dailypoint™
Central Data Management
by Toedt, Dr. Selk & Coll. GmbH

Das Urteil des EuGH zum EU-US-Privacy-Shield und seine Konsequenzen

ACHTUNG DATENSCHUTZ

Vermeiden Sie fahrlässige Verstöße bei der Auswahl von Cloud-Softwaresystemen!

DR. JUR. ROBERT SELK, DR. MICHAEL TOEDT

Spätestens mit der Einführung der DSGVO (E-Mail-Marketing ohne Einwilligung) sollte das Thema Datenschutz ganz oben auf der Agenda stehen. Doch gerade bei der Auswahl von Cloud-Softwaresystemen wird in der Praxis derzeit häufig fahrlässig gegen die geltende Rechtsprechung verstoßen.

Datenübermittlung in ein Drittland

Gemäß der DSGVO dürfen personenbezogene Daten nur dann in ein Drittland übermittelt werden, wenn dort ein angemessenes Schutzniveau sichergestellt ist (Art. 44). Der Datenschutz in den USA gilt allerdings nicht als angemessen. Daher dürften theoretisch keine Datenübermittlungen dorthin getätigt werden. Allerdings sieht Art. 45 DSGVO vor, dass Übermittlungen in ein Drittland dann zulässig sind, wenn durch einen Angemessenheitsbeschluss der Europäischen Kommission festgestellt worden ist, dass das Schutzniveau ausreichend ist. (Quelle: datenschutz.org/privacy-shield/)

Wenn Ihr Cloud-Anbieter außerhalb der EU sitzt

Jeder Cloud-Anbieter ist heute gezwungen, ausreichende technische und organisatorische Maßnahmen bezüglich des Datenschutzes und der Datensicherheit zu treffen.

Darunter fallen auch Regelungen zu etwaigen Unterauftragnehmern, wie z. B. Hosting-Anbieter oder integrierte Softwarebestandteile. Beides ist in aller Regel in Form der sogenannten Auftragsverarbeitungsvereinbarung (AVV) auch Teil der Softwareverträge. Diese werden jedoch – so zeigt die Erfahrung – eher selten durch den Auftragnehmer, also beispielsweise dem Hotel, vor Abschluss auch datenschutztechnisch umfassend geprüft, mit gefährlichen Folgen. Denn seit dem letzten Jahr gibt es eine sehr **folgenreiche Gerichtsentscheidung**, die für all diejenigen Fälle grundlegende Bedeutung hat, in denen entweder der Cloud-Anbieter selbst oder einer seiner Unterauftragnehmer nicht in der EU oder EWR, sondern außerhalb ansässig ist. Dies trifft gerade in der Hotellerie auf viele große Softwareanbieter zu.

dailypoint™
Central Data Management
by Toedt, Dr. Selk & Coll. GmbH

Hintergrund: Schutz vor US-Behörden

Im Juli 2020 hat der **Europäische Gerichtshof (EuGH)** den Nachfolger des Safe Harbor Abkommens, das sogenannte 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 übermitteln wurden, NICHT mehr dorthin transferiert werden dürfen. Dies betrifft **Cloud-Softwareanbieter und Hosting-Firmen in den USA**, genauso wie sämtliche Unterauftragnehmer in den USA. Wer also seine Gastdaten mittels eines US-Cloud-Softwareanbieters 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 4 % des letztjährigen weltweiten Umsatzes geahndet werden kann.

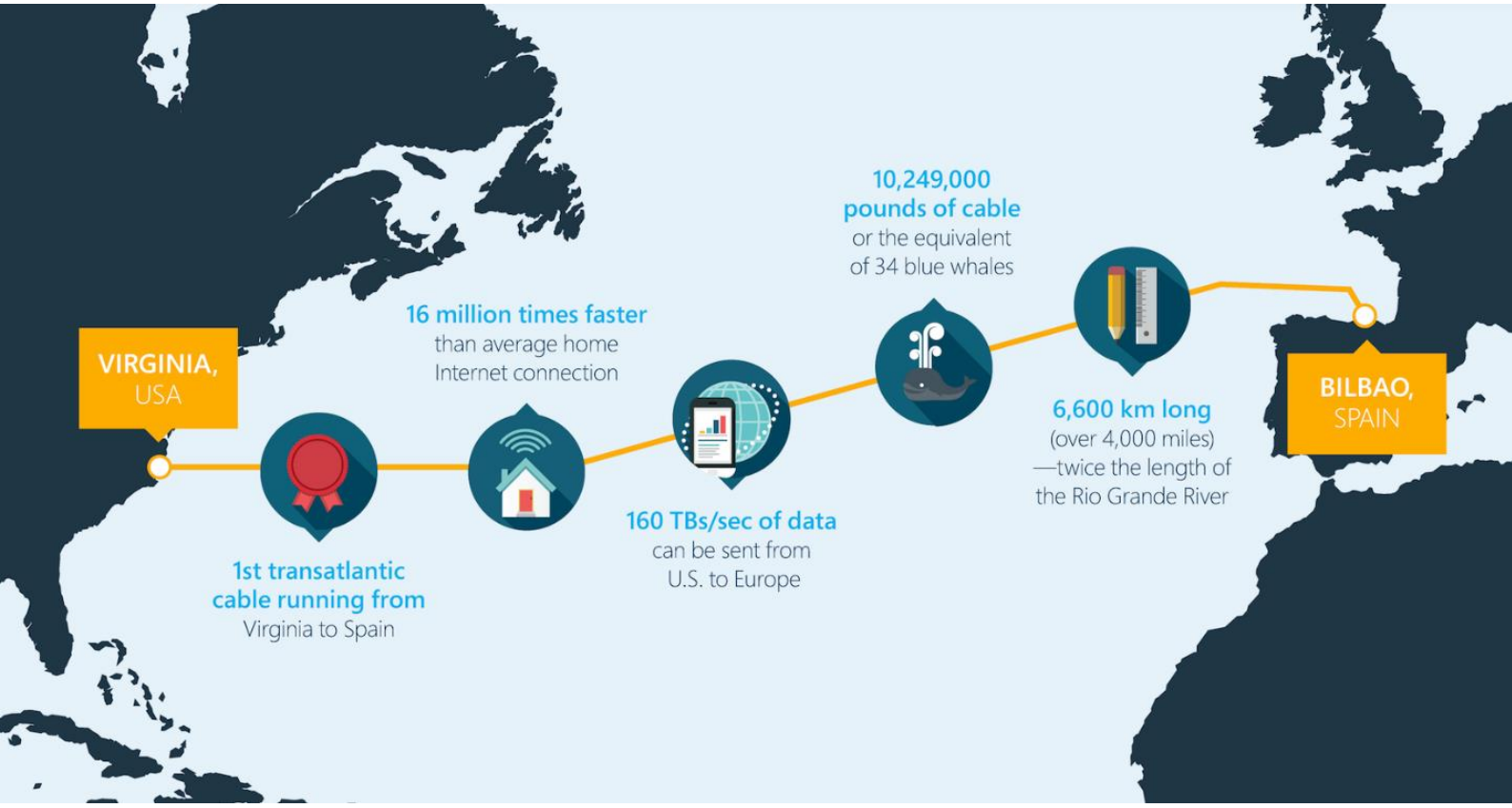
Der Grund für das Gerichtsurteil ist der Umstand, dass das Privacy Shield keinen

Personenbezogene Daten dürfen laut DSGVO nur dann außerhalb der EU transferiert werden, wenn ein gewisses Schutzniveau gewährleistet werden kann (DSGVO Artikel 44, Allgemeine Grundsätze der Datenübermittlung) (Bild: dreamstime.de)

ausreichenden Schutz für die bei den US-Unternehmen gespeicherten Daten vor Zugriffen von US-Behörden bieten könne, da es 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.

Die Privatsphäre der Hotelgäste

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



Übersee-Datenkabel von den USA nach Europa (Quelle: Microsoft/ RUN Studios)

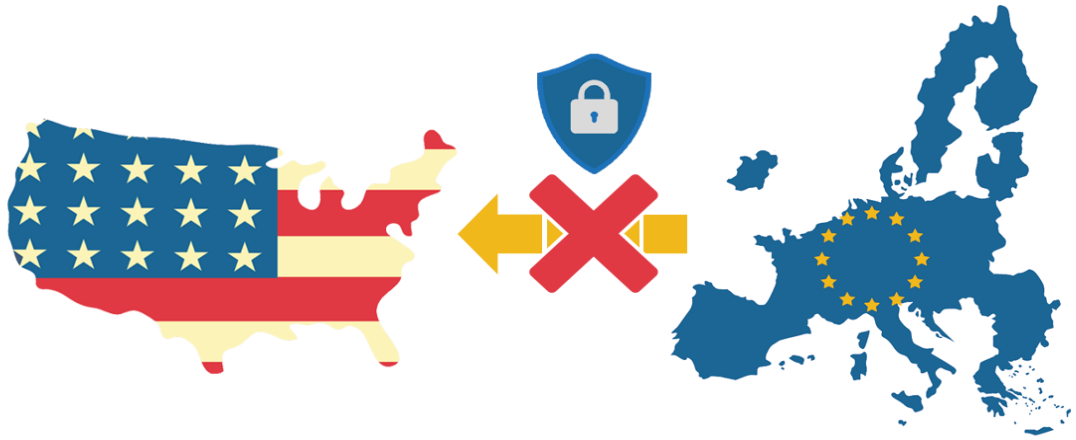
außerhalb der EU, wie etwa in die USA, transferiert und damit dortigen Behördenzugriffen zugänglich gemacht. Gerade einigen Gästen von Luxusherbergen dürften wohl die Haare zu Berge stehen, wüssten sie dies.

Als Alternative zum Privacy Shield konnte man bislang von der EU standardmäßig fest vorgegebene Datenschutzverträge abschließen, die sogenannten **EU-Standarddatenschutzverträge**. Diese waren zwar nicht gegenständlich im Verfahren des EuGH, so dass 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 etwa das Hotel und einen US-Cloudanbieter – lassen sich in rechtlicher Hinsicht die Überlegungen des EuGH in weiten Teilen auch auf diese Lösungsvariante übertragen, also die EU-Standardverträge. 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.

> *„Das Privacy Shield bietet keinen ausreichenden Schutz vor Zugriffen von US-Behörden."*

Datenverschlüsselung mit Tücken

Eine solche strenge Verschlüsselung ist durchaus denkbar. Allerdings ist dies bislang weitestgehend nur für Daten im Rahmen eines Hostings möglich. Hinsichtlich cloudbasierten SaaS-Softwarelösungen oder anderen typischen Cloudanwendungen, die nicht nur aus einem reinen Hosting der Daten bestehen, sondern bei denen es um echte Softwarefunktionalitäten geht, ist dies bislang in der Praxis kaum möglich. Selbst die großen US-Unternehmen bieten keine technischen Lösungen an, bei denen selbst bei SaaS-



Suchen Sie sich europäische Lösungen für Ihre Cloud-Software! (Bild: datenschutz-generator.de)

oder Cloud-Anwendungen die Daten durchgängig verschlüsselt sind und somit nicht einmal die Cloud-Anbieter selbst mehr Zugriff haben, aber dennoch die Funktionalitäten anbieten können. Es gibt zwar rechtlich einige kleinere **Ausnahmemöglichkeiten**, für die große Masse von Fällen sowie bei dem Einsatz von US-Cloud-Anwendungen 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-Cloud-Software gleich.

Das Problem ist mittlerweile zumindest bei den großen US-Softwarefirmen angekommen. Aufgrund des Urteils haben diese daher die letzten Monate 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, solang die eigentliche Verwaltung der Daten aus den USA erfolgt und über diesen Umweg weiterhin eine Zugriffsmöglichkeit von US-Behörden besteht. Das bedeutet, dass auch etwa 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

Doch was ist nun die Lösung? Eine Lösung ist die angesprochene sichere technische Verschlüsselung der transferierten oder in einer Cloud-Anwendung 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 ist bzw. für eine cloudbasierte Anwendungssoftware technisch bislang gar nicht umsetzbar ist.

Welche Möglichkeiten haben Hotels nun in der EU, bzw. 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 obigen 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 EWR ansässigen Software-Anbieter zu nutzen, der auch nur in der EU/ 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/ 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 dennoch 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 Cloud-Software versuchen, datenschutzrechtlich auf der sicheren Seite zu bleiben, also innerhalb der Grenzen der EU/ EWR.

Über dailypoint™ - Software made by Toedt, Dr. Selk & Coll. GmbH

dailypoint™ ist die führende Daten-Management- und CRM-Plattform für anspruchsvolle Individualhotels und Hotelgruppen. dailypoint™ sammelt Daten aus allen relevanten Quellen wie PMS, POS, Webseite, Newsletter oder W-Lan und erstellt automatisch ein zentrales und konsolidiertes Gast-Profil. In 350 Stufen werden die Daten verarbeitet und mittels künstlicher Intelligenz (KI) angereichert, um ein bisher nie dagewesenes Gast-wissen zu erstellen. Die cloudbasierte SAAS-Lösung besteht aus 16 Modulen und wird durch den dailypoint™ Marketplace mit mehr als 160 Lösungspartnern ergänzt. dailypoint™ bietet aber nicht nur ein messbares Marketing, sondern deckt darüber hinaus die gesamte Customer Journey ab und unterstützt somit alle Abteilungen innerhalb eines Hotels. Das integrierte Privacy Dashboard ist darüber hinaus das zentrale Element für die technische Umsetzung der DSGVO.

dailypoint™ besteht aus drei miteinander verbundenen Bereichen: die dailypoint™ Data Management Plattform, die CRM & E-Marketing Suite und Loyalty.

dailypoint™ hat seinen Hauptsitz in München, Deutschland und wird weltweit direkt, bzw. durch seine Vertriebspartner D-EDGE und XNProtel vertrieben und betreut.

Weitere Informationen finden Sie unter **www.dailypoint.com**

Über Dr. Michael Toedt

Dr. Michael Toedt ist geschäftsführender Gesellschafter der Toedt, Dr. Selk & Coll. GmbH in München. Sein bisheriges Berufsleben kann in zwei Bereiche unterteilt werden: Aufgewachsen im elterlichen Hotelbetrieb war es zunächst sein Ziel diesen zu übernehmen. Nach zwei fachbezogenen Ausbildungen und Erfahrungen in der Sternegastronomie studierte er BWL mit Schwerpunkt Hotellerie an der Hochschule München. Im Jahr 2000 startete er sein zweites Berufsleben im Bereich CRM bei der Schörghuber Unternehmensgruppe, um 2005 die Toedt, Dr. Selk & Coll. GmbH zu gründen. TS&C, heute bekannt unter dem Namen dailypoint™, hat sich seither als Softwarefirma und Thinktank für ein datengetriebenes Management einen Namen gemacht. Neben seiner Tätigkeit bei Toedt, Dr. Selk & Coll. ist Michael Toedt u.a. Lehrbeauftragter an der Hochschule München zum Thema „CRM im Tourismus" sowie Dozent bei der Hotellerie Suisse im NDS Managementprogramm. Er veröffentlicht regelmäßig Fachartikel im Bereich Big Data und Digitalisierung. Er ist u.a. Verfasser des „Leitfaden Kunden-Bindungsmanagement" des Österreichischen Hotelverbands (ÖHV), sowie des Buches „Big Data – Chancen und Risiken für die Hotellerie" erschienen im Deutschen Fachverlag. 2015 und promovierte er an der University of Latvia zum Themenbereich „Einfluss von Kommunikation auf das Wiederkaufverhalten in der Hotellerie".

Über Dr. jur. Robert Selk

Rechtsanwalt Dr. jur. Robert Selk, Fachanwalt für IT-Recht, ist Partner bei SSH Rechtsanwälte in München. Er promovierte 2002 im Bereich des Internet- und Datenschutzrechts, Schwerpunkt seines parallelen Master- Aufbaustudiums war das europäische und internationale Wirtschaftsrecht (Master of Law, LL.M.). Seine Tätigkeit betrifft seit vielen Jahren das Computer-, Internet- und Datenschutzrecht sowie das Marken-, Urheber- und Wettbewerbsrecht. Dr. Selk ist ferner in verschiedenen international tätigen Unternehmen als externer Datenschutzbeauftragter bestellt, umfangreich als Referent im IT- und Datenschutzrecht tätig sowie Mitglied u.a. des Gesetzgebungsausschusses zum IT-Recht des deutschen Anwaltvereins und Mitvorsitzender des Fachausschusses „Datenschutz" der Deutschen Gesellschaft für Recht und Informatik. Daneben veröffentlicht er regelmäßig juristische Beiträge.

dailypoint™
Central Data Management
by Toedt, Dr. Selk & Coll. GmbH

Für weitere Informationen: michael.toedt@dailypoint.net

www.dailypoint.com