Die EU-Datenschutz-Grundverordnung (DSGVO) im Tourismus

I. Rechtliches

1. Inkrafttreten der EU-Datenschutz-Grundverordnung (DSGVO)

Die EU-Datenschutz-Grundverordnung ist bereits am 25. Mai 2016 in Kraft getreten. Sie sieht jedoch eine Übergangsfrist von zwei Jahre vor, um den betroffenen Unternehmen eine angemessene Vorbereitung und Anpassung der betroffenen Prozesse zu ermöglichen. Danach ist die DSGVO ab 25. Mai 2018 für alle Mitgliedstaaten verbindlich anzuwenden. Somit können die Datenschutzbehörden ab Ende Mai 2018 die Einhaltung der gesetzlichen Vorgaben überprüfen und im Falle von Verstößen Sanktionen verhängen. Daneben besteht auch weiterhin die Gefahr von Abmahnungen durch Wettbewerbsvereine oder Mitbewerber.

2. Ziele der DSGVO

Ziel der DSGVO ist neben dem Schutz der Grundrechte und Grundfreiheiten von Personen durch den Schutz personenbezogener Daten auch der Schutz des freien Verkehrs personenbezogener Daten, also die Möglichkeit erhobene Daten im Rahmen des Zulässigen auch zu verwenden.

Anknüpfungspunkt sind dabei stets „personenbezogene Daten“. Gemeint sind hiermit alle Angaben, die sich einer bestimmten Person zuordnen lassen und sie dadurch identifizieren oder identifizierbar machen kann. Unproblematisch ist dies z.B. bei dem Namen und der Wohnanschrift einer Person. Allerdings liegen auch dann personenbezogene Daten vor, wenn die erhobenen Informationen unter Zuhilfenahme weiterer verfügbarer Daten und technischer Mittel einer bestimmten Person zugeordnet werden können, wie dies z.B. bei Telefonnummern, KFZ-Kennzeichen, Kundennummern und auch IP-Adressen der Fall ist.

3. Was bleibt: unveränderte Regelungen

In rechtlicher Hinsicht unterliegt die Verarbeitung von personenbezogenen Daten auch weiterhin einem sog. Verbot mit Erlaubnisvorbehalt. Danach ist die Verarbeitung personenbezogener Daten grundsätzlich verboten, es sei denn, es liegt eine ausdrücklich erteilte Einwilligung oder eine gesetzliche Erlaubnis vor. Eine solche Erlaubnis nimmt das Gesetz z.B. an, wenn die Erfüllung eines Vertrages nur durch

die Erhebung und Verarbeitung von personenbezogenen Daten überhaupt möglich ist. So ist es z.B. erforderlich, im Rahmen der Erbringung von touristischen Leistungen auch in Erfahrung zu bringen, wer der Vertragspartner ist. Demnach müssen hier notwendigerweise Name und Adresse der Reisenden erhoben und gespeichert werden. Nur so kann z.B. eine Rechnung erstellt werden. Auch die Erfüllung von Meldepflichten ist nur bei Kenntnis der Daten der Vertragspartner möglich.

Die wesentlichen Datenschutzgrundsätze des bisher geltenden Rechts, wie z.B. die Datensparsamkeit, die Zweckbindung und das Gebot der Transparenz gelten auch unter der Datenschutzgrundverordnung weiter fort. So sieht das Gesetz z.B. besondere Einschränkungen bei der Verarbeitung besonders sensibler Daten vor. Gemeint sind hier insbesondere Angaben zur rassischen und ethnischen Herkunft, politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen, Gewerkschaftszugehörigkeit sowie Gesundheit und Sexualität. Diese Daten dürfen nur bei Erforderlichkeit der Kenntnis und nur mit ausdrücklicher Einwilligung der betroffenen Person verarbeitet werden. So ist denkbar, dass bestimmte Angaben zu gesundheitlichen Besonderheiten gerade bei der Erbringung touristischer Leistungen, z.B. in Form von Wellnessanwendungen, die der konkrete Gast nicht „verträgt“, erforderlich sind (Hautkrankheiten, Bluthochdruck u.ä.).

Darüber hinaus bleibt in den meisten privaten oder auch öffentlich-rechtlich organisierten Unternehmen die Stellung eines betrieblichen oder externen Datenschutzbeauftragten auch weiterhin verpflichtend. So ist grundsätzlich in Unternehmen, bei denen in der Regel mindestens 10 Mitarbeiter mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, ein Datenschutzbeauftragter zu bestellen. Zudem ist eine Bestellung notwendig, wenn die Datenverarbeitung eine Kerntätigkeit des Unternehmens ist und einen großen Umfang aufweist.

4. Das ist neu: Wesentliche Änderungen für Unternehmen nach der DSGVO

Anwendungsbereich: Die neue Datenschutzverordnung gilt zunächst für alle Unternehmen, die ihren Sitz in der EU haben. Darüber hinaus gelten die Vorgaben der Datenschutzgrundverordnung auch für Unternehmen, die nicht in der EU niedergelassen, jedoch auf dem europäischen Markt tätig sind. Auch diese Unternehmen haben die europäischen, datenschutzrechtlichen Vorgaben zu beachten. Wenn man sich also der Dienste solcher Unternehmen bedient, indem z.B. Daten in einer Cloud eines solchen Anbieters gespeichert werden oder man sich einer Datenbank eines nicht in der EU ansässigen Anbieters bedient, muss sichergestellt sein, dass

die europäischen Datenschutzstandards auch durch diese Unternehmen erfüllt werden.

Eine weitere Neuerung ist der Grundsatz der **Privacy by Design**: Hiermit ist eine datenschutzfreundliche Technikgestaltung gemeint, die durch die Einführung von technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten erreicht werden soll. Diese datenschutzfreundliche Gestaltung soll bereits bei der Entwicklung von Vorgängen Beachtung finden und zum grundlegenden Standard werden.

Wenn z.B. eine App entwickelt wird, soll sie standardmäßig nur solche personenbezogenen Daten verarbeitet, die für deren Funktion unabdingbar sind (z.B. Grundfunktion = Kommunikation). Sollen weitere Funktionen freigeschaltet werden und sind hierfür weitere Daten des Betroffenen erforderlich, bedarf es einer zusätzlichen Einwilligung des Betroffenen (z.B. Erweiterung durch Verknüpfung mit externen Kalendern).

Privacy by Default: Dieses Prinzip soll den auch zurzeit bereits geltenden Grundsatz der Datensparsamkeit ergänzen. Daten sollen nur erhoben werden, wenn Sie auch tatsächlich benötigt werden. Dies betrifft auch den Umfang der erhobenen Daten. Privacy by Default will genau dies erreichen. Durch die Verpflichtung zu datenschutzfreundlichen Voreinstellungen von Programmen und Prozessen soll gewährleistet werden, dass nur die erforderliche Daten erhoben und verarbeitet werden, also solche Daten, die man zur Erreichung des Erhebungszwecks auch tatsächlich benötigt. Es sollen damit insbesondere unnötige Erhebungen und Verarbeitungen sowie unzulässige Speicherdauern vermieden werden. So wäre z.B. ein Internet-Browser nach der Installation standardmäßig so einzustellen, dass ein Setzen von Cookies, die es Dritten ermöglichen, Informationen über das Surfverhalten des Nutzers zu erlangen, nur mit Zustimmung des Nutzers möglich ist.

Meldepflicht bei Datenpannen: Wenn der Schutz personenbezogener Daten verletzt wurde, z.B. im Falle einer Datenpanne, hat das Unternehmen verschiedene Meldepflichten zu erfüllen. Hierbei ist zwischen Meldepflichten gegenüber der Aufsichtsbehörde (Landesbeauftragten für Datenschutz und Informationsfreiheit) und entsprechenden Pflichten gegenüber den von der Verletzungshandlung Betroffenen zu unterscheiden.

Im Falle einer Verletzung personenbezogener Daten muss das Unternehmen dies der Aufsichtsbehörde innerhalb von 72 Stunden melden. Diese Verpflichtung besteht jedoch nicht, wenn die konkrete Datenpanne voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten von Personen führt.

Darüber hinaus hat eine Benachrichtigung an die von der Verletzung betroffene Person zu erfolgen, wenn die Verletzung personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge hat. Hierbei sind jedoch Ausnahmetatbestände vorgesehen, bei deren Vorliegen eine Benachrichtigung des Betroffenen nicht erforderlich ist, so z.B. wenn die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre – hier ist eine öffentliche Bekanntmachung ausreichend.

Sanktionen: Im Falle von Verstößen gegen die DSGVO sieht das Gesetz empfindliche Bußgelder vor. So können Verstöße Geldbußen bis zu 20.000.000,- Euro (bisher max. 300.000 Euro) oder im Falle eines Unternehmens bis zu 4 Prozent des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden – je nachdem, welcher Betrag höher ist. Wie hoch diese Sanktionen in der Praxis ausfallen werden, bleibt abzuwarten, da es hier naturgemäß noch an entsprechender Rechtsprechung fehlt.

5. Verbesserungen für Verbraucher

Recht auf Datenübertragbarkeit: Betroffene haben künftig das Recht, ihre personenbezogenen Daten zu einem anderen Anbieter mitzunehmen, z.B. Social-Media oder E-Mail-Anbieter. Dies kann auch die Daten eines Verbandsmitglieds betreffen, das seine Mitgliedschaft kündigt und die Daten zu einem anderen Interessenverband „mitnehmen möchte“. Dabei haben die Betroffenen einen Anspruch gegenüber dem Verantwortlichen auf Bereitstellung der Daten in einem strukturierten, gängigen und maschinenlesbaren Format. Hierdurch soll dem Verbraucher ein Wechsel von einem Anbieter zu einem anderen erleichtert werden.

Einwilligung in die Datenverarbeitung: Wie auch bisher ist eine Datenerhebung und -verarbeitung zulässig, wenn Sie aufgrund einer vorherigen Einwilligung des Betroffenen erfolgt. Verschärft wurde allerdings der Grundsatz der Freiwilligkeit: Danach darf der Vertragsschluss nicht von einer Einwilligung in eine nicht erforderliche Verarbeitung abhängen (sog. Koppelungsverbot). Zudem kann der Betroffene seine Einwilligung zu jedem Zeitpunkt widerrufen.

Recht auf Löschung: Danach müssen die verarbeitenden Stellen die Daten löschen, wenn z.B. der Zweck wegfällt oder die Einwilligung widerrufen wird (sog. „Recht auf Vergessenwerden“).

Auskunftsrecht: Der Betroffene ist umfassend insbesondere über den Inhalt der Datenverarbeitung, den Zweck der Verarbeitung und die betroffenen Daten sowie die ihm zur Verfügung stehenden Rechte zu informieren (z. B. Widerrufsrecht, Beschwerderecht, Recht auf Löschung). Auch hat der Verantwortliche auf Verlangen des Betroffenen eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, in einem gängigen elektronischen Format zur Verfügung zu stellen.

II. Praktische Umsetzung durch die Tourismusorganisation: Was ist zu tun bis 25. Mai 2018

Bei der Umsetzung der DSGVO sind in der touristischen Praxis insbesondere folgende Punkte zu beachten:

1. Profiling – Erstellen ausführlicher Gästeprofile

Weit verbreitet ist es heutzutage, das Internet mittels spezieller Programme nach frei verfügbaren Informationen des Gastes zu durchsuchen. Hierdurch können bereits bekannte und notwendigerweise erhobene Gästeinformationen, die z.B. zur Durchführung des Vertrages benötigt werden, ergänzt werden. So werden z.B. Nutzerprofile von Gästen in sozialen Medien ausfindig gemacht und die dort enthaltenen Informationen zu einem Gesamtprofil des Gastes mit den vorhandenen Erhebungsdaten zusammengeführt. Dabei ergibt sich ein weitaus detaillierteres Bild der Bedürfnisse des Gastes, was sodann zu Werbezwecken Verwendung findet.

Wenn sich also aus dem öffentlich zugänglichen Social-Media Auftritt des Gastes dessen Hang zu sportlichen Aktivitäten entnehmen lässt, könnte z.B. zielgerichtet mit dem neu eingerichteten Fitnessbereich des Beherbergungsbetriebes oder nahe gelegenen Sporteinrichtungen geworben werden.

Für die Zulässigkeit dieses Vorgehens spricht der Umstand, dass es sich um frei zugängliche Daten handelt. Fraglich ist jedoch, ob eine solche Verknüpfung bestehender mit öffentlich zugänglichen Daten zur Bedarfsermittlung und letztlich zu Werbezwecken auch in datenschutzrechtlicher Hinsicht zulässig ist. Denn hier wird grundsätzlich die Schwelle der Erforderlichkeit der erhobenen Daten überschritten,

da die Daten für den konkreten Zweck der Vertragsabwicklung, hier der Durchführung der Reise, gerade nicht zwingend benötigt werden. Daten die daher nicht benötigt werden, hierbei insbesondere die besonderen Kategorien der Daten (z.B. rassisch/ ethnische Herkunft, politische Meinung, religiöse und weltanschauliche Überzeugung), dürfen keinesfalls gespeichert werden.

Bei der Frage der Möglichkeit des Profilings sieht der europäische Gesetzgeber eine datenschutzrechtliche Zulässigkeit vor, wenn ein Interesse des Gastes an der konkreten Nutzung angenommen werden kann, die Informationen für jedermann auffindbar waren und der Gast vernünftigerweise damit rechnen konnte, dass die öffentlich auffindbaren Informationen vom Gastgeber verwendet werden. Dies ist bei öffentlich zugänglichen Daten aus Social-Media-Auftritten zunächst der Fall. Dabei ist jedoch im Einzelfall dennoch stets eine Abwägung der betroffenen Interessen, zum einen des Gastes sowie andererseits des Beherbergungsbetriebes/ Reiseveranstalters/ DMO vorzunehmen.

2. Versand von Newslettern

Bedarf die postalische Werbung grundsätzlich keiner vorherigen Einwilligung des Gastes, so ist diese für den Newsletterversand per E-Mail zwingend vorab einzuholen. Hierbei muss der Versender der Mail als verantwortliche Stelle in der Lage sein, den Nachweis für eine wirksame Einwilligung des Betroffenen zu erbringen (DSGVO - Rechenschaftspflicht, Dokumentation!).

Dabei sind hohe Anforderungen an die Wirksamkeit der Einwilligung des Betroffenen zu stellen. Diese muss grundsätzlich freiwillig, informiert und ausdrücklich erfolgen. Zudem hat der Betroffene das Recht zum jederzeitigen Widerruf und ist über dieses Recht vor Erteilung der Einwilligung klar und verständlich zu informieren. Dies war nach noch geltender Rechtslage keine zwingende Voraussetzung für die Wirksamkeit der Einwilligung.

Besonderes Augenmerk ist auf die Prüfung bestehender Einwilligungen zu setzen. Eine weitere Verwendung gespeicherte Daten aufgrund dieser Einwilligungen ist nur dann zulässig, wenn diese „Alt-Einwilligungen“ inhaltlich den Anforderungen des neuen Datenschutzrechts entsprechen. So müssen diese Alt-Einwilligungen z.B. auch einen Hinweis auf das Widerrufsrecht enthalten. Verstoßen alte Einwilligungen gegen das Gebot der Freiwilligkeit und insbesondere gegen das neu verankerte Kopplungsverbot, gelten sie nicht fort und müssen erneut eingeholt werden.

Nach der Datenschutzgrundverordnung soll eine unzulässige Kopplung bereits vorliegen, wenn der Vertragsschluss oder die Vertragserfüllung von einer Einwilligung in hierfür nicht erforderliche Verarbeitungen abhängig gemacht wird. Ein solcher Fall ist z.B. gegeben, wenn die Teilnahme an einem Gewinnspiel oder die Möglichkeit einen Vertrag zu schließen von der Zustimmung in den Empfang eines Newsletters abhängig gemacht wird.

3. Zulässigkeit von Datenerhebungen im Meldescheinverfahren

Nach § 30 Abs. 2 des Bundesmeldegesetzes (BMG) müssen die dort genannten Daten im Meldeschein erfasst werden. Hierzu zählen auch bestimmte personenbezogene Daten. Diese Daten dürfen grundsätzlich nur für die Zwecke der Erhebung, hier die Erfüllung der Meldepflicht verwendet werden. Die Meldescheine sind für den Zeitraum eines Jahres nach dem Tag der Anreise des Gastes zu verwahren und nach Ablauf weiterer 3 Monate zu vernichten.

In direkter Verbindungen mit den Meldescheinen wird in der Praxis jedoch oft auch eine schriftliche Einwilligung für andere Zwecke, z.B. den späteren Versand von Newslettern eingeholt. Hier sind jedoch verschiedene Zwecke betroffen, die klar voneinander abzugrenzen sind. Zudem gelten hier unterschiedliche Aufbewahrungs- und Löschfristen von Meldeschein und Einwilligung in Newsletterversand. Keinesfalls dürfen diese Einwilligungen daher miteinander vermischt werden, auch um den Eindruck einer datenschutzrechtlich unzulässigen Kopplung der beiden Erklärungen zu vermeiden.

Es ist aus diesem Grunde empfehlenswert, räumlich voneinander getrennte Erhebungen durchzuführen. Neben dem ausgefüllten Meldeschein sollte daher eine separate Einwilligungserklärung eingeholt werden.

4. Speicherung von Gästedaten nach Durchführung des Vertrages

Nach Abreise des Gastes und Erfüllung aller Vertragspflichten ist die weitere Vorhaltung der Gästedaten (Ausnahme Meldeschein) dem Grunde nach nicht mehr erforderlich. Insbesondere die Legitimation einer Datenerhebung zu Zwecken der Vertragsdurchführung kann hier nicht mehr greifen.

Es bedarf daher zwingend einer Einwilligung in die konkrete Art der Verwendung, hier z.B. in die Versendung eines Newsletters, Kundenzufriedenheitsumfrage, die Speicherung in einer Kundendatenbank für spätere Werbung oder die Aufnahme in

ein sog. Treueprogramm. Dabei sind die Vorgaben der DSGVO hinsichtlich der Voraussetzungen einer wirksamen Einwilligung zu beachten. Die Informationen müssen:

- verständlich und
- in einfacher Sprache formuliert sein und
- eindeutige Information über Art, Umfang und Zweck der Datenverarbeitung sowie
- etwaige Empfänger der Daten enthalten.

Unbedingt ist der Gast hierbei auf sein Recht zum Widerruf der Einwilligung hinzuweisen. Wenn ein solcher Hinweis fehlt, ist die Einwilligung unwirksam. Zudem ist ein besonderes Augenmerk auf die Information hinsichtlich des Zweckes der Datenverwendung zu legen. Wenn also ein späterer Newsletterversand oder eine Kundenbefragung durchgeführt werden, muss die Einwilligungserklärung genau diese Zwecke erfassen.

Bei Vorliegen einer wirksamen Einwilligung und Beachtung der Zweckbindung können die Gästedaten sodann weiter gespeichert werden. So ist die Information von Stammgästen z.B. über aktuelle Angebote grundsätzlich auch im Interesse der angesprochenen Personenkreise. Dennoch ist auch hier eine einzelfallbezogene Interessenabwägung notwendig und vorzunehmen. Darüber hinaus ist der Kreis der zugriffsberechtigten Personen zu prüfen sowie Löschfristen festzulegen und zu dokumentieren.

Auch hier darf eine Speicherung zudem nur so lange erfolgen, wie vernünftigerweise von einem Interesse des Kunden ausgegangen werden darf. Längere Untätigkeit spricht eindeutig dagegen, so dass in diesen Fällen eine Löschung vorzunehmen ist.

5. Datensicherheit

Die verantwortliche Stelle (z.B. die Tourismusorganisation oder der Betreiber des Beherbergungsbetriebes) ist verpflichtet, geeignete Maßnahmen zur Sicherheit der Datenverarbeitung zu treffen. Dies betrifft sowohl die Absicherung des Zugangs zu Räumen, in denen sich die EDV-Technik, z.B. Server und EDV-Systeme (PC´s etc.) befinden, aber auch die Sicherung der Datenverarbeitungssysteme selbst, z.B. durch Virenschutzprogramme, Verschlüsselung bei E-Mailversand.

Neben diesen Maßnahmen zum Schutz der eingesetzten Datenverarbeitungs-Systeme (z.B. durch Key-Cards, Zahlungsterminals, Software mit neuesten Sicherheitsupdates) sollten Sicherheitsschulungen von Mitarbeitern durchgeführt werden.

Erfolgen zudem Datenverarbeitungen durch Dritte, muss eine sorgfältige Auswahl dieser Externen erfolgen und hinreichende vertragliche Grundlagen, insbesondere Verträge zur Auftragsdatenverarbeitung erstellt werden. Der Auftraggeber muss sicherstellen, dass ihm auch weiterhin eine Kontrolle über die Daten und deren Verwendung möglich ist (insbesondere vertraglich abgesichertes Weisungsrecht!).

Die Einhaltung der technischen und auch organisatorischen Maßnahmen (TOM) und Sicherheitsstandards durch den eingeschalteten Dritten ist vor Auftragsvergabe zu überprüfen. Diese Prüfung muss nicht zwingend persönlich vor Ort durchgeführt werden. Eine Zertifizierung des Auftragsdatenverarbeiters nach ISO 27001 stellt hier z.B. ein starkes Indiz für die Einhaltung der datenschutzrechtlichen Vorgaben dar.

Unternehmen sollten zudem auch bestehende Verträge zur Auftragsdatenverarbeitung auf die Einhaltung der Vorgaben des DSGVO überprüfen und ggf. überarbeiten.

III. Fazit

Was Sie unbedingt beachten sollten, um auf die Neuerungen des Datenschutzrechts durch Geltung der Datenschutzgrundverordnung vorbereitet zu sein:

1. Prüfung, ob Pflicht zur Bestellung eines Datenschutzbeauftragten besteht
2. Bestandsaufnahme des aktuellen IST-Zustandes
3. Abgleichung des IST-Zustandes mit den Vorgaben des neuen Datenschutzrechts, insbesondere Datenschutz
    - durch Technikgestaltung („Privacy-by-Design“) und
    - durch datenschutzfreundliche Voreinstellungen („Privacy-by-Default“)
4. Sensibilisierung der Mitarbeiter durchführen, insbesondere durch Schulungen
5. Überprüfen Sie bestehende Verträge über die Verarbeitung von personenbezogenen Daten durch Dritte

6. Treffen Sie organisatorische Vorkehrungen, wie im Fall einer Datenpanne vorzugehen ist (Meldepflichten, Fristen beachten, Information von Betroffenen)
7. setzen Sie Dokumentationspflichten um
8. erstellen Sie ein Verfahrensverzeichnis
9. überprüfen Sie die Berechtigung der Datenerhebung, insbesondere das Vorliegen einer Einwilligung mit Hinweis auf die Möglichkeit eines Widerrufs

Berlin, 04.04.2018

Hinweis:

Dieser Beitrag wurde mit größter Sorgfalt erstellt. Eine Gewähr für Richtigkeit, Vollständigkeit und Aktualität des Inhalts kann jedoch nicht übernommen werden. Für Schäden, die aus der Benutzung dieses Beitrages entstehen, können wir keine Haftung übernehmen.