Reisenetz

Deutscher Fachverband für Jugendreisen

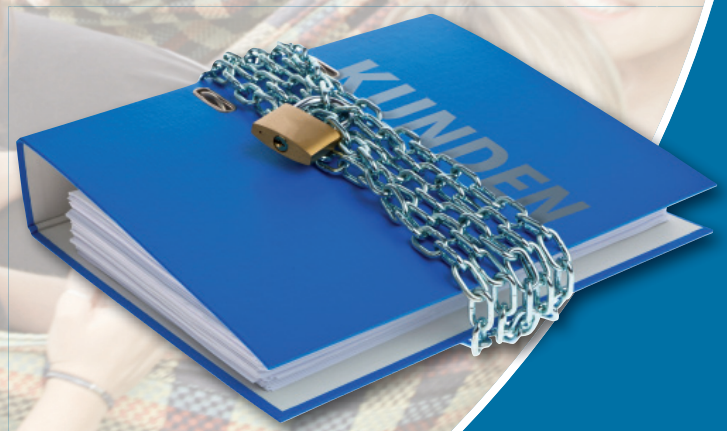
Köpenicker Straße 126 | 10179 Berlin | Germany
Fon +49 (0)30.24 62 84 30 | Fax +49 (0)30.24 62 84 90
info@reisenetz.org | **www.reisenetz.org**

Reisenetz

Deutscher Fachverband für Jugendreisen

Datenschutz bei Kinder- und Jugendreisen

Leitfaden zum praktischen Umgang mit dem Datenschutzrecht



Die Erstellung dieses Leitfadens wurde gefördert durch das Bundesministerium für Familie, Senioren, Frauen und Jugend.

INHALTSVERZEICHNIS

VORWORT

Die Akteure des Kinder- und Jugendreisens sind daran gewöhnt, sich mit einer ganzen Reihe von gesetzlichen Rahmenbedingungen auseinander zu setzen. Ob BGB mit seinem (Reise)-Vertragsrecht und den Grundlagen der Aufsichtspflicht, Jugendschutzgesetz, Personenbeförderungsgesetz oder KJHG – viele dieser Gesetze sind Bestandteil der täglichen Arbeit. Anders sieht es mit dem Bundesdatenschutzgesetz aus, das in der ersten Fassung bereits 1975 in der Bundesrepublik Deutschland verabschiedet wurde.

Wer an Datenschutz denkt, denkt automatisch an die großen Skandale, welche in der jüngeren Vergangenheit Einzug in die Medien gehalten haben. Aber Datenschutz beginnt weit früher: bei alltäglichen geschäftlichen Kontakten. Im Zeitalter der schnellen und globalen Kommunikation sind Daten rasch übertragen und einfach veröffentlicht – aber kaum jemals rückholbar. Datenschutz endet auch nicht an den Grenzen Deutschlands oder der Europäischen Union. Gerade in den so genannten „Drittländern“, also Staaten außerhalb des Europäischen Wirtschaftsraums, ist die gesetzliche Situation, geschweige denn deren Umsetzung, mit jener in Europa kaum vergleichbar. Dennoch ist es mitunter erforderlich, so z. B. in der Touristik, Daten von Kunden auch an Empfänger in diesen Ländern zu übermitteln. Hier kann besondere Vorsicht, Aufmerksamkeit und Zurückhaltung erforderlich werden.

Die gesetzlichen Bestimmungen zum Datenschutz greifen immer nur dann, wenn es sich um personenbezogene Daten, also Angaben zu einer natürlichen Person handelt. Neben der Kenntnis der elementaren gesetzlichen Bestimmungen zum Datenschutz sind immer auch Einfühlungsvermögen und Fingerspitzengefühl gefragt, wenn es darum geht, Persönlichkeitsrechte Dritter und ökonomische Zielsetzungen und Zwänge zu vereinen.

Dieser Reisenetz-Leitfaden kann und soll nicht sämtliche Aspekte des Datenschutzes beleuchten; nicht alle sich in diesem Zusammenhang stellenden Fragen beantworten. Es kann und soll aber einen Überblick über die einschlä-

gigen gesetzlichen Regelungen und deren spezifischen Anwendungsbereiche im Bereich Kinder- und Jugendreisen geben und darüber hinaus Tipps und Tricks vermitteln, mittels derer sich Datenschutzprobleme der täglichen Praxis ohne großen Aufwand erkennen, vermeiden oder lösen lassen.

Frank Jander
(Kedua GmbH, Berlin)

1. EINFÜHRUNG IN DAS DATENSCHUTZRECHT

1.1 Was ist durch das Datenschutzrecht geschützt?

Das Datenschutzrecht der Bundesrepublik Deutschland schützt nicht sämtliche Daten. So sind z.B. technische Daten, welche ein Maschinenführer zur Bearbeitung eines Werkstücks eingibt, nicht vom gesetzlichen Schutz erfasst. Dies ist darauf zurückzuführen, dass das Datenschutzrecht ausschließlich geschaffen wurde, um die Persönlichkeit von Menschen vor den Risiken der zunehmenden Technisierung und Automatisierung zu schützen. Menschen sind Individuen mit eigenen Gedanken, Vorstellungen, Zielen, Wünschen, Eigenschaften und Erinnerungen, die nicht unbedingt dazu bestimmt sind, anderen Personen oder gar der breiten Öffentlichkeit zugänglich gemacht zu werden. Hieraus bestimmt sich das Schutzgut aller Datenschutzgesetze in Deutschland – personenbezogene Daten.

1.2 Personenbezogene Daten

Selbstverständlich stellt sich in diesem Zusammenhang zunächst die Frage, was denn überhaupt personenbezogene Daten sind. Bei der Beantwortung dieser Frage ist der Gesetzgeber selbst sehr hilfreich gewesen, da er einige Begriffe unmittelbar im Gesetz definiert hat. Demnach sind personenbezogene Daten „Angaben zu persönlichen oder sachlichen Verhältnissen einer bestimmten oder bestimmbaren natürlichen Person“ (§ 3 Abs. 1 BDSG). Somit beschränkt sich der gesetzliche Schutzbereich auf lebende Menschen, aber auch auf Personengesellschaften. Grundsätzlich nicht erfasst hingegen sind die Kapitalgesellschaften, wie GmbH oder AG, also die juristischen Personen, aber auch eingetragene Vereine (e.V.).

Erfasst werden nicht nur diejenigen Daten, welche unmittelbare Rückschlüsse auf einen Menschen und dessen Lebensverhältnisse zulassen, sondern auch solche, die nur einen mittelbaren Personenbezug ermöglichen. Dies gilt ins-

besondere bei pseudonymisierten Datensätzen, welche eine Repersonifizierung zulassen, z.B. Nicknames, Kundennummern, Personalnummern, IP-Adressen ö.ä..

1.3 Besondere Arten personenbezogener Daten

Einer gesteigerten Schutzbedürftigkeit unterliegen die so genannten „besonderen Arten personenbezogener Daten“ gemäß § 3 Abs. 9 BDSG („**sensitive Daten**“), also Angaben, welche bei unbefugter Weitergabe oder Nutzung zu erheblichen **Nachteilen materieller wie immaterieller Art** beim Betroffenen führen können. Sensitiv sind laut Gesetzgeber Angaben über

- rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder philosophische Überzeugungen,
- Gewerkschaftszugehörigkeit,
- Gesundheit oder
- Sexualleben

eines Betroffenen.

Die nähere Betrachtung dieser Aufstellung zeigt, dass nicht nur im Sektor der Personaldatenverwaltung sensitive Daten erhoben, verarbeitet oder genutzt werden (religiöse Überzeugungen, Gesundheit, evtl. Gewerkschaftszugehörigkeit), sondern in der Reisebranche durchaus auch im Kundensegment solche Daten vorhanden sein können (Gesundheit, ethnische Herkunft, Religion etc.). Solche Angaben sind durch besondere Maßnahmen so zu schützen, dass Risiken für die Betroffenen nach dem aktuellen Stand der Technik weitestgehend ausgeschlossen werden können.

2. GESETZLICHE BESTIMMUNGEN

2.1 Recht und Gesetz

Beim Thema Datenschutz ist die Frage, welches Gesetz zur Anwendung kommt, häufig nur schwer zu beantworten. Neben dem bereits erwähnten Bundesdatenschutzgesetz (BDSG) besteht für jedes Bundesland noch ein Landesdatenschutzgesetz (LDSG). Die Landesdatenschutzgesetze befassen sich jedoch ausschließlich mit den Belangen der öffentlichen Landesverwaltungen. Gleiches gilt für den zweiten Abschnitt des BDSG, welcher die Datenverarbeitung der öffentlichen Bundesverwaltung normiert.

Innerhalb des Sektors der privaten Wirtschaft nimmt der Gesetzgeber keine weiteren Differenzierungen, z.B. nach Branchen vor. In der Praxis hat es sich bewährt, folgende Kriterien zu hinterfragen:

- Sensitivität der zur Verarbeitung kommenden Daten (insbes. § 3 Abs. 9 BDSG),
- Schadenshöhe, welche potentiell seitens des Betroffenen erwartet werden kann (hierzu zählen auch immaterielle Schäden) und
- Schadenseintrittswahrscheinlichkeit.

Neben dem Bundesdatenschutzgesetz können aber noch andere Rechtsvorschriften zur Anwendung gelangen, denn das BDSG ist lediglich ein so genanntes „Auffanggesetz“. Dies bedeutet, dass es immer nur dann zur Anwendung kommt, wenn kein spezielleres Gesetz es verdrängt. Nur dann, wenn keine spezialgesetzlichen Regelungen vorhanden sind, oder wenn diese Regelungslücken aufweisen, kann das BDSG überhaupt angewandt werden. Diese Spezialgesetze haben häufig völlig andere Schutzgüter, als das eigentliche, das spezifische, Datenschutzrecht. Will letzteres die Persönlichkeitsrechte von Menschen schützen, vgl. oben, verfolgen die Spezialgesetze häufig andere Schutzinteressen, verfügen aber nebenher noch über datenschutzrechtlich relevante Inhalte.

Der Vorrang solcher Vorschriften gegenüber dem BDSG ergibt sich aus § 1 Abs. 3 S. 1 BDSG: „Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor."

Beispiel:
Das Mutterschutzgesetz hat zum Ziel, Leib, Leben und körperlicher Unversehrtheit von Mutter und Kind zu schützen, seine Schutzrichtung ist somit eine völlig andere, als jene des BDSG (Persönlichkeitsrechte). Wenn aber nun das Mutterschutzgesetz den Arbeitgeber einer schwangeren Beschäftigen verpflichtet, Schutzmaßnahmen einzurichten und deren Umsetzung zu gewähren, so enthält es hierin auch einen Erlaubnistatbestand zugunsten des Arbeitgebers. Dieser ist nicht nur verpflichtet, sondern auch berechtigt, die zur Umsetzung der Schutzmaßnahmen erforderlichen, höchstpersönlichen, Daten seiner Mitarbeiterin zu erfassen und zu dem vom Mutterschutzgesetz definierten Zweck auch zu verwenden.

2.2 Struktur des Bundesdatenschutzgesetzes (BDSG)

Das BDSG gliedert sich in sechs Abschnitte:

1. Abschnitt: Allgemeine und gemeinsame Bestimmungen
Der erste Abschnitt beinhaltet alle diejenigen Vorschriften, welche gleichermaßen für alle nachfolgenden Abschnitte zur Anwendung kommen sollen. Hier wird praktisch auf mathematische Art und Weise „vor die Klammer gezogen", was für das gesamte nachfolgende Gesetz Anwendung findet („Allgemeiner Teil").

2. Abschnitt: Datenverarbeitung der öffentlichen Stellen
Vorschriften aus diesem Abschnitt sind sachlich für Unternehmen der privaten Wirtschaft nicht anwendbar! Auf den zweiten Abschnitt des BDSG wird deshalb an dieser Stelle bewusst nicht näher eingegangen.

3. Abschnitt: Datenverarbeitung nicht öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen
Gemeinsam mit dem ersten Abschnitt bildet dieser Abschnitt den Kernbereich der Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Sektor der privaten Wirtschaft. Er untergliedert sich in drei Unterabschnitte:

- Rechtsgrundlagen der Datenverarbeitung,
- Rechte der Betroffenen und
- Aufsichtsbehörde.

Der erste Unterabschnitt beinhaltet die wesentlichen Erlaubnistatbestände für die Datenverarbeitung durch privatwirtschaftliche Unternehmen. Ihm kommt somit eine besondere Bedeutung zu.

4. Abschnitt: Sondervorschriften
Vorschriften des vierten Abschnitts finden nur in Ausnahmefällen Anwendung. Bislang galt dieser Abschnitt der Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen sowie durch die Medien. Anlässlich der Reform des BDSG im Jahre 2009 wurde der vierte Abschnitt um eine neue Vorschrift erweitert: die „Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten", § 42a BDSG. Sie verpflichtet Unternehmen der privaten Wirtschaft in bestimmten Fällen, Aufsichtsbehörden, Betroffene oder gar die Öffentlichkeit über Datenschutz-Pannen in Kenntnis zu setzen.

5. Abschnitt: Schlussvorschriften
Hinter dieser harmlos klingenden Überschrift verbergen sich Ordnungswidrigkeiten und Straftatbestände.

6. Abschnitt: Übergangsvorschriften
Dieser Abschnitt dient der Anpassung bei Reformen des BDSG. Derzeit besteht lediglich eine Übergangsregelung für den Bereich der personifizierten Werbung. Sie gilt noch bis zum 31. August 2012 und nur für Daten, welche vor dem 01. September 2009 erhoben wurden.

2.3 Wesentliche Regelungen

Wie bereits oben festgestellt, ist für den Bereich der privaten Wirtschaft nicht das gesamte BDSG anwendbar. Völlig irrelevant ist der gesamte zweite Abschnitt, da dessen Vorschriften ausschließlich die Datenverarbeitung der öffentlichen Bundesverwaltung betreffen. Ebenfalls von geringer Bedeutung ist schließlich der sechste Abschnitt. Mit einer Ausnahme, s.o. bereits hinfällig sind die dort enthaltenen Übergangsvorschriften.

2.3.1 Verbot mit Erlaubnisvorbehalt

Unbedingt beachtet werden sollte, dass das BDSG ein im gesamten Sektor des Schutzes personenbezogener Daten geltendes „Verbot mit Ausnahmevorbehalt" normiert, vgl. § 4 Abs. 1 BDSG. Dies bedeutet, dass es zunächst einmal unzulässig ist, personenbezogene Daten Dritter zu erheben, zu verarbeiten oder zu nutzen, es sei denn, dass im konkreten Einzelfall ein Erlaubnistatbestand dies gestattet. Der Erlaubnistatbestand kann sich einerseits aus einer spezialgesetzlichen Regelung oder aus dem BDSG selbst ergeben. Für das Vorhandensein eines solchen Erlaubnistatbestandes trägt im Streitfalle immer die für die Erhebung, Verarbeitung oder Nutzung der Daten verantwortliche Stelle die Verantwortung und die Beweislast. Aus diesem Grunde ist jedes Unternehmen gut beraten, die Rechtsgrundlagen, auf welche Verarbeitungsprozesse personenbezogener Daten gestützt werden, nachweisbar zu dokumentieren.

2.3.2 Die wichtigsten Erlaubnistatbestände

Immer, wenn ein Unternehmen personenbezogene Daten erheben, verarbeiten oder nutzen möchte, bedarf es eines Erlaubnistatbestandes, auf welchen der jeweilige Vorgang gestützt werden kann. Die wichtigsten Arten von Erlaubnistatbeständen sind:

- gesetzliche Verpflichtungen,
- die Einwilligung des Betroffenen,
- rechtsgeschäftliche oder sonst zulässige Zweckbestimmung,
- Interessenabwägung,
- Öffentlichkeit der Daten.

Gesetzliche Verpflichtungen

Wie bereits oben dargestellt, verpflichtet der Gesetzgeber sehr häufig Unternehmen, personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen, bzw. diese über den Wegfall ihrer ursprünglichen Zweckbestimmung hinweg aufzubewahren. Neben den bereits erwähnten Pflichten aus dem Mutterschutzgesetz lassen sich hier insbesondere folgende Beispiele nennen:

- Einkommenssteuergesetz – verlangt die Speicherung aller abrechnungsrelevanten Unterlagen über einen Zeitraum von 10 Jahren,
- ELENA-Gesetzgebung – verlangt die Weitergabe vieler Daten aus Arbeitsverhältnissen an Finanzämter.

Aber auch ausländische Anforderungen können hierunter fallen, wie z.B. die Weitergabe von Informationen an Regierungsstellen der USA bei Einreisen (Flugdaten, Pass- und Meldedaten, etc.). Diese Datenübermittlung wurde von der Europäischen Union überprüft und legitimiert. Gleiches gilt für die Swift-Daten im internationalen Zahlungsverkehr.

Einwilligung des Betroffenen

Die Einwilligung des Betroffenen in bestimmte Verarbeitungsprozesse ist der Kernausdruck des Rechts auf informationelle Selbstbestimmung. Jedermann darf selbst uneingeschränkt in die Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einwilligen. Die Einwilligung ist ein im BDSG ausdrücklich vorgesehener Erlaubnistatbestand, § 4 Abs. 1 BDSG i.V.m. § 4a BDSG.

Dabei gilt es, viele Details zu beachten, damit die Einwilligung auch wirksam zustande kommt:

- Eine Einwilligung muss immer im Vorfeld der beabsichtigten Tätigkeit eingeholt werden. Eine nachträgliche Zustimmung genügt nicht (dies wäre im rechtstechnischen Sinne dann eine Genehmigung).

- Die Einwilligung muss in der Regel schriftlich erteilt werden. **Hier gilt es insbesondere zu beachten, dass eine einfache E-Mail ohne qualifizierte digitale Signatur das Schriftformgebot juristisch nicht beweisfähig erfüllt!**
- Die Einwilligung muss freiwillig, d.h. ohne physischen und psychischen Zwang, erteilt werden.
- Die Einwilligung kann durch den Betroffenen grundsätzlich jederzeit und formlos zurückgenommen werden.
- Wird die Einwilligung innerhalb eines Vertragswerkes eingeholt, muss die entsprechende Klausel drucktechnisch hervorgehoben (z.B. fett gedruckt) werden.
- Bei der Verwendung elektronischer Medien kann die Einwilligung auch auf elektronischem Wege eingeholt werden.
- Kommt es zu einem späteren Zeitpunkt zu einem Streit über das Vorliegen einer Einwilligung oder deren Wirksamkeit, liegt die Beweislast bei der verantwortlichen Stelle.

Rechtsgeschäftliche Zweckbestimmung

Den im Bereich der privaten Wirtschaft wohl wichtigsten Erlaubnistatbestand stellen Verträge dar. Geregelt ist dies in § 28 Abs. 1 Nr. 1 BDSG. Demnach ist es zulässig, personenbezogene Daten Dritter für eigene Geschäftszwecke zu erheben, zu verarbeiten oder zu nutzen, **sofern dies für die Begründung, Durchführung oder Beendigung des Rechtsverhältnisses erforderlich ist**. Es dürfen nur die im Einzelfall erforderlichen Angaben verwendet werden. Das Vertragsverhältnis muss gegenüber dem Betroffenen bestehen; dieser ist also entweder selbst Vertragspartner oder zumindest Begünstigter. Neben dem eigentlichen Vertragsverhältnis ist ausdrücklich auch das vorvertragliche Vertrauensverhältnis, also das Stadium der Vertragsanbahnung mit erfasst, selbst wenn im Ergebnis kein Vertrag zustande kommt. Einer separaten Zustimmung des Betroffenen bedarf es nicht.

Unerheblich ist, um welche Art von Vertragsverhältnis es sich handelt. Dies kann z.B. ein Kaufvertrag, ein Dienstleistungsvertrag oder ein individuelles Vertragsverhältnis sein. Somit stellt § 28 Abs. 1 Nr. 1 BDSG den wohl bedeutsamsten Erlaubnistatbestand für die Reisebranche dar, denn hier werden personenbezogene Kundendaten regelmäßig für die Anbahnung oder Durchführung von Vertragsverhältnissen genutzt. Wichtig ist, dass die betreffenden Daten für das Vertragsverhältnis tatsächlich erforderlich sind; bloße Dienlichkeit genügt seit der Reform des BDSG vom September 2009 nicht mehr! Wichtig ist ferner, dass das die Datenverarbeitung legitimierende Vertragsverhältnis mit dem Betroffenen selbst, bzw. ggf. mit dessen gesetzlichen Vertretern, besteht. Ein Vertrag mit Dritten genügt nicht.

§ 28 Abs. 1 Nr. 1 BDSG ist nicht auf Beschäftigungsverhältnisse und die damit im Zusammenhang stehenden personenbezogenen Daten anwendbar. Hier gilt die Sonderregelung des § 32 Abs. 1 S. 1 BDSG, welche allerdings insoweit inhaltsgleich mit § 28 Abs. 1 Nr. 1 BDSG ist.

Interessenabwägung

Außerhalb der vertraglichen Zweckbestimmung kann es zulässig sein, personenbezogene Daten Dritter zu erheben, zu verarbeiten oder zu nutzen, wenn es für die berechtigten Interessen der verantwortlichen Stelle erforderlich ist und keine schutzwürdigen Interessen des Betroffenen überwiegen, § 28 Abs. 1 Nr. 2 BDSG. Die stets erforderliche Interessenabwägung muss stets einzelfallbezogen vorgenommen und dokumentiert werden. Die Beweislast für eine ordnungsgemäße Interessenabwägung liegt bei der verantwortlichen Stelle.

Öffentlichkeit der Daten

Wenn Daten allgemein zugänglich sind, dürfen sie von der verantwortlichen Stelle ohne weitere Einschränkungen verarbeitet werden, § 28 Abs. 1 Nr. 3 BDSG. Entscheidend ist dabei nicht die Quelle der Daten oder die Form ihrer Speicherung, sondern die Tatsache, dass jedermann darauf zugreifen kann. Somit sind auch Angaben erfasst, welche aus Internetpräsenzen gewonnen wurden, sofern diese sich nicht in geschlossenen Bereichen befinden.

Weitere Erlaubnistatbestände

Neben den hier genannten Erlaubnistatbeständen kennt das Datenschutzrecht noch mehrere weitere Berechtigungsnormen für die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten Dritter durch Unternehmen der privaten Wirtschaft. Erwähnenswert sind in diesem Zusammenhang die personifizierte Werbung, Scoring-Verfahren oder die Tätigkeit von Auskunfteien.

2.4 Grundsatz der Datenvermeidung und Datensparsamkeit

Auch wenn es nach den vorgenannten Kriterien gestattet ist, personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen, ist dies dennoch nicht gänzlich ohne Einschränkungen zulässig. Vielmehr findet der Grundsatz der Datenvermeidung und der Datensparsamkeit (§ 3a BDSG) Anwendung. **Dem zufolge ist es nur gestattet, diejenigen Daten zu verwenden, welche für die Erreichung des (legitimen) Zwecks unbedingt benötigt werden. Es ist hingegen nicht zulässig, darüber hinausgehende Angaben zu erfassen oder sie zu verwenden.** Die eingesetzten Datenverarbeitungsanlagen müssen so beschaffen und administriert sein, dass es jederzeit möglich ist, nicht mehr benötigte Daten ohne großen Aufwand und ohne den Verlust oder die Veränderung anderer Datensätze zu löschen.

Die Datenverarbeitung muss immer auch verhältnismäßig sein. Dies bedeutet, sie muss geeignet, erforderlich und angemessen sein, um das legitime Ziel zu erreichen.

3. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN ZUM DATENSCHUTZ

§ 9 BDSG trifft die Aussage, dass personenbezogene Daten sowohl in technischer, als auch in organisatorischer Sicht zu schützen sind. Man unterscheidet dabei zwischen Datenschutz und Datensicherheit. Im Grundsatz lassen Datenschutz und Datensicherheit problemlos voneinander trennen. Datenschutz ist der Schutz vor unbefugter Weitergabe und vor unbefugter Kenntnisnahme personenbezogener Inhalte. Datensicherheit hingegen ist die Verlustfreiheit, somit die jederzeitige und vollständige Verfügbarkeit des Datenmaterials. Redundanz, Schutz vor Einbruch, Feuer und Wasser sind also ebenfalls Faktoren, welche das Datenschutzmanagement berücksichtigen sollte.

§ 9 BDSG benennt kein konkretes Schutzniveau, das zu gewährleisten ist. Vielmehr gilt es, das erforderliche Schutzniveau im konkreten Einzelfall zunächst zu definieren, s.o. Hierbei wird zumeist eine Abwägung erfolgen müssen zwischen den Schutzzielen des Gesetzes (Wahrung der Persönlichkeitsrechte von Betroffenen) einerseits und den betriebswirtschaftlichen Zwängen und Fakten andererseits. Letztere dürfen allerdings niemals als alleiniges Kriterium herangezogen werden, da sie die Perspektive der Betroffenen völlig außer Acht lassen. Zur Bestimmung des Erforderlichen Schutzniveaus haben sich in der Praxis drei Prüfpunkte bewährt, auch wenn diese im Gesetzestext nicht ausdrücklich benannt sind:

- Sensitivität der zur Verarbeitung gelangenden Daten (§ 3 Abs. 9 BDSG),
- Schadenspotential aus der Sicht der Betroffenen (auch immaterielle Schäden),
- Schadenseintrittswahrscheinlichkeit.

Zu beachten ist, dass auch die Übermittlung personenbezogener Daten in die Prüfung einbezogen werden muss. Insbesondere die Übermittlung per nicht verschlüsselter E-Mail stellt keine hinreichend geschützte Übertragungsform dar.

3.1 Auftragsdatenverarbeitung

Der Begriff der „Auftragsdatenverarbeitung“ ist dem datenschutzrechtlichen Laien wahrscheinlich nicht näher bekannt. Dennoch ist Auftragsdatenverarbeitung im heutigen Wirtschaftsleben allgegenwärtig. Die datenschutzrechtliche Problematik ist aber erheblich.
Eine Auftragsdatenverarbeitung (§ 11 BDSG) liegt dann vor, wenn ein Dritter personenbezogene Daten ohne eigenes Interesse für den Auftraggeber verarbeitet, also dann, wenn Verarbeitungsvorgänge ausgelagert und an Dritte übertragen werden. Z.B. ist ein Fall der Auftragsdatenverarbeitung gegeben, wenn ein Unternehmen seine Lohn- und Gehaltsrechnung nicht selbst vornimmt, sondern von einem Steuerberater durchführen lässt. Auch Vermittlung von Dienstleistungen, z.B. in der Reisebranche, können unter bestimmten Voraussetzungen Auftragsdatenverarbeitungen darstellen, sofern personenbezogene Kundendaten übertragen werden.

Die Auftragsdatenverarbeitung bedarf nicht der Zustimmung der Betroffenen; diese müssen noch nicht einmal hierüber informiert werden. **Allerdings verbleibt die datenschutzrechtliche Verantwortlichkeit beim Auftraggeber**, auch wenn sich beim Auftragnehmer eine Datenpanne ereignen sollte. Im Ergebnis hat somit der Auftraggeber Verarbeitungsprozesse aus der Hand gegeben, bleibt aber dem Betroffenen gegenüber rechtlich voll verantwortlich. Hieraus ergeben sich nicht nur Haftungsrisiken, sondern auch eine Vielzahl von Pflichten, welche den Auftraggeber einer Auftragsdatenverarbeitung treffen. Der Katalog des § 11 Abs. 2 BDSG zählt diese Pflichten auf. Entsprechende Klauseln müssen zwingend in die Verträge mit der Auftragsdatenverarbeitung aufgenommen werden. Eine nicht den Vorschriften des § 11 Abs. 2 BDSG entsprechende Vertragsgestaltung kann eine Ordnungswidrigkeit darstellen und mit einem Bußgeld geahndet werden.

Auftragsdatenverarbeitungen können nicht nur in Deutschland, sondern im gesamten Bereich der Europäischen Union erfolgen, nicht allerdings darüber hinaus. Bei Verarbeitungen außerhalb der EU handelt es sich um Übermittlungen an Dritte, welche in der Regel der Zustimmung der Betroffenen bedürfen.

3.2 Funktionsübertragung

Von der Auftragsdatenverarbeitung abzugrenzen ist die sogenannte „Funktionsübertragung“. Auch hier werden Daten zur weiteren Verarbeitung oder Nutzung an einen Dritten übermittelt, doch arbeitet dieser nicht strikt weisungsgebunden, (auch) im Eigeninteresse oder der Sitz des Empfängers befindet sich außerhalb der Europäischen Union. In diesen Fällen handelt es sich um eine Übermittlung personenbezogener Daten an Dritte. Dies bedeutet:

- die datenschutzrechtliche Verantwortlichkeit für die sichere Verarbeitung der Daten liegt beim Empfänger,
- die Vorschriften über die Vertragsgestaltung (§ 11 Abs. 2 BDSG) finden keine Anwendung,
- es bedarf der ausdrücklichen Zustimmung des Betroffenen oder einer zwingenden Notwendigkeit für die Durchführung eines mit dem Betroffenen bestehenden Vertragsverhältnisses, um die Übermittlung zu rechtfertigen.

3.3 Der betriebliche Datenschutzbeauftragte

Die wohl wichtigste Figur des Datenschutzmanagements ist zumeist der betriebliche Datenschutzbeauftragte des Unternehmens. Ihm kommen weitgehende Rechte und Pflichten zu.

3.3.1 Wann wird ein betrieblicher Datenschutzbeauftragter benötigt?

Jedes Unternehmen der privaten Wirtschaft ist verpflichtet, einen betrieblichen Datenschutzbeauftragten (bDSB) zu bestellen, wenn **regelmäßig mehr als neun Personen** mit der automatisierten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt werden. Gleiches gilt, wenn ein Unternehmen mehr als zwanzig Personen mit der nicht automatisierten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten betraut, was in der Praxis jedoch recht selten sein dürfte. Aber auch kleine Unterneh-

men, die auf die Bestellung eines bDSB verzichten können, sind nicht von der Aufrechterhaltung eines wirksamen und den gesetzlichen Anforderungen genügenden Datenschutzmanagements befreit. Hier ist vielmehr die Geschäftsleitung in der Verantwortung.

3.3.2 Interner oder externer betrieblicher Datenschutzbeauftragter?

Wer dazu verpflichtet ist, einen bDSB zu bestellen, steht vor der Qual der Wahl. Zwei alternative Möglichkeiten bieten sich an: der interne und der externe betriebliche Datenschutzbeauftragte. Beide Ansätze sind im Ergebnis – der Erfüllung der gesetzlichen Verpflichtungen – gleich gestellt, verfügen aber dennoch über ihre spezifischen Vor- und Nachteile. Diese sollten sorgfältig gegeneinander abgewogen werden. Welcher Weg der bessere ist, lässt sich pauschal nicht sagen. Dies richtet sich ausschließlich nach den unternehmensindividuellen Strukturen.

Interner betrieblicher Datenschutzbeauftragter

Die Bestellung eines internen betrieblichen Datenschutzbeauftragten, also einer Mitarbeiterin/eines Mitarbeiters des eigenen Unternehmens, ist die in der Praxis am häufigsten gewählte Lösung. Zumeist wird der Datenschutz zusätzlich zum bisherigen Aufgabebereich zu bewältigen sein, was oftmals zu zeitlichen Engpässen oder verzögerter Umsetzung führt. Zu beachten ist, dass die auserkorene Person sachlich und persönlich geeignet sein muss, diese Aufgabe wahrzunehmen. Dies bedeutet zunächst, dass sie über die erforderliche Sachkunde verfügen muss, um die Querschnittsaufgabe aus den Bereichen Rechtswissenschaft, Informatik und Betriebswirtschaftslehre bewältigen zu können. Da diese umfassende Fachkunde in aller Regel nicht vollständig vorhanden sein wird, bedarf es einer Ausbildung, welcher bei Bedarf Fortbildungen folgen können und müssen. Hinzu kommt, dass ein betrieblicher Datenschutzbeauftragter auch persönlich geeignet sein muss. Ein interner betrieblicher Datenschutzbeauftragter darf sich nicht in Führungspositionen besonders kontrollrelevanter Bereiche befinden, um das Auftreten von Kontrollkonflikten weitgehend ausschließen zu können. **So dürfen Mitglieder der Geschäftsleitung sowie Leiter von Personal- und EDV-Abteilungen nach allgemeiner Ansicht NICHT zum internen betrieblichen Datenschutzbeauftragten bestellt werden.** Als sehr problematisch wird auch die Inhaberschaft einer Führungsposition im Bereich Controlling betrachtet.

Aus wirtschaftlicher Sicht kann die interne Bestellung kostengünstiger sein, als die Beauftragung eines externen Dienstleisters. Diesem Kostenvorteil stehen folgende Nachteile gegenüber:

- Benachteiligungsverbot – ein interner bDSB genießt ein Benachteiligungsverbot, das einen Kündigungsschutz enthält, wie er in ähnlicher Form auch für Mitglieder des Betriebsrates gilt.
- Verlust einer qualifizierten Fachkraft – die Arbeitszeit, welche ein interner bDSB für den Datenschutz aufwenden muss, steht für dessen eigentliche Tätigkeit im Unternehmen nicht zur Verfügung. Der Zeitfaktor sollte gerade in den ersten Monaten nach der Bestellung nicht unterschätzt werden.
- Der Ausbildung können bzw. müssen Fortbildungen folgen. Der interne bDSB hat einen Rechtsanspruch hierauf.
- Im Schadensfalle verbleibt die Haftung für Schadensfälle beim Unternehmen.

Externer betrieblicher Datenschutzbeauftragter

Eine Alternative zur Bestellung des internen bDSB ist die Bestellung einer externen Fachkraft. Diese wird in vielen Fällen kostenseitig zunächst den höheren Aufwand mit sich bringen. Auch benötigt der externe bDSB in aller Regel auch einen oder mehrere Ansprechpartner im Unternehmen, welche ihm als Außenstehenden Vorgänge und Abläufe des Unternehmens transparent machen kann.

Andererseits stehen diesen Nachteilen einige gewichtige Vorteile gegenüber:

- Leichte Kündbarkeit durch Befristung von Verträgen bzw. Kündigungsfristen,

- hohe fachliche Kompetenz auf aktuellem rechtlichen und technischem Stand,
- oftmals höhere Akzeptanz als eigene Kollegen,
- Haftungsübernahme, im günstigsten Falle durch eine spezielle Haftpflichtversicherung des externen bDSB.

3.3.3 Aufgaben des betrieblichen Datenschutzbeauftragten

Ob interne oder externe Lösung – die eigentlichen Aufgaben des betrieblichen Datenschutzbeauftragten sind die gleichen.

Zunächst einmal ist der bDSB berechtigt und verpflichtet, überall dort im Unternehmen, wo personenbezogene Daten erhoben, verarbeitet oder genutzt werden, Überprüfungen vorzunehmen. Diese Überprüfungen haben das Ziel, festzustellen, ob alle gesetzlichen Anforderungen erfüllt sind oder noch diesbezüglicher Handlungsbedarf besteht. Sollte ein solcher vorhanden sein, muss der bDSB Vorschläge zur Problemlösung einbringen. Allerdings ist er nicht befugt, Verfügungen für das Unternehmen zu treffen, so dass seine Stellungnahmen, welche gegenüber der Geschäftsleitung erfolgen müssen, stets nur empfehlenden, nicht aber verpflichtenden Charakter haben.

Eine Ausnahme von der Kontrollbefugnis bildet der Betriebsrat. Dieser kann dem bDSB die Zustimmung zur Kontrolle seiner Räumlichkeiten, Anlagen sowie der für die Betriebsratstätigkeit genutzten Speichermedien verweigern. Probleme können dann entstehen, wenn die Datenschutzkontrolle den Bereich einer Berufsgeheimnisträgerschaft tangiert (z.B. den betriebsärztlichen Dienst).

3.3.4 Die Aufsichtsbehörden

Der betriebliche Datenschutz unterliegt aber nicht nur der Kontrolle durch den betrieblichen Datenschutzbeauftragten. Vielmehr überwachen staatliche Aufsichtsbehörden, welche auf Landesebene angesiedelt sind, die Umsetzung des Datenschutzes in Unternehmen. Hierzu sind diese mit entsprechenden Kontrollbefugnissen ausgestattet. Geforderte Auskünfte müssen erteilt werden, sofern kein Zeugnisverweigerungsrecht besteht. Zur Durchsetzung ihrer Rechte, aber auch zum Zwecke der Sanktionierung von Verstößen, sind die Behörden in bestimmten Fällen berechtigt, Ordnungswidrigkeiten mit Bußgeldern zu ahnden. Hierzu enthält das BDSG in seinem § 43 eine Aufzählung von Tatbeständen, bei deren Erfüllung eine Ordnungswidrigkeit vorliegt. So müssen z.B. Unternehmen, welche entgegen einer entsprechenden Pflicht keinen bDSB wirksam bestellt haben, mit einem Bußgeld rechnen. Gleiches ist bei der nicht gesetzeskonformen Gestaltung einer Auftragsdatenverarbeitung der Fall oder dann, wenn im Rahmen personifizierter Werbung die Betroffenen nicht über ihr Widerspruchsrecht informiert werden. Die Höhe eines Bußgeldes kann im Extremfall bis zu 300.000,00 EUR betragen; die durch den Datenschutzverstoß erzielten Gewinne können darüber hinaus abgeschöpft werden.

3.4 Meldepflicht

In einigen Fällen, nämlich dann, wenn besondere Arten von personenbezogenen Daten im Sinne des § 3 Abs. 9 BDSG, personenbezogene Daten, welche einem Berufsgeheimnis unterliegen, personenbezogene Daten, die sich auf Straftaten oder Ordnungswidrigkeiten, bzw. entsprechende Verdachtsmomente beziehen oder personenbezogene Daten zu Bank- oder Kreditkartenkonten unbefugten bekannt werden, kann das die Daten speichernde Unternehmen verpflichtet sein, die Betroffenen und die zuständige Aufsichtsbehörde über die Datenpanne zu informieren, § 42 BDSG. Sollte sich der Kreis der Betroffenen nicht eingrenzen lassen oder derartig umfangreich sein, dass eine individuelle Benachrichtigung nicht in Betracht kommt, kann statt dessen die Information auch an die Öffentlichkeit gerichtet werden. Dies muss durch eine mindestens halbseitige Annonce in zwei überregional erscheinenden Tageszeitungen erfolgen.

3.5 Datenübermittlung ins Ausland

Das Datenschutzrecht der Bundesrepublik Deutschland leitet sich, ebenso wie die entsprechenden Bestimmungen in den anderen Mitgliedsstaaten der Europäischen Union, von der Europäischen Richtlinie zum Datenschutz aus dem Jahre 1995 ab. Daraus folgt, dass innerhalb der EU und sogar des EWR ein vergleichbares und hohes Datenschutzniveau vorhanden ist. Aufgrund dieser Tatsache wiederum ist die Übermittlung personenbezogener Daten an Empfänger, welche ihren Sitz in einem Mitgliedsstaat der EU bzw. des EWR haben, datenschutzrechtlich als eine Inlandsübertragung zu bewerten.

Anderes gilt hingegen, wenn personenbezogene Daten an Empfänger außerhalb des EWR übertragen werden sollen, was in der Reisebranche in der Regel unerlässlich ist. Hier dürfen personenbezogene Daten Dritter nur übermittelt werden, wenn dies für die Erfüllung vertraglicher Pflichten gegenüber dem Betroffenen erforderlich ist, das ausdrückliche Einverständnis des Betroffenen vorliegt, oder wenn seitens der empfangenden Stelle ein EU-adäquates Schutzniveau gewährleistet werden kann. Hierfür stehen verschiedene Optionen zur Verfügung:

- das Land, in welchem das die Daten empfangene Unternehmen ansässig ist, wird auf der so genannten „Positivliste“ der Europäischen Kommission geführt,
- zwischen dem übermittelnden und dem empfangenden Unternehmen besteht eine vertragliche Regelung unter Verwendung der Standard-Vertragsklauseln der Europäischen Kommission,
- das die Daten empfangene Unternehmen ist Mitglied des „Safe Harbor“ Abkommens (nur bei Unternehmen mit Sitz in den USA),
- es kann auf sonstige Art und Weise, z.B. aufgrund der durch das empfangende Unternehmen verwendete Private Policies ein hinreichendes Schutzniveau gewährleistet werden.

3.6 Rechte der Betroffenen

Betroffenen räumt das BDSG eine Reihe von Rechten ein. So muss ihnen von der verantwortlichen Stelle Auskunft über die Art der zu ihrer Person gespeicherten Daten, deren Herkunft sowie über die Identität der verantwortlichen Stelle erteilt werden. Ferner hat jedermann das Recht, Einblick in den öffentlichen Teil der Verfahrensverzeichnisse zu verlangen. Dieser muss kostenfrei gewährt werden.

Verfahrensverzeichnisse

Unternehmen der privaten Wirtschaft sind verpflichtet, Verfahrensverzeichnisse zu führen. Diese sollen die Verarbeitungsprozesse personenbezogener Daten transparent machen und nicht zuletzt den Betroffenen dazu dienen, zu erkennen, zu welchem Zweck das Unternehmen personenbezogene Daten erhebt, verarbeitet oder nutzt.

Die Verfahrensverzeichnisse sind von der verantwortlichen Stelle und somit dem Unternehmen zu erstellen, dem betrieblichen Datenschutzbeauftragten zu übergeben und durch diesen zu führen. Ist ein betrieblicher Datenschutzbeauftragter nicht vorhanden, sind die Verfahren der Aufsichtsbehörde zu melden. Jedermann hat ein Recht auf Einsichtnahme in den öffentlichen Teil des Verzeichnisses.

Das Verfahrensverzeichnis besteht aus insgesamt neun Punkten, zu welchen verpflichtend Stellung genommen werden muss:

1. Name oder Firma der verantwortlichen Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,

6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung von Daten,
8. eine geplante Übermittlung in Drittstaaten,
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 BDSG (technische und organisatorische Maßnahmen) zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

Während die Punkte 1 bis 8 öffentlich sind und auf Antrag jedermann Einsicht in diesen Teil des Verzeichnisses erhalten muss, handelt es sich beim neunten Punkt um einen nicht öffentlichen Eintrag.

In der Praxis ergeben sich zahlreiche Schwierigkeiten bei der Erstellung der Verfahrensverzeichnisse. Hinzu kommt, dass das Einsichtnahmerecht für Jedermann häufig die Befürchtung birgt, dass Unternehmensinterna nach außen dringen könnten. Aus diesen Gründen sind viele Verfahrensverzeichnisse sehr kurz und knapp gehalten; sie orientieren eng am Unternehmenszweck, z.B. der „Vornahme kaufmännischer Geschäfte".

Derartige Verzeichnisse erfüllen die durch den Gesetzgeber aufgestellten Anforderungen zumeist nicht. Vielmehr erlauben sie dem Betroffenen keinen Rückschluss darauf, welche seiner Daten zu welchem konkreten Zweck verarbeitet werden sollen.

4. FAZIT

Auch wenn dieser kurze Abriss nur einen Überblick über die im Bereich der privaten Wirtschaft im Zusammenhang mit dem betrieblichen Datenschutz und dessen Umsetzung auftretenden Problemfelder geben konnte, lässt sich doch erkennen, dass eine Lösung sich zumeist nicht leicht und nicht mit geringem personellen und materiellen Aufwand erreichen lässt.

Problemlösungen lassen sich aber auch in aller Regel nicht „von der Stange kaufen". Vielmehr gilt es, in jedem Einzelfall unternehmensindividuell zunächst einen Status der datenschutzrechtlichen und -technischen Situation möglichst objektiv zu fertigen, Schwachpunkte festzustellen und Lösungswege aufzuzeigen. Deren Umsetzung obliegt dann nicht mehr dem betrieblichen Datenschutzbeauftragten, sondern der Geschäftsleitung. Allerdings treffen den Datenschutzbeauftragten umfassende Dokumentationspflichten.

Nicht außer Acht bleiben sollten auch die Haftungsrisiken. Hierunter fallen nicht nur die oben bereits erwähnten Bußgelder, die bei Ordnungswidrigkeiten verhängt werden können. Vielmehr sollten auch etwaige Schadensersatzansprüche Betroffener und mittelbare Schäden durch Vertrauensverluste im Falle des Auftretens von Datenskandalen keinesfalls unberücksichtigt bleiben.

5. HÄUFIG GESTELLTE FRAGEN ZUM DATENSCHUTZ IN DER REISEBRANCHE

Unterliegen alle Daten dem gesetzlichen Datenschutz?

Nein, nur personenbezogene Daten sind gesetzlich geschützt. Diese fallen aber nicht nur im Kundensegment, sondern auch im Personalwesen und darüber hinaus ggf. bei der Kundenakquise oder gegenüber Geschäftspartnern an. Daten juristischer Personen sind ebenfalls nicht erfasst.

Benötige ich immer die Einwilligung des Betroffenen, wenn dessen Daten erhoben, verarbeitet oder genutzt werden sollen?

Nein, die Einwilligung ist entbehrlich, wenn es sich um öffentliche Daten handelt, eine gesetzliche Verpflichtung zur Weitergabe/Speicherung besteht oder wenn die Angaben zur Anbahnung, Durchführung oder Abwicklung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen (zumeist Vertrag) erforderlich sind.

Welche Formvorschriften gelten für Einwilligungserklärungen?

Die Einwilligung muss in der Regel schriftlich erfolgen. Mündliche Erklärungen genügen damit ebenso wenig diesen Anforderungen, wie Einwilligungen, die per eMail erteilt wurden. Nur in wenigen Ausnahmefällen kann vom Schriftformgebot abgewichen werden, namentlich im Massengeschäftsverkehr und bei der Nutzung elektronischer Medien.
Kann sich das Unternehmen auf eine vertragliche Zweckbestimmung berufen, vgl. oben, bedarf es nicht zwingend einer schriftlichen Erklärung des Betroffenen. Hier können sich im Streitfalle aber Probleme im Hinblick auf die Beweisführung ergeben.

Was muss ich bei der Speicherung personenbezogener Daten beachten?

Es dürfen zunächst nur diejenigen Daten gespeichert werden, welche im Einzelfall für die Verfolgung legitimer und vorab definierter Zwecke erforderlich sind. Alle erfassten Daten müssen mit einer Aufbewahrungsfrist versehen sein. Diese richtet sich entweder nach den betrieblichen Belangen oder nach gesetzlichen Vorgaben. Nach Ablauf dieser Frist sind die Daten zu löschen.

Ferner muss die Aufbewahrung sicher sein, d.h., es muss ein hinreichender Schutz gegen missbräuchliche Nutzung eingerichtet werden. Dieser kann z.B. durch eine Festplattenverschlüsselung, aber auch durch andere adäquate Maßnahmen hergestellt werden. Weiterhin muss die jederzeitige Verfügbarkeit von personenbezogenem Datenmaterial gewährleistet werden. Somit ist nach dem Stand der Technik eine redundante Speicherung erforderlich, welche auch etwaige Schäden durch Brand- und Löschwassereinwirkung berücksichtigen sollte.

Was ist bei der Löschung personenbezogener Daten zu beachten?

Die Löschung muss so erfolgen, dass die Wiederherstellung der Datenträger nach dem jeweiligen Stand der Technik weitestgehend ausgeschlossen werden kann. Dies bedeutet, dass ein einfaches Verschieben von Dateien in den virtuellen Papierkorb und selbst dessen Leerung nicht genügt. Vielmehr müssen professionelle Programme zur Datenlöschung angewandt werden. Auch Papierunterlagen sind zu berücksichtigen. Diese müssen im Kreuz- bzw. Partikelschnitt geschreddert werden. Längststreifenschnitt genügt nicht. Werden Unternehmen mit der Datenträger- bzw. Aktenvernichtung beauftragt, stellt auch dies eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG dar. Besondere Probleme ergeben sich derzeit im Bezug auf die Löschung von Festplatten aus Fotokopier-Geräten und Druckern, wenn diese nach Ende der Nutzungsdauer abgegeben werden sollen.

Gelten Besonderheiten, wenn andere Dienstleister zur Leistungserbringung gegenüber dem Kunden eingeschaltet werden?

Immer dann, wenn personenbezogene Daten des Kunden an einen Fremddienstleister übermittelt werden, gilt es, bestimmte Regen zu beachten. Hierfür ist zunächst zu differenzieren, ob es sich um eine Auftragsdatenverarbeitung oder eine Datenübermittlung handelt.

Bei der Auftragsdatenverarbeitung verbleibt die datenschutzrechtliche Verantwortlichkeit beim Auftraggeber. Im Gegenzug bedarf es keiner Einwilligung des Betroffenen in die Weitergabe der Daten. Dieser muss noch nicht einmal hierüber in Kenntnis gesetzt werden. Eine Auftragsdatenverarbeitung ist nur möglich, wenn der Auftragnehmer seinen Sitz in einem Mitgliedsstaat des EWR hat. Bei der Auftragsdatenverarbeitung handelt der Auftragnehmer immer strikt weisungsgebunden und ohne Eigeninteresse an den Daten.

Für die Funktionsübertragung gelten die oben genannten Voraussetzungen nicht. Die Funktionsübertrag stellt immer eine Übermittlung personenbezogener Daten an Dritte dar, welcher der Einwilligung des Betroffenen oder einer zwingenden vertraglichen oder gesetzlichen Rechtsgrundlage bedarf. Werden besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) übermittelt, muss der Betroffene hierüber informiert werden.

Gelten Besonderheiten für die Personaldatenverarbeitung?

Im Grundsatz sind Beschäftigtendaten personenbezogene Daten im Sinne des BDSG, so dass dieses auch hier zur Anwendung kommt. Zu beachten ist jedoch, dass § 28 Abs. 1 Nr. 1 BDSG nicht für die Anbahnung, Durchführung oder Beendigung von Beschäftigungsverhältnissen zur Anwendung kommt. Hier gilt § 32 BDSG. Dieser schreibt vor, dass nur diejenigen Daten durch den (potentiellen) Arbeitgeber erfasst werden dürfen, die für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich sind. Der Begriff des „Beschäftigten" ist in § 3 Abs. 11 BDSG definiert und umfasst einen wesentlich größeren Personenkreis als nur Arbeitnehmerinnen und Arbeitnehmer.

Besonderheiten gelten auch für die Überwachung von Beschäftigten am Arbeitsplatz. Insbesondere die heimliche Überwachung ist nur in sehr engen Grenzen gestattet. Auch hier finden sich die einschlägigen Regelungen im § 32 BDSG.

Ferner kommen im Bereich der Beschäftigungsverhältnisse besonders viele spezialgesetzliche Regelungen zur Anwendung, z.B. das Betriebsverfassungsgesetz, das Mutterschutzgesetz, das Arbeitszeitgesetz, das der neunte Band des Sozialgesetzbuches bei der Beschäftigung von Schwerbehinderten, das Kündigungsschutzgesetz, etc. Diese ergänzen oder verdrängen das allgemeine BDSG.

Benötige ich einen betrieblichen Datenschutzbeauftragten?

Die Bestellung eines betrieblichen Datenschutzbeauftragten ist zwingend immer dann vorgeschrieben, wenn regelmäßig mehr als neun Personen mit der automatisierten, bzw. mehr als zwanzig Personen mit der nicht automatisierten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt werden.

Darf ich ein CRM nutzen und wo sind die Grenzen?

So genannte Customer Relationship Management Tools erfreuen sich beim Vertrieb großer Beliebtheit. Hier können Daten zu Kontaktpartnern gespeichert werden, welche später die Kontaktaufnahme oder die Gesprächsführung erleichtern. Insbesondere dann aber, wenn hier personenbezogene Angaben erfasst werden, welche über die reinen geschäftlichen Kontaktdaten hinaus gehen, also Angaben zu persönlichen Verhältnissen, Hobbys, Familienangehörigen (auch von Reiseteilnehmern) o.ä. ist dies datenschutzrechtlich unzulässig, sofern keine ausdrückliche und formgerechte Einwilligung hierzu besteht.

In welcher Form darf ich personifizierte Werbung betreiben?

An dieser Stelle befinden sich die gesetzlichen Regelungen derzeit in einem Reformprozess. Unkritisch ist personifizierte Werbung zumeist dann, wenn es

sich um eigene Kunden des werbenden Unternehmens handelt und die Daten aus dem eigenen Bestand stammen. Gleiches gilt für Interessenten. Eine Profilbildung, z.B. über Reisegewohnheiten, sollte allerdings unterbleiben.

Kritischer zu betrachten ist die Nutzung von Fremddaten, vor allem solcher Angaben, die über Adresshändler bezogen werden. Seit dem 01. September 2009 dürfen diese nur noch dann Verwendung finden, wenn der Betroffene dem ausdrücklich zugestimmt hat („Opt-In"). Das bloße Unterlassen eines Widerspruchs („Opt-Out") genügt hingegen nicht mehr. Daten, die bis zum Ablauf des 31. August 2009 nach den bis dahin geltenden Vorschriften erhoben wurden, dürfen jedoch noch bis zum 31. August 2012 verwendet werden, sofern keine Änderungen hieran vorgenommen werden.

6. BESONDERHEITEN DES DATENSCHUTZES BEI JUGENDREISEN

Wie in allen anderen Rechtsgebieten auch, gelten bei Jugendreisen grundsätzlich dieselben gesetzlichen Regelungen, die allgemein und bei anderen Reisearten Anwendung finden. In der Praxis ergeben sich jedoch Sonderfälle, die einer gesonderten Betrachtung bedürfen.

Bitte beachten: Alle folgenden Ausführungen sind gewissenhafte Interpretationen geltender gesetzlicher Bestimmungen und deren Anwendung. Durch das Fehlen einer höchstrichterlichen Rechtsprechung im Einzelfall sind diese Interpretationen **nicht** als juristisch gesicherte Tatsachen zu betrachten und geben lediglich eine Orientierung, wie praktische Organisation von Jugendreisen und gesetzeskonformes Verhalten in Übereinstimmung gebracht werden können.

Zur Erinnerung: Es dürfen Daten ohne besondere Zustimmung erhoben werden, die zur Erfüllung des Vertragsverhältnisses notwendig sind. Das dies im Bereich Jugendreisen weit mehr Daten sind, als bei einem „normalen" Pauschalreisevertrag, soll beispielhaft in folgendem Szenario verdeutlicht werden:

Der kleine Fritz, 10 Jahre, wird von seinen Eltern zu einer Kinderreise angemeldet. Über die üblichen Personendaten hinaus erhält der Veranstalter folgende Informationen, die für eine erfolgreiche Abwicklung des Reisevertrages (qualifizierte Betreuung!) notwendig sind:

1. *Fritz ist Bettnässer.*
2. *Fritz hat eine Allergie gegen Kuhmilchprodukte (Laktoseintoleranz).*
3. *Fritz ist Nichtschwimmer.*
4. *Die Eltern von Fritz haben unterschiedliche Adressen.*
5. *Die Mutter verbringt zeitgleich ihren Urlaub im Bayerischen Wald.*
6. *Der Vater ist während der Reise des Kindes zu Hause erreichbar.*
7. *Fritz isst aus religiösen Gründen kein Schweinefleisch.*
8. *Fritz hat während der Reise Geburtstag.*

Zu 1.:
Die Information, dass Fritz Bettnässer ist, gehört zweifellos zu den „sensitiven Daten". Sie ist sinnvoll und erforderlich, um zu gewährleisten, dass Betreuer auf auftretende Probleme vorbereitet sind. Fraglich ist allerdings, ob **allen** Betreuern diese Information zugänglich sein muss. Grundsätzlich kann diese Frage eher verneint werden. Allerdings können bestimmte Arbeitsweisen (Team) die Verbreitung der Information angemessen erscheinen lassen. Bei einer arbeitsteiligen Organisation im Büro des Veranstalters ist allerdings nicht einzusehen, warum z.B. die Buchhaltung Zugriff auf diese Informationen haben sollte, da sie zur Abrechnung der Reise unnötig sind. Nach Ende der Reise, spätestens einen Monat nach Reiseende (wegen möglicher Mängelanzeige des Kunden), ist diese Information endgültig und gründlich zu löschen, da sie keine Relevanz für mögliche spätere oder fortdauerende Geschäftsbeziehungen besitzt (es handelt sich hier um keine dauerhafte „Eigenschaft"). Eventuelle schriftliche Unterlagen, sind vorschriftsmäßig zu beseitigen.

Zu 2.:
Auch hier handelt es sich um Gesundheitsdaten und somit um verstärkt schutzbedürftige Angaben gemäß § 3 Abs. 9 BDSG. Da es bei der Verpflegung von Fritz zu ernsthaften gesundheitlichen Bedrohungen kommen kann, sind die Daten zu speichern und auch allen Betreuenden zur Verfügung zu stellen. Ebenso kann die Speicherung der Daten nach Abschluss der Reise gerechtfertigt sein, z.B. um auch bei einem möglichen Nachtreffen darauf zu achten und bei einer eventuell folgenden Reise sensibilisiert zu sein, um den aktuellen Stand abzufragen. Diese Daten sind dann zu beseitigen, wenn ein erneuter Kontakt zu Fritz unwahrscheinlich ist.

Zu 3.:
Auch hier ist es im Sinne des Kunden, die Daten zu erheben, zu speichern und dem Betreuungspersonal zugänglich zu machen, damit hier mit besonderer Sorgfalt auf die Sicherheit geachtet werden kann. Allerdings - und das gehört zur Aufsichtspflicht und nicht zum Datenschutz – müssen Betreuer sich ohnehin vor dem Schwimmen gehen von den Schwimmfähigkeiten jedes einzelnen Kindes überzeugen. Die Angaben der Eltern sind hier KEINE ausreichend zuverlässigen Quellen. Wie in Punkt 1. sind diese Daten nach Abschluss der Reise endgültig zu beseitigen.

Zu 4. – 6.:
Grundsätzlich sind nur die Daten des vertragsschließenden Elternteils zur Vertragserfüllung unbedingt nötig. Zur Absicherung bei einem eventuell auftretenden Notfall ist es sicher auch ohne besondere Einverständniserklärung zulässig, die Adressdaten des anderen Elternteils und eventuelle Urlaubsadressen vorübergehend zu speichern. Achtung: Im Zweifelsfall hat sich der Veranstalter, besonders bei getrennt lebenden Eltern, darüber zu vergewissern, welchem Elternteil das Sorgerecht zusteht. Nur dieser Elternteil ist formal berechtigt eine Reiseanmeldung vorzunehmen (Aufenthaltsbestimmungsrecht), das Kind nach der Reise in Empfang zu nehmen oder auch während der Reise eventuell notwendige Entscheidungen zu treffen. Ggf. kann eine Übertragung an das andere Elternteil durch Vollmacht erfolgen.
Grundsätzlich dürfen von diesen Daten nur diejenigen gespeichert bleiben, die z.B. im Rahmen von fiskalischen Aufbewahrungspflichten oder anderen gesetzlichen Regelungen vorgeschrieben sind. Dazu gehört sicher NICHT eine Urlaubsadresse der Eltern. Ein eklatanter Verstoß gegen das Datenschutzgesetz wäre es, Eltern aufgrund der Kenntnis ihres Urlaubsortes in der Zukunft diesbezügliche Werbung zuzusenden. Es sei denn, man hat hierzu ausdrücklich und schriftlich das Einverständnis eingeholt.

Zu 7.:
Hierbei handelt es sich wiederum um ein sensitives Datum (Religionszugehörigkeit). Dessen Speicherung ist erforderlich, um den an die Religionsausübung gekoppelten Bedürfnissen gerecht zu werden. Für andere Zwecke dürfen diese Angaben nicht verwendet werden; nach Abschluss der Reise sind sie unverzüglich zu löschen. Der Kreis der zu informierenden Personen sollte möglichst klein gehalten werden.

Zu 8.:
Die Speicherung eines in den Reisezeitraum fallenden Geburtstages ist zur Durchführung der Reise nicht zwingend erforderlich. Es kann jedoch durchaus

im Interesse des Kindes liegen, einen solchen Termin nicht einfach in Unwissenheit zu übergehen. Hier ist eine Interessenabwägung mit den möglicherweise tangierten Schutzinteressen des Betroffenen erforderlich. Da solche nicht erkennbar sind, wäre eine Speicherung zulässig. Nach Abschluss der Reise müssen die Daten, sofern nicht eine ausdrückliche Zustimmung der Erziehungsberechtigten vorliegt, unverzüglich gelöscht werden. Das spätere Übersenden von Glückwunschkarten, ggf. gekoppelt mit Werbeinformationen, wäre hingegen rechtswidrig.

7. 10 WICHTIGE FRAGEN ZUM DATENSCHUTZCHECK

1. **Welche Daten benötige ich zur Vertragserfüllung?**
2. **Welche Daten möchte ich zusätzlich erheben?**
3. **Wie hole ich das Einverständnis hierzu ein?**
4. **Wie speichere ich die Daten so, dass ich problemlos kurzfristig zu löschende von aufzubewahrenden Daten trennen kann?**
5. **Wer darf/muss Zugang zu den Daten haben?**
6. **Wie gewährleiste ich Datensicherheit gegenüber Unbefugten?**
7. **Wie gewährleiste ich, dass zu löschende Daten zum richtigen Zeitpunkt nachhaltig beseitigt werden?**
8. **Wie kann ich in ZULÄSSIGEM Rahmen Kundendaten zu Werbezwecken nutzen?**
9. **Wie installiere ich in meinem Unternehmen zuverlässige und regelmäßige Kontrollen zum rechtmäßigen Umgang mit Kundendaten?**
10. **Benötige ich einen Datenschutzbeauftragten?**

Reisenetz
Deutscher Fachverband für Jugendreisen

Das **Reisenetz** bildet **Vertrauen.**

Seit über 20 Jahren ist das Reisenetz der Deutsche Fachverband für Jugendreisen. Unser Wunsch nach Integration von Pädagogik und Touristik ist in Erfüllung gegangen:

Bei uns arbeiten kommerzielle und gemeinnützige Organisationen aus dem In- und Ausland partnerschaftlich zusammen. Das Reisenetz ist damit das aktivste und größte Netzwerk im Bereich Jugendreisen in Deutschland und trägt mit seiner heterogenen Mitgliederstruktur umfassend zur Professionalisierung des Jugendreisens bei. Partnerschaft ist dabei unser Schlüssel zur Professionalisierung des Jugendreisens.

Vertrauen ist die Basis für unser gemeinsames professionelles Wirken – nach innen und außen.

Für die **Professionalisierung** des **Jugendreisens.**

Wir sehen es als unsere Aufgabe, als Deutscher Fachverband für Jugendreisen die Professionalisierung des Jugendreisens voranzutreiben und dabei die Wertigkeit unserer Mitglieder insgesamt zu stärken und zu festigen.
Deshalb blicken wir gemeinsam praxisnah über den Tellerrand hinaus und profitieren partnerschaftlich voneinander:

- Hilfestellungen des Verbandes bei Gründung, Entwicklung, Sicherung bzw. die weitere Mitglieder-Qualifizierung durch regelmäßig stattfindende offene Fachtagungen, Seminare, Workshops oder Arbeitshilfen
- professioneller, produktübergreifender und kollegialer Erfahrungsaustausch
- vielfältige B2B-Möglichkeiten durch unsere heterogene Mitgliederstruktur
- zusätzliche Verkaufsargumente und Synergie-Effekte durch mitgliederorientiertes kooperatives Reisenetz-Marketing

Unsere Mitglieder sind gleichzeitig verlässliche Partner für Eltern und Lehrer. Denn mit der besonderen Situation der Reise sorgen sie sicher für die Erlebnisse und Begegnungen, die Kinder und Jugendliche für ihre weitere Persönlichkeitsentwicklung benötigen.

Reisenetz
Deutscher Fachverband für Jugendreisen

Mit **Leidenschaft** zur **Qualität**.

Als Deutscher Fachverband für Jugendreisen betreibt das Reisenetz seit Jahren eine nachhaltige Qualitätsentwicklung. Mit der Vergabe des Gütesiegels „Geprüfte Reisenetz Qualität" bietet der Verband die erste integrierte Zertifizierungsmöglichkeit im Bereich Jugendreisen an. Derzeit gibt es das Siegel für die Bereiche „Jugendunterkünfte", „Schulfahrten und Jugendgruppenreisen", „Betreute Jugendreisen" sowie „Programmanbieter".

Weitere Informationen finden Sie auf unserer Homepage www.reisenetz.org.

Wenn Sie sich für unsere Angebote oder für eine Mitgliedschaft interessieren, stehen wir Ihnen jederzeit gern zur Verfügung:

Reisenetz e.V. – Deutscher Fachverband für Jugendreisen
Köpenicker Straße 126 | 10179 Berlin | Germany
Fon +49 (0)30.24 62 84 30 | Fax +49 (0)30.24 62 84 90
info@reisenetz.org | www.reisenetz.org

IMPRESSUM

Herausgeber: Reisenetz e.V.
Köpenicker Straße 126 | 10179 Berlin

Text: Frank Jander, Ludwig Ottenbreit, Sandra Türk
Redaktion: Ludwig Ottenbreit, Sandra Türk
Layout: www.tegler-mediendesign.de

Stand: März 2011

Die Erstellung dieses Leitfadens wurde gefördert durch das Bundesministerium für Familie, Senioren, Frauen und Jugend.