundesmeldegesetz abschließend geregelt.

III. Darf der Hotelier weiterhin ausschließlich den papierhaften Meldeschein zur Datenerfassung des Gastes nutzen und nur diesen vorlegen?

Ja. Erklärtes Ziel der Novellierung des Bundesmeldegesetzes ist die ergänzende Öffnung des Meldeerfordernisses im Beherbergungsgewerbe für digitale Lösungen unter gleichzeitiger Erhaltung des bereits bestehenden papierhaften Verfahrens. Damit obliegt dem Hotelier die Wahlmöglichkeit zwischen neuen digitalen Lösungen und/oder der gängigen Praxis wie bisher. Beispielsweise wird bei nichteuropäischen ausländischen Gästen regelmäßig eine Starke Kundenauthentifizierung bei kartengebundenen Zahlungsvorgängen (noch) nicht möglich sein, so dass in diesen Fällen eine papierhafte Erfüllung der Hotelmeldepflicht der Standard bleiben wird.

IV. Was passiert, wenn eine elektronische Datenerhebung vom Gast nicht gewünscht wird?

Das Bundesmeldegesetz setzt ausdrücklich die Zustimmung der beherbergten Person in die elektronische Datenerhebung voraus. Verweigert ein Hotelgast

demnach seine Zustimmung, muss der papierhafte Meldeschein vom Hotelier vorgelegt und seitens des Gastes unterschrieben werden.

Achtung: Sofern auf der Homepage, über das Buchungsportal oder im persönlichen Kontakt im Voraus zweifelsfrei darüber informiert wurde, dass im Hotel beispielsweise einzig ein elektronischer Check-in z.B. über einen Automaten möglich ist und der Gast in Kenntnis dessen bucht, gehen wir davon aus, dass der Gast auch seine konkludente Zustimmung zu diesem Verfahren erteilt hat und beim möglicherweise nächtlichen Eintreffen nicht auf einem papierhaften Meldeschein statt der Nutzung des Check-in-Automaten beharren kann.

V. Dürfen die melderechtlich relevanten Daten tatsächlich erst am Tag der Ankunft gespeichert werden?

Die Meldedaten der Gäste dürfen auch schon vor dem Tag der Anreise, beispielsweise zum Zeitpunkt der Reservierung, zweckgebunden gespeichert werden. Auch können bestimmte Daten beispielsweise per Pre-Stay-E-Mail beim Gast abgefragt werden. Dem Gast kann die Datenübermittlung zudem mittels elektronischen Identitätsnachweises über das Internet mit seinem Online-Ausweis eingeräumt werden.

Weiterhin müssen die Datensätze der Hotelgäste am Tag der Ankunft vervollständigt werden, sollten vorher noch einzelne melderechtlich notwendige Angaben gefehlt haben.

Für den elektronischen Check-in ist es aber in jedem Fall erforderlich, dass die zu beherbergende Person die Richtigkeit und Vollständigkeit ihrer elektronisch erhobenen Daten und ihre tatsächliche Anreise am Tag der Ankunft bestätigt, auch wenn diese Daten möglicherweise schon vorher komplett gespeichert wurden.

VI. Wie müssen die zu speichernden Datensätze angelegt werden und ausgestaltet sein?

Die dateispezifischen, wesentlichen Anforderungen an die Datenspeicherung regelt die Beherbergungsmeldedatenverordnung (BeherbMeldV). Dort finden sich die technischen Vorgaben zum Dateiformat, zur Anordnung und Namensgebung der Dateien sowie zu deren Struktur.

Die Daten sind als strukturierter, maschinenlesbarer Datensatz im Dateiformat der Extensible Markup Language (XML) zu speichern. Weiterhin sind die Daten im UNICODE-Zeichensatz UTF 8 zu codieren.

Die Datei ist nach dem Muster „JJJJMMTT_BeherbMeldeschein_Zaehler.xml“ zu benennen. Die Datensätze sind schließlich sortiert in Ordnerstrukturen nach Jahren und Monaten zu speichern.

Das Bundesministerium des Innern, für Bau und Heimat hat dazu die Schema-Definition und eine Beispiel-XML auf seiner Webseite veröffentlicht: www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2020/07/schema-beherbmeldv.html. Im Sinne des Datenschutzes ist dabei sicherzustellen, dass keine unbefugten Personen Zugriff auf diese Daten erlangen.

VII. Wie werden die Daten exportiert?

Die gemäß Bundesmeldegesetz erhobenen Gästedaten müssen den berechtigten Behörden nur auf deren Verlangen zur Verfügung gestellt werden. Dies hat über eine Datenschnittstelle zu den zuständigen Behörden oder durch Übergabe eines Datenträgers zu erfolgen.

VIII. Wie lange müssen die elektronischen Daten des Gastes gespeichert werden?

Auch die auf elektronischem Wege erlangten, melderechtlich zu erhebenden Daten sind zwölf Monate aufzubewahren.

Sofern eine Starke Kundenauthentifizierung des Gastes erfolgt ist, muss auch die zweckgebundene Zuordnungsnummer des eingesetzten Zahlungsmittels (der sogenannte „Token“) zusammen mit den Daten des Gastes ein Jahr lang gespeichert werden.

Innerhalb von drei Monaten nach Ablauf des Jahres sind die Gästedaten sodann zu löschen/zu vernichten.

B. Kartengebundener Zahlungsvorgang mit Starker Kundenauthentifizierung (SCA)

I. Wie lässt sich ein elektronischer Check-in mittels kartengebundenem Zahlungsvorgang mit Starker Kundenauthentifizierung umsetzen?

1. Kartenzahlung an der Rezeption

Eine Kreditkarte wird für die Zahlung oder Reservierung eines Betrages beim Check-in vom Gast an der Rezeption vorgelegt und durch den/die Mitarbeiter/in oder dem Gast in ein Zahlungsterminal eingelesen. Die Starke Kundenauthentifizierung erfolgt in aller Regel durch Eingabe der PIN, die den Karteninhaber identifiziert.

2. Check-in-Terminal

Der Check-in kann auch unabhängig vom Hotelpersonal an einem Terminal erfolgen. Dabei wird ebenfalls der Einsatz einer Kreditkarte zur Bezahlung oder Reservierung eines Betrages verlangt. Auch hier wird eine Starke Kundenauthentifizierung durchgeführt. Sind alle Eingaben abgeschlossen und die Daten vom Hotelgast bestätigt, erhält er in der Regel seinen Zimmerschlüssel in Form einer Key Card oder eines Zugangscodes zum Zimmer.

3. App

Der Check-in im Hotel ist vielerorts auch über eine auf einem Smartphone oder Tablet gespeicherte App des Hotels möglich. Während des Buchungsvorgangs wird der Gast zur Eingabe seiner persönlichen Daten, unter anderem auch der melderechtlich zu erhebenden Daten, aufgefordert. Im System kann der Gast ggf. auch seine Kreditkartendaten hinterlegen. Abgeschlossen wird der Check-in-Vorgang dann am Tag der Ankunft mit Eingabe der PIN oder einem biometrischen Verfahren, wie etwa einem auf dem Smartphone oder dem Tablet gespeicherten Fingerabdruck des Gastes oder einer digitalen Gesichtserkennung.

II. Muss zwangsläufig eine kartengebundene Zahlung des Gastes erfolgen, um eine Starke Kundenauthentifizierung auszulösen?

Als Zahlungsvorgang zählt laut Zahlungsdienste-Richtlinie auch die Reservierung eines Betrages auf der Kreditkarte (mit entsprechender Aufklärung und Zustimmung des Gastes, bestätigt durch eine Starke Kundenauthentifizierung).

Ist dies nicht gewünscht kann auch eine Zahlung von 0,00 € durch den Gast ausgelöst und mittels Starker Kundenauthentifizierung bestätigt werden. Der Gast muss also zum Zeitpunkt des Check-ins nicht zwingend einen Eurobetrag an das Hotel übermitteln.

III. Wie erfolgt die Erhebung und Speicherung der Gästedaten infolge der Starken Kundenauthentifizierung?

Die Starke Kundenauthentifizierung erfordert mindestens zwei voneinander unabhängige Elemente der Kategorien Wissen (z. B. die PIN), Besitz (z. B. der Chip auf der Debit- oder Kreditkarte) und Inhärenz (z. B. ein Fingerabdruck). Die handschriftliche Unterschrift auf dem papiergebundenen Meldeschein wird in diesem Fall ersetzt durch die Speicherung einer zweckgebundenen Zuordnungsnummer für wiederkehrende Zahlungen, dem sogenannten „Token“.

Dieser Token wird im Zuge der Abwicklung zwischen Hotel und kartenausgebender Stelle oder bei jedem Einsatz einer Zahlungskarte generiert und ermöglicht, die Zahlung einem bestimmten Karteninhaberkonto und damit einer bestimmten Person zuzuordnen. Nur dadurch kann auf eine eigenhändige Unterschrift des Gastes auf dem Meldeschein als eindeutigem Identifizierungsmerkmal verzichtet werden.

IV. Wie gelangt das Hotel an jene Gästedaten, die der Gast bei der Buchung regelmäßig nicht angibt, wie beispielsweise das Geburtsdatum oder die Staatsangehörigkeit?

Im Rahmen des Check-ins muss der/die Rezeptionist/-in auch weiterhin das Geburtsdatum des Gastes und die Staatsangehörigkeit in Erfahrung bringen und in das System eingeben.

Beim digitalen Check-in wird regelmäßig ein Teil der notwendigen Meldedaten schon aus der Buchung vorliegen, so dass diese dem Gast beim Check-in auf

einem Display angezeigt werden können und dieser dann nur noch die fehlenden Angaben ergänzen muss.

V. Wie findet die Bestätigung der Richtigkeit und Vollständigkeit der Daten statt?

Die Bestätigung der Richtigkeit und Vollständigkeit der Daten erfolgt durch den Gast, indem er einen kartengebundenen Zahlungsvorgang mittels Starker Kundenauthentifizierung auslöst. Das Hotel hat den Gast hierauf hinzuweisen.

VI. Wann hat die Starke Kundenauthentifizierung zu erfolgen?

Die Starke Kundenauthentifizierung muss zwingend am Tag der Ankunft durchgeführt werden. Den rechtlichen Erfordernissen wird nicht genügt, wenn die Starke Kundenauthentifizierung schon im Vorhinein, beispielsweise im Rahmen der Online-Reservierung oder einer vorherigen Anzahlung, erfolgt.

VII. Wie verhält es sich, wenn ein anderer für den Gast mit einer anderen Kreditkarte zahlt?

Wichtig ist, dass eine Starke Kundenauthentifizierung am Tag der Ankunft durchgeführt wird, sei es durch den Gast persönlich oder eine dritte Person, die als berechtigte Kartennutzer ja vermutlich in einem persönlichen oder geschäftlichen Verhältnis zur beherbergten Person steht.

VIII. Wie verhält es sich, wenn der Gast zur Barzahlung wechselt?

In Fällen, in denen ein Hotelgast zum Zeitpunkt des Check-ins via Kreditkarte authentifiziert wurde und seinen Aufenthalt später aber mithilfe eines Zahlungsmittels ohne Starke Kundenauthentifizierung bezahlt, beispielsweise durch Barzahlung oder mittels einer außereuropäischen Kreditkarte, müssen die eingangs erhobenen Daten weiterhin gespeichert bleiben.

IX. Kann es sein, dass die Kreditkarte eines Hotelgastes nicht SCA-fähig ist?

Die Umsetzung der Starken Kundenauthentifizierung ist eine verbindliche Anforderung der EU-Zahlungsdienste-Richtlinie. In der Europäischen Union ansässige Kartenherausgeber geben nur noch Kreditkarten aus, die über eine Starke Kundenauthentifizierung verfügen. Damit dürften auch in Deutschland faktisch bald kaum noch Karten im Umlauf sein, die bei ihrem Einsatz keine Starke Kundenauthentifizierung erfordern/anfordern.

Anders verhält es sich mit Zahlungskarten von Gästen außerhalb der EU und des Europäischen Wirtschaftsraums, deren Kreditkarten bis auf weiteres kein Erfordernis einer Starken Kundenauthentifizierung aufweisen/auslösen.

X. Verstößt die 12-monatige Speicherung des Tokens möglicherweise gegen die PCI-Compliance?

Sowohl die 12-monatige Speicherung des „Tokens“ im Hotel, als auch beim Zahlungsdienstleister ist PCI-compliant (Abkürzung für Payment Card Industry Data Security Standard, PCI-DSS). Sämtliche Daten sind verschlüsselt und für Unbefugte weder einsehbar, noch zu entschlüsseln.

XI. Wie wirkt es sich aus, wenn die Kreditkarte des Gastes nur noch weniger als zwölf Monate gültig ist?

Der Hotelier muss lediglich darauf achten, dass die Kreditkarte des Gastes zum Zeitpunkt der Starken Kundenauthentifizierung noch gültig ist. Danach ist es für das Hotel melderechtlich irrelevant, wann die Kreditkarte des Gastes ihre Gültigkeit verliert. Die melderechtlich zu erhebenden Daten liegen vor und sind für den Zeitraum von 12 Monaten abgespeichert.

C. Identifizierung mit Personaldokumenten

I. Der elektronische Identitätsnachweis mit dem Online-Ausweis

Alternativ zur Verknüpfung mit Zahlungsdaten ist eine elektronische Speicherung der Daten auch möglich, wenn der Gast der Erfassung und Übermittlung seiner Daten nach erfolgreichem elektronischem Identitätsnachweis mit dem

Online-Ausweis des Personalausweises, des elektronischen Aufenthaltstitels oder der eID-Karte für EU/EWR-Bürger zustimmt.

Um dieses Vorgehen anbieten zu können, muss ein Hotelier gewisse Voraussetzungen erfüllen:

- Besitz eines Berechtigungszertifikats von der Vergabestelle für Berechtigungszertifikate (VfB) beim Bundesverwaltungsamt
  (Formulare unter:
  https://www.personalausweisportal.de/Webs/PA/DE/wirtschaft/diensteanbieter-werden/schriftlicher-antrag/schriftlicher-antrag-node.html);
- Besitz eines technischen Berechtigungszertifikats
  (Formulare unter:
  https://www.personalausweisportal.de/Webs/PA/DE/wirtschaft/technik/berechtigungszertifikate/berechtigungszertifikate-node.html);
- Einrichtung eines eigenen eID-Servers oder Auswahl eines eID-Service-Providers.

Eine ausführliche Übersicht zum Thema „Das Hotel als Diensteanbieter“ bietet das Bundesministerium des Innern, für Bau und Heimat auf seiner Homepage.

Grundsätzlich steht es dem Hotelier auch frei, einen Identifizierungsdiensteanbieter mit dem technischen Teil des Verfahrens (Technisches Berechtigungszertifikat, eID-Server/Service) zu beauftragen. Dieser übernimmt sodann die Identifizierung der Gäste als Dienstleistung.

Nicht nur den Hotelier, sondern auch den Gast treffen gewisse Pflichten, um den elektronischen Identitätsnachweis mit dem Online-Ausweis zu ermöglichen:

- Freischaltung der Online-Ausweisfunktion;
- Kenntnis der eigenen PIN.

Für den elektronischen Identitätsnachweis mit dem Online-Ausweis wird folgender Ablauf in Gang gesetzt:

- Der Onlinedienst des Hotels bittet den Gast sich auszuweisen;
- Der Gast stellt die Verbindung zwischen Ausweisdokument und Smartphone oder Kartenleser her;
- Der Gast kann sehen, wer seine Daten abfragen möchte und welche Daten benötigt werden;
- Der Gast stimmt durch Eingabe der selbstgewählten, sechsstelligen PIN einer Datenübertragung zu;
- Der im Ausweisdokument integrierte Chip prüft, ob der Anbieter des Onlinedienstes des Hotels die staatliche Berechtigung zur Abfrage der Daten besitzt.

Eine ausführliche Übersicht zum Thema „Ihr Personalausweis – digital, online und sicher“ bietet das Bundesministerium des Innern, für Bau und Heimat auf seiner Homepage.

II. Vor-Ort-Auslesen von Personaldokumenten an der Rezeption

Durch das Vor-Ort-Auslesen von Personaldokumenten an der Rezeption können Gästedaten direkt in ein elektronisches Formular übernommen werden.

Auch um dieses Vorgehen anbieten zu können, muss ein Hotelier gewisse Voraussetzungen erfüllen. Diese gleichen denen für den elektronischen Identitätsnachweis mit dem Online-Ausweis (siehe vorherige Seite 10).

Eine Aktivierung der Online-Ausweisfunktion des Ausweisdokuments oder eine Geheimnummer (PIN) sind für diese Form der Datenübertragung nicht nötig.

Für das Vor-Ort-Auslesen von Personaldokumenten an der Rezeption wird folgender Ablauf in Gang gesetzt:

- Der Gast weist sich vor Ort an der Rezeption mit seinem Personaldokument aus
- Der/die Rezeptionist/-in führt einen Lichtbildabgleich durch;
- Der Personalausweis, der elektronische Aufenthaltstitel oder die eID-Karte für EU/EWR-Bürger wird auf das Lesegerät gelegt;
- Über den Chip in der Karte wird geprüft, ob das Hotel die Daten des Gastes abfragen darf;
- Die Zugangsnummer (CAN) wird eingegeben und bestätigt;
- Die Daten des Gastes werden wie auf Knopfdruck sicher verschlüsselt und fehlerfrei in das Formular übertragen.