Rechtssicher in der Cloud mit der richtigen Software

Die sichere Verwahrung der Gästedaten ist jedem Hotelier ein Anliegen. Doch die Wahl eines DSGVO-konformen Cloudsoftwaresystems birgt einige Tücken – und kann im Zweifel ernsthafte Konsequenzen nach sich ziehen. Dr. Michael Toedt vom Spezialisten für Datenmanagement Dailypoint erläutert, wie Gastgeber die richtige Entscheidung treffen.

Spätestens mit der Einführung der Datenschutzgrundverordnung (DSGVO) muss Datenschutz bei Hoteliers ganz oben auf der Agenda stehen. Doch gerade bei der Auswahl von Cloudsoftwaresystemen wird in der Praxis häufig unwissentlich fahrlässig gegen die geltende Rechtsprechung verstoßen.

Wenn der Cloudanbieter außerhalb der EU sitzt

Jeder Cloudanbieter ist heute gezwungen, ausreichende technische und organisatorische Maßnahmen bezüglich des Datenschutzes und der Datensicherheit zu treffen. Darunter fallen Regelungen zu etwaigen Unterauftragnehmern wie etwa Hosting-Anbietern oder integrierten Softwarebestandteilen. Beides ist in aller Regel in Form der sogenannten Auftragsverarbeitungsvereinbarung (AVV) auch Teil der Softwareverträge. Diese werden jedoch – so zeigt die Erfahrung – durch den Auftragnehmer, also das Hotel, vor Abschluss eher selten datenschutztechnisch umfassend geprüft – mit gefährlichen Folgen. Denn seit 2020 gibt es eine folgenreiche Gerichtsentscheidung, die für alle Fälle grundlegende Bedeutung hat, in denen entweder der Cloudanbieter selbst oder einer seiner Unterauftragnehmer nicht in der EU oder im Europäischen Wirtschaftsraum (EWR), sondern außerhalb ansässig ist. Dies trifft gerade in der Hotellerie auf viele große Softwareanbieter zu.

Hintergrund: Schutz vor US-Behörden

Im Juli 2020 hat der Europäische Gerichtshof (EuGH) den Nachfolger des „Safe-Harbor-Abkommens“, das „Privacy Shield Framework“ zwischen den USA und der Europäischen Union, für ungültig erklärt. Das bedeutet, dass personenbezogene Daten, die auf Basis dieses Abkommens zu Empfängern in den USA übermittelt wurden, nicht mehr dorthin transferiert werden dürfen. Dies betrifft Cloudsoftwareanbieter und Hosting-Firmen in den USA genauso wie sämtliche Unterauftragnehmer in den USA. Wer also seine Gastdaten mittels eines US-Cloudsoftwareanbieters verarbeitet oder diese in einer Hosting-Umgebung in den USA speichert, begeht – soweit dies weiterhin vor dem Hintergrund des „Privacy Shields“ geschieht – einen Datenschutzverstoß, der mit einer Geldbuße von bis zu vier Prozent des letztjährigen weltweiten Umsatzes geahndet werden kann.

Dr. Michael Toedt ist Gründer und CEO des Datenmanagement-Unternehmens Dailypoint.

Laut DSGVO dürfen personenbezogene Daten nur dann außerhalb der EU transferiert werden, wenn ein gewisses Schutzniveau gewährleistet werden kann (DSGVO Artikel 44, Allgemeine Grundsätze der Datenübermittlung). Der Grund für das Gerichtsurteil ist der Umstand, dass der „Privacy Shield“ für die bei den US-Unternehmen gespeicherten Daten keinen ausreichenden Schutz vor Zugriffen von US-Behörden bieten könne, da er zwar die US-Unternehmen binde, nicht aber staatliche Ermittlungsbehörden in den USA. Das EU-Gericht, das einige Jahre zuvor auch schon das „Safe-Harbor-Abkommen“ als Vorgängerregelung gekippt hatte, sieht darin einen gravierenden Verstoß gegen die hohen europäischen Datenschutzvorgaben zum Schutz der Betroffenen, im Hotelbereich primär der Hotelgäste.

Schutz der Privatsphäre bei Hotelgästen

Diese Rechtsauffassung ist durchaus nachvollziehbar und hat speziell für die Hotellerie eine große Bedeutung. Auf der einen Seite versuchen Hotels alles, um ihre Gäste und deren Privatsphäre zu schützen. Auf der anderen Seite werden die Daten der Gäste aber häufig ohne deren Wissen oder Einwilligung in ein Land außerhalb der EU, wie etwa in die USA, transferiert und damit dortigen Behördenzugriffen zugänglich gemacht.

Sind EU-Standarddatenschutzverträge ausreichend?

Als Alternative zum „Privacy Shield“ konnte man bislang von der EU standardmäßig fest vorgegebene Datenschutzverträge abschließen, die sogenannten EU-Standard-

Bild: Dailypoint

datenschutzverträge. Diese waren zwar nicht gegenständlich im Verfahren des EuGH, sodass der EuGH über diese nicht urteilen durfte. Da aber auch Verträge nie einen nationalen Geheimdienst oder Ermittlungsbehörden binden können, sondern nur die beiden Vertragsparteien – also das Hotel und den US-Cloudanbieter –, lassen sich in rechtlicher Hinsicht die Überlegungen des EuGH in weiten Teilen auch auf die EU-Standardverträge übertragen.

Nach Meinung der EU-Datenschutzbehörden in Form des Europäischen Datenschutzausschusses ist es so, dass speziell für die USA auch der Abschluss solcher EU-Standarddatenschutzverträge nicht mehr ausreicht – es sei denn, die Daten können so streng und sicher verschlüsselt beim US-Anbieter abgelegt werden, dass ein Zugriff von Ermittlungsbehörden und Geheimdiensten nicht mehr möglich ist.

Datenverschlüsselung mit Tücken

Eine solche strenge Verschlüsselung ist durchaus denkbar. Allerdings ist dies bislang weitestgehend nur für Daten im Rahmen eines Hostings möglich. Hinsichtlich cloudbasierter SaaS-(Software-as-a-Service-)Lösungen oder anderer typischer Cloudanwendungen, die nicht nur aus einem Hosting der Daten bestehen, sondern bei denen es um echte Softwarefunktionalitäten geht, ist dies bislang in der Praxis kaum möglich.

Quasi-Verbot von Einsatz der US-Cloudsoftware

Selbst die großen US-Unternehmen bieten keine technischen Lösungen an, bei denen bei SaaS- oder Cloudanwendungen die Daten durchgängig verschlüsselt sind und somit nicht einmal die Cloudanbieter selbst Zugriff haben, aber dennoch die Funktionalitäten anbieten können. Es gibt zwar rechtlich kleinere Ausnahmemöglichkeiten. Für die große Masse von Fällen sowie beim Einsatz von US-Cloudanwendungen im Massengeschäft spielen diese aber bislang keine Rolle. Faktisch kommt daher die aktuelle Ansicht der Datenschutzbehörden in der EU einem weitgehenden Verbot des Einsatzes von US-Cloudsoftware gleich.

ÜBER DAILYPOINT

Dailypoint ist eine der führenden Daten-Management- und CRM-Plattformen für Individualhotels und Hotelgruppen. Die Firma sammelt Daten aus allen relevanten Quellen wie PMS, POS, Webseite, Newsletter oder WLAN und erstellt automatisch ein zentrales und konsolidiertes Gastprofil.

Wie ist die Regelung bei den US-Tochterfirmen in Europa?

Das Problem ist mittlerweile zumindest bei den großen US-Softwarefirmen angekommen. Aufgrund des Urteils haben diese begonnen, eigene Rechenzentren und Instanzen in der EU zu installieren und die Daten auch physisch in der EU zu hosten. Doch die Thematik ist komplizierter und das Hosting innerhalb der EU keine nachhaltige Lösung, solange die eigentliche Verwaltung der Daten aus den USA erfolgt und über diesen Umweg weiterhin eine Zugriffsmöglichkeit von US-Behörden besteht. Das bedeutet, dass auch Tochterunternehmen von US-Konzernen, die somit den Weisungen aus den USA zu folgen haben, kritisch zu betrachten sind. Zumal selbst der Support aus den USA als unerlaubte Datenweitergabe zählt.

Raus aus der Zwickmühle

Was ist nun die Lösung? Eine Möglichkeit ist die angesprochene sichere technische Verschlüsselung der transferierten oder in einer Cloudanwendung vorhandenen Daten in einem Umfang, dass diese für fremde Behörden nicht mehr lesbar sind. Doch hier kann es sein, dass dies US-Firmen unter Umständen untersagt oder für eine cloudbasierte Anwendungssoftware technisch bislang gar nicht umsetzbar ist.

Welche Möglichkeiten haben Hotels nun in der EU beziehungsweise solche, die die DSGVO umfassend beachten müssen? Bevor ein Softwarevertrag mit einem US-Anbieter (oder einem EU-Anbieter, der US-Unterauftragnehmer nutzt) unterschrieben wird, sollte dieser datenschutzrechtlich speziell zu den angesprochenen Themen geprüft werden. Eine detaillierte datenschutzrechtliche Prüfung von Softwareverträgen durch einen darauf spezialisierten Fachanwalt kann viel Geld kosten. Noch dazu ist es derzeit wenig wahrscheinlich, dass in den hier besprochenen Fällen das Ergebnis der Prüfung eine Befürwortung eines Vertragsabschlusses zum Inhalt hat.

Der rechtlich sicherste Weg

Der rechtlich sicherste Weg ist, die beschriebene datenschutzrechtliche Problematik der Non-EU-Transfers und Dienstleister zu umgehen und einen in der EU oder im EWR ansässigen Softwareanbieter zu nutzen, der auch nur in der EU oder im EWR ansässige Unterauftragnehmer einsetzt. Denn dann sind alle beteiligten Unternehmen direkt der DSGVO und somit dem hohen dortigen Datenschutzniveau verpflichtet, anders als Unternehmen außerhalb der EU oder außerhalb des EWR.

In diesem Zusammenhang ist zu erwähnen, dass die Strafen der DSGVO zwar zunächst die Unternehmen, also etwa das Hotel, treffen und nicht direkt deren gesetzliche Vertreter, wie Geschäftsführer oder Vorstände. Es kann aber nach nationalen Regelungen daneben noch eine persönliche Haftung des Managements geben – etwa in Deutschland unter dem Gesichtspunkt des Organisationsverschuldens.

Wer also ruhig schlafen möchte, sollte bei einem Vertragsabschluss betreffend einer Cloudsoftware immer versuchen, datenschutzrechtlich auf der sicheren Seite zu bleiben, also innerhalb der Grenzen der EU und des EWR.