Schweiz Tourismus.

mll

Whitepaper

Datenschutz und Tourismus

Zürich, 1. Februar 2018

Schweiz Tourismus

www.MySwitzerland.com
Tödistrasse 7 | CH-8027 Zürich

Meyerlustenberger Lachenal AG
Rechtsanwälte – Attorneys at Law

www.mll-legal.com | www.mll-news.com
Zürich | Genève | Zug | Lausanne | Brussels

Whitepaper Datenschutz und Tourismus

Das Datenschutzrecht in Europa steht vor grundlegenden Veränderungen. Auf EU-Ebene wird die Datenschutz-Grundverordnung (DSGVO) am 25. Mai 2018 in Kraft treten. Ausgehend davon ist auch in der Schweiz eine Totalrevision des Datenschutzrechts im Gange. Welche konkreten Änderungen die Revision mit sich bringen wird und wann diese gelten werden, ist aktuell noch offen.

Fest steht immerhin, dass sich der Schweizer Gesetzgeber zu einem grossen Teil am EU-Vorbild orientieren wird. Die Neuerungen werden branchenübergreifend alle Unternehmen und Organisationen sowie nahezu sämtliche Geschäftsprozesse betreffen. Auch die Tourismusbranche steht deshalb vor einer grossen Herausforderung.

Vor diesem Hintergrund zeigt das vorliegende Whitepaper in einem ersten Schritt auf, warum bereits das Inkrafttreten der EU-DSGVO für Unternehmen und Organisationen der Schweizer Tourismusbranche relevant ist. In einem nächsten Schritt werden die zentralen Themen und Vorgaben sowie der daraus resultierende Handlungsbedarf für die Tourismusbranche erklärt.

Schweiz Tourismus.

Inhaltsverzeichnis

I. Datenschutz betrifft nahezu sämtliche Geschäftsvorgänge!

Die Erfahrungen aus der Praxis machen deutlich, dass sich Unternehmen vielfach gar nicht bewusst sind, wie weit die Vorschriften des Datenschutzrechts in ihren Unternehmensalltag hineingreifen.

> Das Datenschutzrecht gilt bei jedem geschäftlichen Umgang mit personenbezogenen Daten.

Die Tragweite zeigt sich bereits aus der Aufzählung der relevanten „Verarbeitungen". Nach der gesetzlichen Umschreibung zählen hierzu insbesondere: „das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung".

→ **Beispiel:**

Das Datenschutzrecht ist also nicht nur zu beachten, wenn Adressangaben eines Hotelgasts an ein Tourismusbüro mitgeteilt werden, sondern **auch bei rein internen Vorgängen**, wie wenn der Hotelgast in der Datenbank einem bestimmten Kundensegment zugeteilt wird.

Auch die Voraussetzung, dass es sich um „personenbezogene Daten" handeln muss, führt nicht zu einer derart weiten Einschränkung, wie häufig angenommen wird. Erforderlich ist zwar eine Information, die einer bestimmten (natürlichen) Person zugeordnet werden kann. Jedoch zählen hierzu insbesondere auch pseudonymisierte Daten. Wenn also beispielsweise in einer Datenbank die Personalien (Name, Adresse etc.) eines Kunden durch eine Nummer ersetzt werden, handelt es sich bei den Bestelldaten zu dieser Nummer immer noch um personenbezogene Daten, wenn eine Person im Unternehmen oder allenfalls gar ein Dritter die Nummer wieder dem Kunden zuordnen kann. Vernachlässigt wird der Datenschutz deshalb vielfach beim Betrieb von Websites.

→ **Beispiel:**

Sucht ein Nutzer auf der Website von Schweiz Tourismus Informationen für seinen nächsten Ferien-Aufenthalt in der Schweiz, hinterlässt er bereits beim blossen Aufruf der Homepage eine Vielzahl von technischen Daten (insb. die IP-Adresse). Diese werden (automatisch) auf dem Server der Website gespeichert und müssen aufgrund der Gerichtspraxis als personenbezogene Daten behandelt werden, selbst wenn der Nutzer seinen Namen nicht oder noch nicht mitgeteilt hat.

II. Warum ist die DSGVO für CH-Unternehmen relevant?

Zwei der grundlegendsten Neuerungen gegenüber der bis Mai 2018 geltenden Rechtslage verdeutlichen die Relevanz der DSGVO für Schweizer Unternehmen. Zum einen drohen bei Verletzung der Vorschriften Bussgelder in Millionenhöhe. Zum anderen verlangen die Vorschriften der DSGVO auch weit über die Grenzen des EU-Binnenmarkts hinaus Geltung.

1. Drastische Verschärfung der Sanktionen bei Verstoss gegen Datenschutzvorschriften

Auf Seiten der Datenschützer wurde die bisher geltende Rechtslage bereits deshalb bemängelt, weil die Sanktionen für Datenschutzverletzungen zu wenig abschreckend waren. Demzufolge hatten die Unternehmen nur wenig Anreiz, um den Aufwand für die Datenschutz-Compliance genügend ernst zu nehmen.

Mit dem Inkrafttreten der DSGVO wird sich dies grundlegend ändern:

Es drohen künftig **Verwaltungssanktionen in der Höhe von bis zu 20 Millionen Euro oder 4% des weltweiten Jahresumsatzes.**

Der Bussgeldrahmen wurde damit EU-weit stark erhöht und vereinheitlicht. Die „alternative" Obergrenze der Sanktion ist davon abhängig, welcher der beiden Werte (20 Millionen Euro oder 4% des Umsatzes) der höhere ist. Inwieweit die zuständigen Aufsichtsbehörden von diesem „Strafrahmen" Gebrauch machen werden und wie häufig überhaupt Sanktionen ausgesprochen werden, lässt sich derzeit nur schwer abschätzen. In Kombination mit den bereits bisher bestehenden Reputationsrisiken stellt aber jedenfalls bereits die Aussicht auf die Verwaltungssanktionen einen sehr gewichtigen Anreiz zur Einhaltung der datenschutzrechtlichen Vorgaben dar.

Darüber hinaus bestehen auch für die von einer Datenbearbeitung betroffenen Personen verschiedene Möglichkeiten zur Durchsetzung ihrer Rechte auf zivilrechtlichem Weg. So können sie beispielsweise ein gerichtliches Verbot bestimmter Handlungen erwirken und unter Umständen Schadenersatz fordern. Namentlich in Deutschland drohen bei Datenschutzverletzungen zudem Abmahnungen von Konkurrenten mit anschliessenden Gerichtsverfahren. Entsprechende Gerichtsentscheide sind gegenüber Unternehmen in der Schweiz in der Regel ohne weiteres vollstreckbar. Schliesslich enthalten die nationalen Gesetze der Mitgliedstaaten weiterhin auch Straftatbestände für bestimmte Datenschutzverstösse.

2. Wann ist die DSGVO auf Schweizer Unternehmen anwendbar?

Ausgehend von den einschneidenden Konsequenzen, die bei der Nichteinhaltung der DSGVO drohen, stellt sich die Frage, für wen diese Vorgaben überhaupt gelten. Dies lässt sich am besten anhand von verschiedenen Konstellationen erläutern. Wie die nachfolgenden Beispiele deutlich machen, ist der Anwendungsbereich der Verordnung bewusst sehr weit gefasst:

Die DSGVO gilt **nicht nur für Datenbearbeitungen, die innerhalb der EU erfolgen.** Vielmehr sind die Vorschriften **auf zahlreiche Unternehmen ohne Niederlassung in der EU anwendbar.**

Von den neuen Vorgaben sind deshalb weit mehr Unternehmen und Organisationen der Schweizer Tourismusbranche betroffen als von anderen EU-Regeln. Wenig überraschend ist vielen auch (noch) nicht bewusst, dass die DSGVO auch für sie gilt.

a. Schweizer Tourismus-Unternehmen mit Niederlassung in der EU

Eine erste Konstellation betrifft Fälle, in welchen es auf den ersten Blick nicht erstaunlich ist, dass die DSGVO Anwendung verlangt:

Unternehmen mit Sitz in der Schweiz müssen die DSGVO einhalten, wenn sie über eine Niederlassung in der EU verfügen und im Rahmen der Tätigkeiten dieser Niederlassung personenbezogene Daten bearbeiten.

Als Niederlassung gelten insbesondere Tochtergesellschaften. Übernimmt die Muttergesellschaft in der Schweiz z.B. HR-Funktionen für die EU-Niederlassung und bearbeitet dabei Daten von Mitarbeitern der Niederlassung, ist die DSGVO anwendbar.

Zu beachten ist, dass der Begriff „Niederlassung" weit verstanden wird. Erfasst werden auch blosse Zweigniederlassungen, Abteilungen oder allgemein „feste Einrichtungen".

➔ **Beispiel:**

Auch die EU-Vertretungen von Schweiz Tourismus kommen als Niederlassungen in Frage. Die DSGVO ist deshalb auf Datenbearbeitungen durch EU-Vertretungen anwendbar.

b. Schweizer Tourismus-Unternehmen ohne Niederlassung in der EU

Über die vorgenannten Fälle mit EU-Niederlassung hinaus bestehen drei weitere Konstellationen, die auch **Schweizer Unternehmen ohne jegliche Einrichtung in der EU in den Anwendungsbereich der DSGVO einschliessen.** Diese Fälle verdeutlichen, die weit über die EU-Grenzen hinaus greifende Wirkung der künftigen Regeln. Die ersten beiden Fälle zielen zu einem wesentlichen Teil auf Online-Sachverhalte ab.

1. Angebot von Waren oder Dienstleistungen an EU-Kunden

Den Vorgaben des EU-Datenschutzrechts unterstellt sind auch Schweizer Unternehmen, die ihre Waren oder Dienstleistungen an Kunden in der EU anbieten und in diesem Zusammenhang personenbezogene Daten bearbeiten.

Als „Anbieten" gilt eigentlich nur ein „offensichtlich beabsichtigtes Angebot" an Kunden in der EU. So sollte beispielsweise ein Schweizer Bergbahnunternehmen noch nicht bereits deshalb der DSGVO unterstellt sein, weil es auch Personen in der EU faktisch möglich ist, auf der Website Skipässe zu bestellen. Allerdings wird für die Beurteilung, ob ein Angebot (auch) auf Personen in der EU ausgerichtet ist, auf Kriterien abgestellt, die in anderen Rechtsgebieten sehr weit interpretiert werden. Entscheidend ist dabei die Frage, ob das Bergbahnunternehmen bewusst und gezielt Anstrengungen unternimmt, potentielle Kunden mit Wohnsitz in der EU anzusprechen und anzuwerben. Ist dies der Fall, ist das Angebot auf EU-Kunden ausgerichtet und diese Kunden können sich bei der Bearbeitung ihrer Daten durch das Schweizer Bergbahnunternehmen auf ihre Rechte unter der DSGVO berufen.

➔ **Beispiel:**

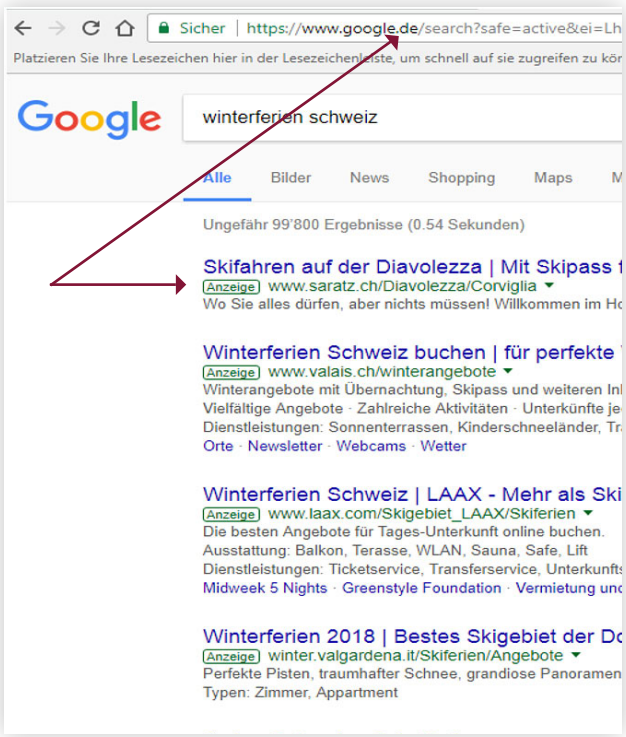
Wer auf seiner Website dem Besucher eine Möglichkeit zur Wahl „seines Landes" zur Verfügung stellt, richtet sich zumindest auch an Kundschaft aus den konkret genannten Ländern. Im Beispiel von Schweiz Tourismus ist die DSGVO daher anwendbar.

So wird insbesondere die zusätzliche Angabe der Preise in Euro oder die Angabe von Versandkosten in EU-Mitgliedstaaten klar für eine solche Ausrichtung sprechen. Wird für ein Angebot gezielt auf EU-Kunden ausgerichtete Online-Werbung betrieben (bspw. durch entsprechend geographisch geplante AdWords-Kampagnen), ist dies ein offensichtlicher

Beleg dafür, dass sich das beworbene Angebot an Kunden im entsprechenden Gebiet richten soll. In diesem Fällen müssen daher für die mit dem Angebot zusammenhängenden Datenbearbeitungen die Vorschriften der DSGVO beachtet werden.

→ **Beispiel:**

Wer also bei Google für die Keywords „Winterferien Schweiz" Anzeigen für die Aufschaltung auf google.de bucht, richtet sein Angebot auch an deutsche Kunden. So dürfte auf die nachfolgenden Anbieter die DSGVO anwendbar sein, sofern nicht andere Gesichtspunkte deutlich gegen eine grenzüberschreitende Ausrichtung sprechen:



Zu einer erheblichen Ausweitung des Anwendungsbereichs führt schliesslich, dass auch **unentgeltliche Angebote** erfasst werden. Somit sind auch die Betreiber von reinen Informations-Websites, wie beispielsweise die Websites der meisten Tourismus-Destinationen und Gemeinden, der DSGVO unterstellt, wenn die Website (auch) auf Personen in der EU ausgerichtet ist. Massgebliche Kriterien für die Beurteilung der Ausrichtung sind hier unter anderem die Sprach-Versionen der Website, die Top-Level-Domain oder die Angabe der internationalen Vorwahl. Insbesondere ist jede Form von gezieltem Online-Marketing in den EU-Märkten ein klarer Beleg für die Ausrichtung.

2. Beobachtung des Verhaltens von Personen in der EU

> Zur Anwendbarkeit der DSGVO führt nicht nur das Anbieten von Waren und Dienstleistungen, sondern bereits die blosse Beobachtung des Verhaltens von Personen in der EU.

Damit zielt die Verordnung primär auf Internetsachverhalte ab. Davon erfasst sind Datenbearbeitungsvorgänge, mit welchen das Verhalten von Personen in der EU, meist zu Werbezwecken, nachvollzogen werden soll.

Deshalb gelangt die DSGVO bei sämtlichen Methoden des sog. User/Customer-Trackings, insbesondere denjenigen, die unter Rückgriff auf Cookies funktionieren, zur Anwendung.

→ **Beispiel:**

Setzt also bspw. eine Tourismusorganisation auf seiner Website Analyse-Tools zur Auswertung der Website-Besuche und des Klickverhaltens (bspw. Google Analytics) ein, so muss von der Anwendbarkeit der DSGVO ausgegangen werden.

3. Beauftragung/Auftrag von EU-Unternehmen

Ein weiterer Umstand, der dazu führt, dass Schweizer Unternehmen ohne Niederlassung in der EU der DSGVO unterstehen, sind sog. *Auftragsdatenbearbeitungsverhältnisse*. Dies ist relevant, wenn ein Schweizer Unternehmen ein anderes Unternehmen oder einen beliebigen Dritten damit beauftragt, eigene Daten (bspw. Mitarbeiter- oder Kundendaten) zu eigenen Zwecken der Auftraggeberin zu bearbeiten.

→ **Beispiel:**

Nutzt ein Schweizer Unternehmen bspw. zur Speicherung von personenbezogenen Daten die Dienste eines Cloud-Anbieters mit Niederlassung in der EU, ist die DSGVO anwendbar. Gleiches gilt umgekehrt, wenn bspw. ein Schweizer Unternehmen Personendaten im Auftrag eines EU-Unternehmens bearbeitet. Erfolgt die zentrale Datenbearbeitung einer Hotelkette also bspw. durch ein Unternehmen in der Schweiz jedoch im Auftrag der einzelnen der Kette zugehörigen Hotels in der EU, müssen die Vorschriften der DSGVO beachtet werden.

Bei den vorgenannten Auftragsdatenbearbeitungskonstellationen kann die Beurteilung der Anwendbarkeit der DSGVO bzw. der Umfang der Anwendung der DSGVO im Einzelfall schwierig sein. In solchen Konstellationen ist eine sorgfältige Analyse der Datenbearbeitungen erforderlich.

III. Was gilt nun im Umgang mit Personendaten, bspw. Kundendaten?

Die DSGVO und auch die laufende Totalrevision des Schweizer Datenschutzrechts bringen weitreichende Neuerungen beim Umgang mit Personendaten mit sich. Das neue Schweizer Datenschutzgesetz (DSG) wird zwar voraussichtlich in verschiedenen Punkten weniger weit gehen als die neuen EU-Regelungen. Aufgrund des dargestellten weiten Anwendungsbereichs der EU-DSGVO werden jedoch, wenn überhaupt, nur sehr wenige Unternehmen der Schweizer Tourismusbranche nicht davon erfasst sein. Die allfälligen Unterschiede zwischen dem revidierten DSG und der DSGVO werden damit nur für ganz wenige Schweizer Unternehmen relevant werden. Bei den nachfolgenden Erläuterungen liegt der Fokus deshalb auf den bereits feststehenden, ab dem 25. Mai 2018 geltenden Vorgaben der DSGVO.

1. Die Bearbeitung von Personendaten ist grundsätzlich verboten, es sei denn…

Zentral aus der Sicht von Schweizer Unternehmen ist das in der DSGVO vorgesehene Konzept des sog. „**Verbots mit Erlaubnisvorbehalt“**:

> Jede Bearbeitung von personenbezogenen Daten ist verboten. Erlaubt ist eine Bearbeitung, bspw. von Kundendaten nur, wenn sich ein Unternehmen auf einen Erlaubnistatbestand berufen kann.

Erlaubnistatbestände sind nach der DSGVO:

- **„Einwilligung“**: Eine Datenbearbeitung ist zulässig, wenn sie auf einer wirksamen Einwilligung der betroffenen Person beruht. Die Anforderungen an eine gültige, rechtswirksame Einwilligung sind aber deutlich erhöht und entsprechen nicht der in der Schweiz bislang vorherrschenden unternehmerischen Praxis im Umgang mit Einwilligungen (s. dazu unten).
- **„Vertrag“**: Eine Datenbearbeitung kann erlaubt sein, wenn sie zur Erfüllung eines Vertrags mit der betroffenen Person erforderlich ist. Deshalb darf ein Hotel natürlich die Daten der Gäste nach wie

vor bearbeiten, soweit es für die Organisation und die Abrechnung des Aufenthaltes notwendig ist.

- **„Gesetz“**: Erlaubt sind Datenbearbeitungen, die zur Erfüllung einer gesetzlichen Verpflichtung (z.B. Aufbewahrungspflichten) erforderlich sind. Zu beachten ist, dass schweizerische Gesetze nicht unter diesen Erlaubnistatbestand fallen. Bei schweizerischen gesetzlichen Pflichten dürfte jedoch regelmässig ein überwiegendes Interesse gegeben sein (siehe nachfolgend).
- **„überwiegendes Interesse“**: Eine Datenbearbeitung kann schliesslich erlaubt sein, wenn sie zur Wahrung eines berechtigten Interesses des Unternehmens erforderlich ist. Das Interesse des Unternehmens muss dasjenige der betroffenen Person überwiegen. Hier ist aber gerade bei bloss wirtschaftlichen Interessen an der Durchführung von Marketingmassnahmen stets eine sorgfältige Prüfung im Einzelfall erforderlich.

2. Grundprinzipien jeder rechtmässigen Datenbearbeitung

Das Vorliegen eines Erlaubnistatbestands führt für sich alleine noch nicht dazu, dass eine Datenbearbeitung den Vorgaben der DSGVO entspricht. Vielmehr sind auch die sog. Datenbearbeitungsgrundsätze einzuhalten. Damit sind Grundprinzipien einer rechtmässigen Datenbearbeitung gemeint, die bereits im geltenden EU- und Schweizer Recht bestanden. Neu sind diese verschärft worden und vor allem ist deren Verletzung neu sanktionsbedroht.

Hervorzuheben sind dabei die folgenden Grundsätze:

- **Zweckbindungsgrundsatz**: Personenbezogene Daten dürfen nur für eindeutig definierte Zwecke erhoben und bearbeitet werden.
- **Transparenzgrundsatz**: Die Datenbearbeitung und die damit verfolgten Zwecke müssen für die betroffene Person ab dem Moment der Erhebung nachvollziehbar sein.
- **Datenminimierung**: Es dürfen nur personenbezogene Daten erhoben werden, die für die Erreichung des festgelegten Verarbeitungszwecks erforderlich sind. Es dürfen keine Daten auf Vorrat erfasst und weiterbearbeitet werden.
- **Speicherbegrenzung**: Personenbezogene Daten dürfen nur so lange gespeichert werden, als es zur Erreichung des festgelegten Verarbeitungszwecks erforderlich ist. Ist der Zweck erfüllt, müssen die Daten gelöscht werden.

3. Umfangreiche neue „Sorgfaltspflichten“ im Umgang mit Daten

Die DSGVO auferlegt den Unternehmen darüber hinaus eine Vielzahl von neuen formellen Pflichten.

Hervorzuheben ist dabei Folgendes:

- **Datenbearbeitungsverzeichnis**: Jedes Unternehmen, welches personenbezogene Daten bearbeitet, muss neu ein Verzeichnis aller relevanten Datenbearbeitungen führen. In diesem Verzeichnis muss für jeden Bearbeitungsprozess eine Reihe von Informationen dokumentiert und detailliert beschrieben werden (bspw. Zweck, Verantwortung, Art der Daten, spezifische Risiken, etc.).
- **Nachweispflicht**: Die DSGVO verlangt explizit, dass Datenbearbeiter jederzeit die Einhaltung der Datenbearbeitungsgrundsätze nachweisen können.
- **Datenschutz-Folgenabschätzung**: Bei Datenbearbeitungen, die voraussichtlich ein hohes Risiko für die Betroffenen in sich bergen können, muss eine Abschätzung dieser Folgen durchgeführt und dokumentiert werden. Dies wird insbesondere bei der Verwendung neuer Technologien und dem Einsatz neuartiger Datenbearbeitungsvorgängen zu prüfen sein. Die Datenschutz-Folgenabschätzung setzt sich aus der Beschreibung und Analyse der Datenbearbeitung, der Bestimmung der Risiken und der Erarbeitung eines Massnahmenplanes zur Reduktion der erkannten Risiken zusammen.
- **„Data Breach Notifications“**: Verstösse gegen die Vorgaben der DSGVO, insb. der Missbrauch oder der Diebstahl von Daten sind unter bestimmten Voraussetzungen der Aufsichtsbehörde und den

betroffenen Personen zu melden. Für die Umsetzung dieser Pflicht müssen in vielen Unternehmen dokumentierte interne Prozesse implementiert werden, d.h. es muss bestimmt werden, in welchen Konstellationen Mitarbeiter an welche interne verantwortliche Person Meldung machen müssen.

- **„Privacy by Design/ by Default"**: Die Datenbearbeitungen sind so auszugestalten, dass die Einhaltung des Datenschutzes und die Ausübungen der Betroffenenrechte (Auskunft, Löschung, Berichtigung) jederzeit sichergestellt ist (Privacy by Design). Zudem muss jede Datenbearbeitung so ausgestaltet sein, dass die datenschutzfreundlichsten Voreinstellungen als Standard hinterlegt sind (Datenschutz by Default).
- **Bestellung eines Vertreters**: Unternehmen ohne Niederlassung in der EU müssen in der Regel einen Vertreter in der EU bestellen.

4. Welche Rechte haben die Personen, deren Daten bearbeitet werden („Betroffenenrechte")

Eine rechtmässige Datenbearbeitung bedingt, dass die Personen, deren Daten bearbeitet werden, jederzeit nachvollziehen können, welche Daten über sie und in welcher Art und Weise bearbeitet werden. Die DSGVO sieht deshalb sog. Betroffenenrechte vor. Ein Grossteil der Rechte bestand zwar bereits im bisherigen Recht, doch wurden sie verschiedentlich ausgebaut und angepasst.

Eine betroffene Person hat insbesondere folgende Rechte. Diese kann sie jederzeit geltend machen:

- **Auskunftsrecht**: Die betroffenen Personen können von Unternehmen jederzeit detaillierte Auskunft über die sie betreffenden Datenbearbeitungen verlangen. Das Auskunftsrecht gilt auch für Arbeitnehmer.
- **Berichtigungsrecht**: Neben der grundsätzlichen Pflicht des bearbeitenden Unternehmens, Massnahmen zur Sicherstellung der Richtigkeit von Daten zu treffen, können betroffene Personen jederzeit die unverzügliche Berichtigung unrichtiger Daten fordern.
- **Löschungs- und Widerspruchsrecht**: Betroffene Personen können unter bestimmten Voraussetzungen der Durchführung einer Datenbearbeitung widersprechen und die Löschung von Daten verlangen.
- **Datenportabilität**: Nach der DSGVO müssen erfasste Daten so bearbeitet werden, dass sie der betroffenen Person jederzeit in einem strukturierten, gängigen und maschinenlesbaren Format herausgegeben werden können.

IV. Zentrale Vorgaben für die Tourismusbranche

Die meisten Unternehmen der Tourismusbranche führen regelmässig Datenbearbeitungen durch, die vom Anwendungsbereich der DSGVO (s. dazu oben) erfasst werden, auch wenn die Bearbeitung in der Schweiz erfolgt. Entsprechend müssen diese Datenbearbeitungen im Hinblick auf das Inkrafttreten der EU-DSGVO überprüft und allenfalls angepasst werden. Stichtag ist der 25. Mai 2018. Nachfolgend werden einige der für die Tourismusbranchen zentralen Datenschutzthemen beleuchtet und die wesentlichsten Problemstellungen erläutert.

1. Transparenz der Datenbearbeitung

a. Wenn die Daten direkt bei Kunden / Geschäftspartnern erhoben werden

Erster Schritt jedes Datenbearbeitungsvorgangs ist die Erhebung bzw. Beschaffung von Daten.

> Nach der DSGVO besteht bei jeder Beschaffung von personenbezogenen Daten die Pflicht,

umfangreiche Informationen rund um die beabsichtigte Datenbearbeitung aktiv, also unaufgefordert, zur Verfügung zu stellen.

Die Liste der gesetzlich vorgeschriebenen Informationen ist stark ausgebaut worden. Verlangt werden „leicht verständliche" und „präzise" Angaben zu den nachfolgenden Punkten:

1. Namen und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
2. Kontaktdaten des allfälligen Datenschutzbeauftragten
3. Zwecke und Rechtsgrundlage der Datenbearbeitung
4. Ggf. die berechtigten Interessen an einer Datenbearbeitung
5. Ggf. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
6. Ggf. die Absicht einer Übermittlung in Drittstaaten oder an eine internationale Organisation
7. Weitere Informationen, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten
8. Dauer der Datenspeicherung bzw. Kriterien für die Festlegung der Dauer
9. Bestehen von Betroffenenrechten wie Auskunft, Berichtigung, Löschung, Sperrung, Widerspruchsrecht oder Datenübertragbarkeit
10. Widerrufsrecht bei einwilligungsbasierter Datenbearbeitung
11. Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
12. Ggf., ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben ist oder für den Vertragsschluss erforderlich ist
13. Bestehen einer automatisierten Entscheidungsfindung einschliesslich Profiling sowie aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person

Diese Informationen müssen überall dort gut sichtbar und zugänglich sein, wo personenbezogene Informationen beschafft werden.

Dies ist insbesondere bei sämtlichen Kontakt- oder Bestellformularen der Fall. Die Unternehmen müssen deshalb Datenschutzerklärungen erstellen, welche die Pflichtinformationen enthalten, oder bereits vorhandene Datenschutzerklärungen überarbeiten. Diese Datenschutzerklärungen müssen schliesslich insbesondere über die Websites einfach und jederzeit auffindbar und zugänglich sein.

→ **Beispiele:**

Auch bei einer Datenerfassung, die nicht über ein elektronisches System erfolgt, etwa im Zusammenhang mit Meldeformularen, CRM-Karten oder Teilnahme-Talons für Gewinnspiele, ist sicherzustellen, dass diese Informationen den betroffenen Personen vorliegen (bspw. aufgedruckt auf der Rückseite einer CRM-Karte).

b. Wenn Daten aus dritten Quellen beschafft werden

Auch bei der Datenbeschaffung „aus Drittquellen" besteht eine Informationspflicht und es müssen, mit gewissen Abweichungen, dieselben umfangreichen Informationen erteilt werden.

Mit der Beschaffung aus Drittquellen sind Fälle gemeint, in welchen die Daten nicht bei den Betroffenen, sondern bspw. bei Dritten oder aus öffentlich zugänglichen Quellen erhoben werden.

→ **Beispiel:**

Solche indirekten Beschaffungen sind in der Tourismusbranche denkbar, wenn ein Hotel von einer Bergbahn Kontaktdaten von Skipassbestellern anfordert, um diesen Übernachtungsangebote zuzustellen. Das Hotel

muss den Kunden daher bei der Kontaktaufnahme darüber informieren, welche Daten es aus welchen Quellen erhalten hat und wozu es diese verwendet. In diesem Beispiel treffen damit sowohl die Bergbahn als auch das Hotel eine Informationspflicht. Sofern es sich bei der vorangehenden Datenweitergabe von der Bergbahn zum Hotel um einen üblichen Vorgang handelt, kann und sollte bereits die Bergbahn darüber informieren, dass und zu welchen Zwecken personenbezogene Daten an das Hotel weitergegeben werden. Diese Information durch die Bergbahn befreit allerdings das Hotel nicht zwingend von seiner eigenen Informationspflicht. Dies vor allem auch dann, wenn das Hotel die von der Bergbahn erhaltenen Daten auch noch für andere Zwecke bearbeiten möchte.

2. Einwilligung

Jede Bearbeitung von personenbezogenen Daten muss sich auf einen sog. Erlaubnistatbestand abstützen, andernfalls ist sie nach der DSGVO verboten. Einen sehr wichtigen Erlaubnistatbestand stellt die Einwilligung der betroffenen Person dar. Die Anforderungen an die Gültigkeit einer solchen Einwilligung werden mit der DSGVO deutlich erhöht.

> Damit eine Einwilligung gültig ist, muss sie insbesondere gestützt auf ausreichender vorgängiger Information und freiwillig erfolgen sowie in unmissverständlicher Form abgegeben werden.

Die erhöhten Anforderungen gelten auch, wenn Betroffene bereits vor dem Inkrafttreten der DSGVO eine Einwilligung erteilt haben. Mit anderen Worten sind auch **„Alteinwilligungen“** nur gültig, wenn sie die Anforderungen der DSGVO erfüllen.

a. Freiwilligkeit und Kopplungsverbot

Eine der zentralsten Anforderungen stellt die Freiwilligkeit der Einwilligung dar. An der Freiwilligkeit kann es fehlen, wenn ein klares Ungleichgewicht zwischen den Leistungen besteht, welche der betroffenen Person unter einem Vertrag zukommen, und den Datenbearbeitungen, in die im Rahmen des Vertrages eingewilligt wird.

Von besonderer Bedeutung ist die Frage, ob künftig ein sog. **Kopplungsverbot** gilt. Danach wäre es verboten, die Erfüllung eines Vertrags von der Einwilligung in weitere Datenbearbeitungen abhängig zu machen. Gemeint sind damit nicht Datenbearbeitungen, die für die Abwicklung eines Vertrags erforderlich sind, sondern primär die Verwendung von Daten zu Werbezwecken.

➔ **Beispiele:**

Im oben genannten Beispiel würde dies bedeuten, dass die Bergbahn die Ausstellung des Skipasses nicht von der Einwilligung des Kunden in die Weitergabe seiner Daten an das Hotel abhängig machen dürfte.

Besonders problematisch wäre ein absolutes Kopplungsverbot auch für die Durchführung von **Gewinnspielen**. So wäre es unzulässig, wenn für die Teilnahme an einem Gewinnspiel die Einwilligung in die Zustellung von Werbe-Mails (insb. Newsletter) verlangt würde.

Fest steht aktuell, dass solche Kopplungen problematisch sein können. Bis zu einer gefestigten Praxis durch die Aufsichtsbehörden sind solche Praktiken risikobehaftet und sollten entweder unterlassen werden oder es sollte den Betroffenen eine Wahlmöglichkeit zur Verfügung gestellt werden.

b. Vorangewählte Kästchen

Die Problematik des Kopplungsverbots wird weiter dadurch verstärkt, dass Einwilligungen nur dann gültig sind, wenn sie durch eine eindeutige, bestätigende Handlung zum Ausdruck gebracht werden.

Stillschweigen oder Untätigkeit der betroffenen Person genügen daher nicht.

→ **Beispiel:**

Im vorher genannten Beispiel des Gewinnspiels würde daher so oder so keine gültige Einwilligung für das E-Mail-Marketing vorliegen, wenn diese auf einem **vorangekreuzten Kästchen** basiert. Der Gewinnspielteilnehmer muss die Checkbox vielmehr selber durch einen Klick markieren, damit seine Einwilligung wirksam ist. Dies führt bei vielen Schweizer Unternehmen zu einer Umstellung. Nach schweizerischer Praxis sind solche vorangekreuzten Check-Boxen zulässig.

3. Weitergabe von Daten

a. Allgemein

Gerade innerhalb der Tourismus-Organisationen besteht ein erhebliches Interesse an der Weitergabe von Daten unter den Beteiligten.

Die Weitergabe von Daten an Dritte ist jedoch eine „Offenlegung durch Übermittlung" und insofern eine Datenbearbeitung, die den Vorgaben der DSGVO untersteht, sofern personenbezogene Daten betroffen sind.

Es besteht deshalb auch hier eine Informationspflicht. Die Weitergabe an sich muss transparent gemacht und es muss unter anderem erklärt werden, zu welchen Zwecken die Weitergabe erfolgt. Zudem muss der Datenübermittler auch hier nachweisen können, dass ein Erlaubnistatbestand (z.B. Einwilligung) gegeben ist.

Vernachlässigt wird dabei vielfach, dass auch die **Einräumung des Zugriffs** auf Daten als Übermittlung gilt.

Ein Beispiel hierfür wäre, dass Personendaten nicht an ein anderes (Partner)-Unternehmen (digital) transferiert werden, sondern dass das Partnerunternehmen z.B. Zugriff auf die Daten im CRM-System des übermittelnden Unternehmens erhält (d.h. das Hotel könnte z.B. direkt über eine Schnittstelle auf die Daten im CRM-System der Bergbahn zugreifen). Abgesehen von den datenschutzrechtlichen Fragen im Zusammenhang mit der Weitergabe von Personendaten, sind mit solchen Zugriffseinräumungen erhebliche Risiken der Datensicherheit verbunden.

b. „Dritte"

Vor diesem Hintergrund ist von besonderer Bedeutung, wer überhaupt als Dritter gilt.

Unternehmen ist oftmals nicht bekannt, dass auch Gesellschaften desselben Konzerns oder (rechtlich eigenständige) Mitglieder eines Verbands Dritte sind.

Deshalb sind auch bei der **konzerninternen Übermittlung** von Daten die Vorschriften der DSGVO zu beachten, also wenn einer Tochter- oder Schwestergesellschaft Zugriff auf personenbezogene Daten gewährt werden.

c. Auftragsdatenbearbeitung

Eine besondere Form der Weitergabe an Dritte erfolgt im Rahmen der sog. Auftragsdatenbearbeitung.

Gemeint sind damit Fälle, in welchen ein Auftraggeber ein anderes Unternehmen damit beauftragt, seine oder von ihm beschaffte Daten (bspw. Mitarbeiter- oder Kundendaten) in seinem Auftrag und für seine Zwecke zu bearbeiten.

Im Unternehmensalltag sind diese Konstellationen sehr häufig und bedeutsam.

➔ **Beispiele:**

Verbreitete Anwendungsfälle ergeben sich etwa beim Rückgriff auf folgende Dienste bzw. Programme:

- Mailchimp für Newsletterversand
- Google Analytics für Webanalyse
- Cloud-Anbieter für Datenspeicherung
- Microsoft 365 (Cloud-Lösung)
- Chatlio (Chatfunktionen auf Webseite)
- Social Monitoring Tools
- Salesforce / Microsoft Dynamics (CRM-Systeme)
- Webhoster

Zentral ist dabei, dass die DSGVO explizit den Abschluss eines Vertrags verlangt, wobei dies auch in einem „elektronischen Format" erfolgen kann. Im Online-Kontext genügt daher der Abschluss über eine Website. Im Vertrag muss sich der Auftraggeber Weisungs- und Kontrollrechte einräumen lassen. Mit anderen Worten muss der Beauftragte dazu verpflichtet werden, die Daten nur nach den Weisungen des Auftraggebers zu bearbeiten. Wichtiger Inhalt des Vertrags ist auch die Frage, ob der Beauftragte selber auf weitere Dritte **(Subunternehmen)** zurückgreifen darf oder nicht. Denn nach der DSGVO ist ihm dies nur mit Genehmigung des Auftraggebers gestattet.

➔ **Beispiel:**

Nutzt ein Tourismusunternehmen zur Analyse der Website-Nutzung den Dienst „Google Analytics" muss Google verpflichtet werden, Daten „weisungsgemäss" zu bearbeiten. Hierfür stellt Google eine Vertragsvorlage zur Verfügung, deren Rechtmässigkeit unter der DSGVO allerdings noch nicht abschliessend geklärt ist.

Der Auftraggeber darf Datenbearbeitungen nur an Unternehmen „auslagern", die durch die Implementierung von technischen und organisatorischen Massnahmen die Verarbeitung im Einklang mit der EU-DSGVO sicherstellen können. Der Auftraggeber bleibt aber in jedem Fall auch beim Einsatz eines Drittens verantwortlich für die Einhaltung der datenschutzrechtlichen Vorgaben. Allerdings treffen zahlreiche Pflichten der DSGVO auch den Auftragsdatenverarbeiter. Zudem können auch gegen ihn Sanktionen verhängt werden.

d. Übermittlung ins Ausland

Besondere Beachtung zu schenken ist stets auch der Frage, in welche Länder Daten übermittelt werden. Namentlich bei Übermittlungen in die USA ist Vorsicht geboten.

Die USA gelten als Land ohne angemessenes Datenschutzniveau, weshalb eine Datenübermittlung ohne besondere Vorkehrungen nicht erlaubt ist.

Eine solche besondere Vorkehrung für die Übermittlung von personenbezogenen Daten in die USA stellt die Zertifizierung durch das Empfängerunternehmen in den USA im Rahmen des sog. „Privacy-Shield"-Abkommens dar. Auch bei einer solchen Zertifizierung sind die anderen Pflichten der DSGVO (z.B. die Informationspflichten oder die Pflicht zur Rechtfertigung der Datenweitergabe) selbstredend weiterhin einzuhalten. In vielen Konstellation wird der Datentransfer in die USA zudem im Rahmen einer Auftragsdatenbearbeitung erfolgen.

In diesen Konstellationen muss nicht nur der Datentransfer DSGVO-konform erfolgen, sondern auch die Auftragsdatenbearbeitung.

Nebst der „Privacy-Shield"-Zertifizierung kommen auch andere besonderen Vorkehrungen in Frage. Aktuell gelten z.B. die sog. EU Standarddatenschutzklauseln als genügende Massnahme für Datentransfers in die USA. Zudem enthalten die meisten Muster-Auftragsdatenbearbeitungsverträge auch bereits diejenigen Bestimmungen, welche für datenschutzkonforme Datentransfers in die USA und andere Länder ohne angemessenes Datenschutzniveau notwendig sind.

➔ **Beispiel:**

Ein Hotel, das auf seiner Website den so genannten Remarketing Pixel von Facebook einsetzt, um personalisiertes Marketing in sozialen Netzwerken zu ermöglichen, übermittelt dabei grundsätzlich personenbezogene Daten an Facebook mit Sitz in den USA. Facebook ist ein unter dem „Privacy Shield" zertifiziertes Unternehmen, weshalb keine zusätzlichen Garantien erforderlich sind. Noch unklar und deshalb problematisch ist allerdings, wie mit Facebook ein ausreichender Auftragsverarbeitungsvertrag abgeschlossen werden kann.

4. CRM-Systeme

Grosse Herausforderungen bringt das Inkrafttreten der DSGVO auch für die Datenbearbeitungen im Rahmen von Kundenmanagement (CRM) Systemen. Der Sinn und Zweck dieser Systeme besteht unter anderem in der zentralen Speicherung aller relevanten Geschäftsvorgänge mit den einzelnen Kunden.

Gerade diese Zusammenführung bzw. Verknüpfung der Vielzahl von Daten aus unterschiedlichen Quellen ist aus datenschutzrechtlicher Sicht jedoch problematisch.

a. Transparenz und Rechtmässigkeit

Aufgrund der Informationspflicht und des Transparenzgebotes müssen die Kunden auf die Verknüpfung und zentrale Speicherung ihrer Daten aufmerksam gemacht werden. Damit verbunden ist auch die Frage nach dem „Rechtfertigungsgrund". Denn für die Speicherung von Bestelldaten kann zwar der Erlaubnistatbestand „Vertrag" in Frage kommen, jedoch wird für die Verknüpfung der Daten meist eine Einwilligung des Kunden erforderlich sein. Diese ist jedoch nur wirksam, wenn sie vom Kunden gestützt auf ausreichende Informationen über die Datenbearbeitung erteilt wird. Eine klare und vollständige Information der betroffenen Kunden ist deshalb unter beiden Aspekten verlangt.

➔ **Beispiel:**

Der Betreiber einer Website, über welche Gletscherwanderungen gebucht werden können, muss den Kunden unmittelbar beim Formular zur Eingabe der Kundendaten darüber informieren, dass seine Daten in einer zentralen Datenbank gespeichert und mit anderen Informationen, wie z.B. Beschwerden aufgrund einer unbefriedigenden Wanderroute, verknüpft werden. Zugleich muss der Betreiber die Einwilligung der Kunden einholen.

Zentral ist dabei, dass auch die von den Kunden erteilten Einwilligungen (inkl. Zeitpunkt sowie Wortlaut der Erklärung und der Informationen) dokumentiert werden und bei Bedarf rasch abgerufen werden können.

b. Zweckbindung und Zweckänderungen

In diesem Zusammenhang ist auch ein besonderes Augenmerk darauf zu richten, dass die vorhandenen Daten nicht zu neuen Zwecken bearbeitet werden,

die durch den ursprünglich angegebenen Zweck nicht mehr gedeckt sind. Dies kann insbesondere bei **„Altdaten“** problematisch sein.

> Sollen personenbezogene Daten aus einer Datenbank in eine andere überführt werden, ist deshalb stets zu prüfen, ob hierdurch nicht eine Zweckänderung erfolgt.

Ist dies der Fall, muss der betroffene Kunde darüber informiert werden und er muss seine Einwilligung in die Datenbearbeitung zum neuen Zweck erteilen.

Die gleiche Herausforderung stellt sich, wenn aus den vorhandenen Daten neue Erkenntnisse abgeleitet werden sollen. Bei solchen **CRM- oder Big-Data-Analysen** lässt sich im Vornherein teilweise nur schwer definieren, welche konkreten Erkenntnisse letztlich gewonnen werden. Daher ist bei der Formulierung der Informationen, insbesondere des Zwecks der Datenbearbeitung, besondere Vorsicht geboten.

→ **Beispiel:**

Hat der Anbieter im obigen Gletscherwanderungs-Beispiel in seiner Datenschutzerklärung darüber informiert, dass die Daten zum Zweck ausgewertet werden, den Kunden einen bestimmten „Scorewert“ zuzuweisen, damit ihnen personalisiert Werbung zugestellt werden kann, dann darf er die Analyse nicht auch auf die Festsetzung eines individualisierten Preises ausweiten. Unter Umständen gehen jedoch später aus der Analyse auch Erkenntnisse hinsichtlich des Preises hervor, sodass bereits eine Zweckänderung vorliegen würde.

Weitgehend ungeklärt ist auch nach wie vor, wie solche Analysen mit dem Grundsatz der **Datensparsamkeit** in Einklang gebracht werden können. Ist doch gerade die Generierung und Auswertung einer möglichst grossen Zahl von Daten für die Aussagekraft der Analyse-Ergebnisse entscheidend. Die DSGVO verlangt aber jedenfalls, dass bereits bei der Erhebung darüber informiert wird, wie lange Daten gespeichert werden oder, „falls dies nicht möglich ist“, welches die Kriterien für die Festlegung der Speicherdauer sind. Die Unternehmen müssen deshalb in jedem Fall auch für das CRM-System ein **Konzept für die Löschung bzw. Aufbewahrung** von personenbezogenen Daten definieren.

c. Zugriffsrechte und Weitergabe

Für den datenschutzkonformen Einsatz von CRM-Systemen ist auch die Regelung der Zugriffsrechte besonders wichtig.

> Es muss sichergestellt werden, dass Mitarbeiter nur auf diejenigen Daten zugreifen können, die für die Erfüllung ihrer Aufgabe erforderlich ist.

Dieses **„Need-to-know-Prinzip“** ist durch ein Berechtigungskonzept umzusetzen, in welchem Zugriffsregeln für einzelne Benutzer oder Benutzergruppen festgelegt werden.

Neben diesem unternehmensinternen Aspekt ergeben sich auch bereits aus der Wahl des jeweiligen CRM-Systems grundlegende Anforderungen. Denn ein Grossteil solcher Systeme basiert auf einer Cloud-Lösung und die Anbieter oder die Hoster befinden sich im Ausland. In diesem Fall sind wiederum die Vorgaben für die **Übermittlung ins Ausland** sowie die **Auftragsdatenbearbeitung** zu beachten.

5. E-Mail-Marketing

Für die Zustellung von Werbe-E-Mails und insbesondere den Versand eines Newsletters ergeben sich weitere Fragestellungen aus dem Zusammenspiel von Datenschutz- und Wettbewerbsrecht. Denn zum einen werden dabei regelmässig personenbezogene Daten bearbeitet und zum anderen sehen die nationalen Gesetze strenge Vorschriften zum Schutz vor „Spam“ vor.

Eine Schweizer Besonderheit besteht darin, dass Verstösse gegen den „Spam-Artikel" bereits heute **strafrechtlich sanktioniert** sind.

Vor diesem Hintergrund sollten Unternehmen beim E-Mail-Marketing besonderen Wert auf die Einhaltung der rechtlichen Vorgaben legen.

a. Einwilligung („Opt-in")

Für die Rechtmässigkeit von Werbe-E-Mails ist regelmässig eine **Einwilligung** des Empfängers erforderlich.

Wie bereits ausgeführt, ist eine Einwilligung nur gültig, wenn sie gestützt auf einer hinreichenden Information über die mit dem Versand verbundenen Datenbearbeitungen erfolgt. Diese Informationen sind daher ebenfalls in die **Datenschutzerklärung** aufzunehmen und im Rahmen des Registrierungsprozesses an prominenter Stelle zu platzieren.

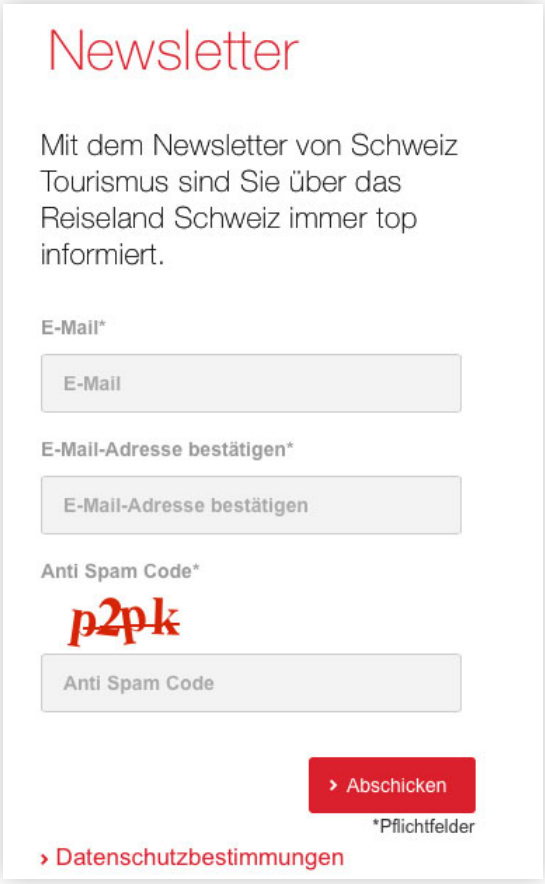
Weiter stellt sich die Frage, in welcher Form die Einwilligung der Interessenten eingeholt werden kann. Es wurde bereits erläutert, dass **vorangekreuzte Kästchen** nach der DSGVO nicht für eine wirksame Einwilligung genügen. Darüber hinaus ist Unternehmen dringend zu empfehlen, das sog. **„Double Opt-in"-Verfahren** einzusetzen:

1. Hierfür wird im Rahmen des Anmeldeprozesses zunächst ein erstes „Opt-in" für die Zustellung des Newsletters an die eingegebene E-Mail-Adresse verlangt.
2. In einem zweiten Schritt wird dann unmittelbar danach und bevor der Newsletter erstmals zugestellt wird, ein E-Mail versandt mit der Aufforderung zur Bestätigung der Anmeldung durch einen Klick auf einen entsprechenden Link (zweites „Opt-In").

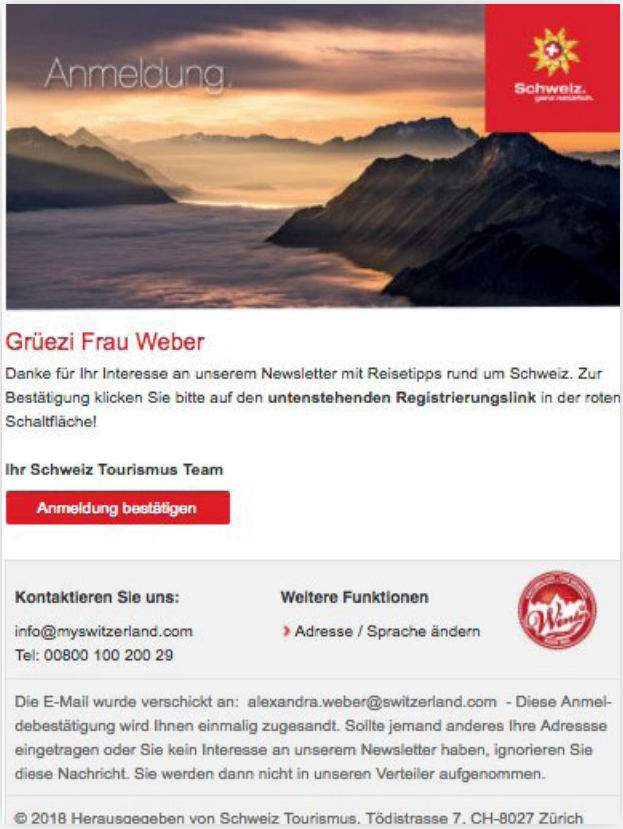
Vorteil dieses Verfahrens ist, dass sich die Einwilligung durch das „zweite Opt-in" relativ leicht und gut dokumentiert nachweisen lässt.

→ **Beispiel:**

Im Beispiel des Newsletters von Schweiz Tourismus sieht Schritt 1 dann folgendermassen aus:



Schritt 2 im Sinne des Double-Opt-In könnte wie folgt umgesetzt werden:



b. Weitergabe an Dritte und Übermittlung ins Ausland

Für den Versand des Newsletters greifen Unternehmen regelmässig auf Tools von Dritten zurück. Je nach konkreter Ausgestaltung kann dies dazu führen, dass ein **Auftragsdatenbearbeitungsverhältnis** vorliegt. In diesem Fall sind die bereits erläuterten Anforderungen einzuhalten, also namentlich eine Vereinbarung über die Weisungs- und Kontrollrechte abzuschliessen. Hinzu kommt, dass verschiedene Anbieter, wie z.B. MailChimp, ihren Sitz in den USA haben und Daten auf diesen Servern gespeichert werden. Dies hat zur Folge, dass auch die Anforderungen (insb. Informationspflicht und Garantien) für die **Übermittlung ins Ausland** zu beachten sind.

Zusätzliche Vorgaben bestehen auch dann, wenn der Versand des Newsletters selbst grenzüberschreitend erfolgt. Sofern ausländischen Interessenten eine Registrierung offen steht, sind unter Umständen auch die **nationalen Vorschriften anderer Staaten** zu beachten. Dies hängt insbesondere davon ab, ob die Website und das Angebot des Newsletters auch auf Kunden in diesen Ländern „ausgerichtet" ist, was relativ rasch der Fall ist. Es gelten somit im Wesentlichen die gleichen Kriterien, wie bei der Frage nach der Anwendbarkeit der DSGVO auf Schweizer Unternehmen ohne EU-Niederlassung (siehe oben).

> In der Konsequenz unterstehen Newsletter von Schweizer Tourismusunternehmen regelmässig auch den Vorschriften des deutschen Rechts.

Im deutschen Recht genügt bereits eine einzige Werbe-Mail ohne Einwilligung um als Spammer eine Abmahnung zu erhalten, mit welcher Unterlassungsansprüche geltend gemacht und die Erstattung von Anwaltskosten verlangt werden. Bei der Ausgestaltung des Newsletter-Prozesses dürfen deshalb neben der DSGVO auch weitere ausländische Rechtsvorschriften nicht vernachlässigt werden.

6. Webanalyse/Tracking

Im Rahmen des Marketingkonzepts spielt selbstredend auch die Website des Unternehmens eine zentrale Rolle. Zur Auswertung der Website-Besuche wird dabei auf Dienste, wie Google Analytics, zurückgegriffen.

Aus datenschutzrechtlicher Sicht sind in diesem Zusammenhang verschiedene Anforderungen einzuhalten, welche bereits an früherer Stelle erläutert wurden. So erfolgt, wie im Beispiel von Google Analytics, häufig eine Datenübermittlung an einen Dritten, der seinen Sitz in den USA hat.

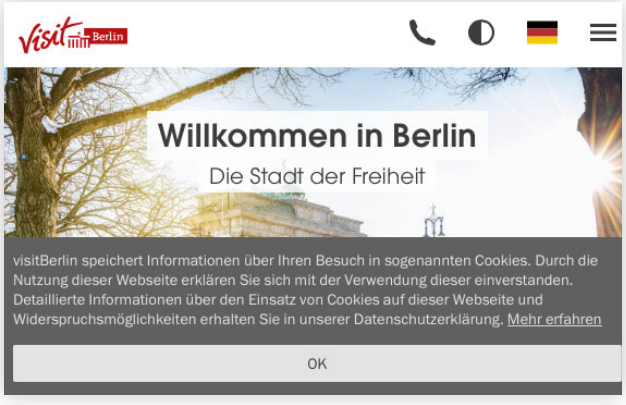
> Deshalb sind die Anforderungen an die Auftragsdatenbearbeitung und die Datenübermittlung

in Drittstaaten einzuhalten. Darüber hinaus müssen der Einsatz solcher Dienste, zur Erfüllung der Informationspflicht, in der Datenschutzerklärung offengelegt und die damit verbundenen Datenbearbeitungen erläutert werden.

Bekanntlich basieren die Analyse-Tools regelmässig auf dem **Einsatz von Cookies** oder vergleichbaren Technologien, durch welche das Klickverhalten der Nutzer über mehrere Seiten nachverfolgt werden kann. Bereits nach geltendem EU-Recht müssen User vor dem Setzen von Cookies hierüber informiert und nach ihrer Einwilligung gefragt werden. In der Praxis wird diese Anforderung derzeit primär über die verbreiteten **Cookie-Banner** umgesetzt, welche beim Einstieg auf eine Website eingeblendet werden.

→ **Beispiel:**

Als Beispiel aus dem benachbarten Deutschland hat Berlin Tourismus auf seiner Website derzeit folgenden Banner eingeblendet.



Quelle: https://www.visitberlin.de/de (besucht am 29.1.2018)

Zu beachten ist jedoch, dass in der EU eine strenge Regelung für Cookies geplant ist, welche ergänzend zur DSGVO zur Anwendung gelangen soll. Der konkrete Inhalt dieser sog. **ePrivacy-Verordnung** steht aktuell noch nicht fest. Allerdings zeichnet sich ab, dass künftig auch die bisherigen Cookie-Banner nicht mehr genügen werden. Die weitere Entwicklung ist deshalb im Auge zu behalten.

7. Social-Media Monitoring

Der Grossteil der Unternehmen ergänzt sein Marketing-Konzept auch mit einer Präsenz auf den einschlägigen Social Media Plattformen. Auf diesen Plattformen äussern sich tausende Nutzer täglich über Produkte und Anbieter. Für viele Unternehmen ist es daher gängige Praxis, neben den klassischen Medien auch Social Media zu beobachten und zu analysieren.

Sowohl im Schweizer als bspw. auch im deutschen Recht bestanden bisher Sondervorschriften für die Datenbearbeitung von öffentlich zugänglich gemachten Daten. Vergleichbare Regelungen sind in der DSGVO nicht mehr vorhanden, weshalb sich die Rechtslage auch in diesem Bereich deutlich verschärft. Die bereits nach bisherigem Recht problematischen Praktiken des Social Media Monitoring sind deshalb mit erheblichen Risiken behaftet.

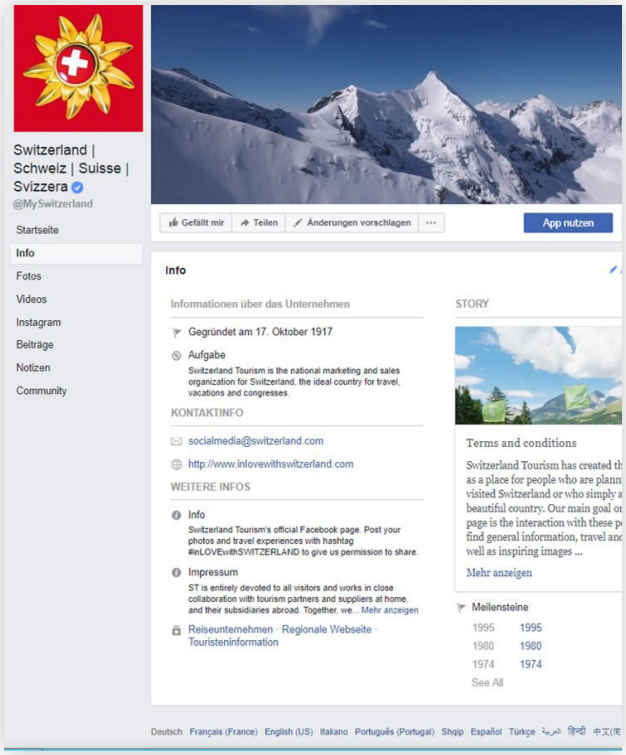
Besondere Herausforderungen stellen sich bereits bei der Erfüllung der **Informationspflicht**. Diese greift auch dann, wenn Daten nicht bei der betroffenen Person selbst erhoben werden.

Auf den Plattformen stellt sich allerdings die Frage, wie diese Informationen den Betroffenen in hinreichender Form erteilt werden können.

Zumindest in Bezug auf Daten, die ein Nutzer auf dem Profil eines Unternehmens (z.B. durch das Verfassen eines Posts) hinterlässt, ist die Platzierung in einer gesonderten Rubrik auf dem Profil denkbar. Anders als bspw. bei Kontaktformularen auf einer Website können diese Informationen allerdings in der Regel nicht unmittelbar dort verlinkt werden, wo der Nutzer seinen Post anbringt. Deshalb ist nach aktuellem Stand fraglich, ob die Aufsichtsbehörden diese Praxis genügen lassen.

→ **Beispiel:**

Würde daher Schweiz Tourismus auf seinem Facebook-Profil unter der Rubrik „Info" neben „Terms and conditions" zusätzliche Informationen zum Datenschutz einbinden, erscheint es fraglich, ob diese genügend transparent sind.



Ausgehend davon müssten die Pflicht-Informationen nachträglich jedem einzelnen Nutzer zur Kenntnis gebracht werden. Dies gilt umso mehr bei der Erhebung von Daten, die Nutzer in anderen öffentlich zugänglichen Bereichen veröffentlicht haben. In diesen Fällen stellt sich allerdings ohnehin die Frage, ob sich das Unternehmen auf einen Erlaubnistatbestand berufen könnte. In der Regel wird ein solcher Fehlen. Was die Sammlung von Daten in nicht-öffentlichen Bereichen betrifft, wird diese, wie bereits nach geltendem Recht, stets unzulässig sein.

→ **Beispiele:**

Hinterlässt ein Nutzer auf dem öffentlichen Facebook-Profil von Schweiz Tourismus einen Post mit einer Frage über ein aktuelles Angebot, darf dieser beantwortet und die ersuchte Leistung grundsätzlich erbracht werden. Unzulässig wäre aber die Einbindung der Daten in das CRM-System, weil hierfür eine informierte Einwilligung des Nutzers erforderlich wäre.

Postet ein Nutzer auf seinem nicht-öffentlichen Facebook-Profil ein Foto und Bemerkungen zu seinem Skiweekend in den Schweizer Bergen, dürfen die Unternehmen darauf weder antworten noch die Daten anderweitig weiterverarbeiten. Denn auch hierfür wäre stets eine informierte Einwilligung erforderlich.

Weitere Informationen zum Thema auf unserem Blog **mll-news.com**.

Haben Sie Fragen? Wir beraten Sie gerne.

Lukas Bühlmann, LL.M.
lukas.buehlmann@mll-legal.com
T +41 44 396 91 91

Meyerlustenberger Lachenal AG
Rechtsanwälte – Attorneys at Law
Schiffbaustrasse 2 | Postfach 1765 | CH-8031 Zürich
www.mll-legal.com | www.mll-news.com

Alexandra Weber
alexandra.weber@switzerland.com
T +41 44 288 12 32

Schweiz Tourismus
Tödistrasse 7 | CH-8027 Zürich
MySwitzerland.com