Der Landesbeauftragte
für den Datenschutz und die
Informationsfreiheit Rheinland-Pfalz

Orientierungshilfe „Datenschutz im Hotelgewerbe“

Persönliche Daten von Hotelgästen fallen regelmäßig bei jedem Hotelaufenthalt an, Diskretion gehört daher zum Standard im Hotelgewerbe. Viele Hotelgastdaten sind zudem besonders persönlich und sensibel, denn der Kontakt zwischen Gast und Hotel ist naturgemäß eng. Das Hotel kennt die Essgewohnheiten und –vorlieben des Gastes, erfährt von seinen Freizeitinteressen, reinigt täglich sein Bad und richtet sein Bett. Häufig hat das Hotel sogar Kenntnis vom Gesundheitszustand des Gastes, von Krankheiten, Allergien oder Diäten. Das Hotel weiß, welche Fernsehprogramme der Gast bevorzugt, welche Besucher er empfängt, welche Zahlungsmittel er einsetzt und welches nächste Reiseziel er ansteuert. Deshalb ist der Schutz der Gastdaten nach dem Datenschutzgesetz absolut notwendig und die Enttäuschung der Gäste bei Fehlern besonders gut nachvollziehbar.

Damit einher geht die hohe Verantwortung des Hoteliers. Kaum ein Gewerbetreibender bekommt einen so umfassenden Einblick in die Persönlichkeit des Kunden. Während andere Dienstleister und Kaufleute immer nur Ausschnitte aus der Lebenswirklichkeit des Kunden erhalten – und viel Geld für data mining ausgeben müssen, um zusätzliche Informationen über Persönlichkeit des Kunden zu erlangen – erhält der Hotelier Einblick in das gesamte Lebensumfeld des Gastes.

Dies verpflichtet ihn in besonderer Weise, das informationelle Selbstbestimmungsrecht seines Gastes zu wahren.

Diese Orientierungshilfe zum Datenschutz im Hotelgewerbe soll einerseits den Hoteliers eine Handreichung für den Umgang mit persönlichen Daten der Gäste, Mitarbeiter und Geschäftspartner geben, andererseits auch die Hotelgäste über Datenschutzfragen informieren und Tipps für kommende Hotelaufenthalte geben.

(Stand: April 2013)

I. Rechtsgrundlagen

Die wesentlichen rechtlichen Grundlagen für den Datenschutz in Hotels finden sich im **Bundesdatenschutzgesetz** (BDSG), daneben können auch Vorschriften des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG) einschlägig sein.

Das BDSG regelt, welche **persönlichen Angaben** zu Gästen, Mitarbeitern und Geschäftspartnern zu schützen sind (personenbezogene Daten, § 3 Abs. 1 BDSG) und wer hierfür **verantwortlich** ist (verantwortliche Stelle, § 3 Abs. 7 BDSG). Verantwortlich ist danach die **Geschäftsleitung** des Hotels. Handelt es sich um eine Hotelkette, deren einzelne Häuser als selbstständige juristische Personen geführt werden, so ist die örtliche Geschäftsleitung verantwortlich, bei unselbständigen Niederlassungen die Leitung des Hauptsitzes.

Im Datenschutzrecht gilt ein **Verbot mit Erlaubnisvorbehalt** (§ 4 Abs. 1 BDSG): Die Erhebung, Verarbeitung oder Nutzung der persönlichen Daten seiner Gäste ist dem Hotelier daher nur gestattet, wenn der Hotelgast hierin ausdrücklich **eingewilligt** hat oder eine **Rechtsvorschrift** den Hotelbetrieb ausdrücklich hierzu verpflichtet (etwa das Meldegesetz) oder berechtigt (etwa § 28 BDSG).

Eine solche **Einwilligung** muss **freiwillig** sein und auf der Grundlage **vollständiger Information** über den Zweck der Datenerhebung und –nutzung erfolgen. Sie ist grundsätzlich **schriftlich** einzuholen. Erteilte Einwilligungen können jederzeit mit Wirkung für die Zukunft widerrufen werden. In der Praxis hat es sich bewährt, dem Hotelgast für die Ausübung des Widerrufs einer Einwilligung einen festen Ansprechpartner bzw. feste Kontaktdaten zu nennen.

Das BDSG sieht eine Reihe von **Pflichten des Hoteliers** vor. So hat er seine Beschäftigten zu einem sorgsamen Umgang mit personenbezogenen Daten anzuhalten (§ 5 BDSG: **Verpflichtung auf das Datengeheimnis**) und bei der Einschaltung von Dienstleistern deren Umgang mit den geschützten Daten zu kontrollieren (§ 11 BDSG: **Auftragsdatenverarbeitung**). Darüber hinaus hat er einen angemessenen technischen Standard der Datensicherheit zu gewährleisten (§ 9 BDSG: **Technische und organisatorische Maßnahmen**) und den **Grundsatz der Datensparsamkeit** zu beachten (§ 3a BDSG).

Von besonderer Bedeutung sind diese drei Pflichten: Der Hotelier muss dem Betroffenen auf Verlangen Auskunft zu allen über ihn gespeicherten Daten geben (§ 34 BDSG: **Auskunftsrecht**); er muss ab einer Zahl von 10 Mitarbeitern, die personenbezogene Daten verarbeiten, einen betrieblichen Datenschutzbeauftragten bestellen (§ 4f BDSG: **Beauftragter für den Datenschutz**) und er muss für den Fall, dass ihm persönliche Daten abhanden kommen, hierüber die Aufsichtsbehörde und alle Betroffenen unterrichten (§ 42a BDSG: **Informationspflicht bei Datenpannen**).

Zuständige Aufsichtsbehörde ist der **Landesbeauftragte für den Datenschutz** (§ 38 BDSG); er unterstützt die Hotelleitung bei der Erfüllung ihrer Pflichten, kontrolliert sie aber auch und kann bei Pflichtverletzungen Strafen aussprechen.

Was ist ein betrieblicher Datenschutzbeauftragter (bDSB)
Der bDSB unterstützt die Hotelleitung bei der Erfüllung der oben genannten Aufgaben. Zum bDSB kann nur bestellt werden, wer die für diese Aufgaben erforderliche **Fachkunde**, regelmäßig nachgewiesen durch ein Zertifikat, und die nötige **Zuverlässigkeit** besitzt. Dies bedeutet, dass er bei seiner Arbeit nicht in einen Interessenkonflikt mit seinen anderen Tätigkeiten (z.B. als Leiter der EDV oder als Familienangehöriger des Geschäftsführers) kommen darf.

Zum bDSB kann ein Mitarbeiter des Betriebs (**interner bDSB**) oder ein entsprechend qualifizierter Dienstleister (**externer bDSB**) bestellt werden. Der bDSB ist der Geschäftsleitung unmittelbar unterstellt und in Bezug auf Datenschutzfragen weisungsfrei, also unabhängig tätig. Die Geschäftsleitung ist verpflichtet, die permanente Aus- und Weiterbildung des bDSB zu gewährleisten, entsprechende Arbeitsmittel und Arbeitszeit zur Erfüllung seiner Aufgaben bereit zu stellen. Wird ein interner bDSB bestellt, so genießt er einen besonderen gesetzlichen Kündigungsschutz.

Die gesetzlichen Regelungen zum bDSB und seinen Aufgaben finden sich in den §§ 4f und 4g BDSG.

II. Die wichtigsten Problemfelder

1. Umgang mit Meldedaten

Zu Beginn des Hotelaufenthalts ist der Hotelier verpflichtet, die Meldedaten des Gastes abzufragen (§ 16 Abs. 1 Satz 1 MRRG iVm § 26 Meldegesetz (MG) Rheinland-Pfalz vom 22. Dezember 1982).

Danach hat die beherbergte Person bei ihrer Ankunft einen besonderen Meldeschein auszufüllen und zu unterschreiben. Mangels gesetzlicher Regelung zu einer elektronischen Unterschrift hat diese handschriftlich auf Papier zu erfolgen. Wer als Ehegattin, Ehegatte, Lebenspartnerin oder Lebenspartner mitreist, kann auf den Meldeschein mit aufgenommen werden. Minderjährige Kinder in Begleitung eines Elternteils sind nur der Zahl nach anzugeben. Beherbergte ausländische Gäste haben sich bei der Anmeldung den Leiterinnen und Leitern der Beherbergungsstätten oder ihren Beauftragten gegenüber durch die Vorlage eines gültigen Identitätsdokuments auszuweisen.

Nach § 27 MG muss der Meldeschein Angaben enthalten über

1. den Tag der Ankunft und den der voraussichtlichen Abreise,
2. den Familiennamen,
3. den gebräuchlichen Vornamen (Rufnamen),
4. den Tag der Geburt,
5. die Anschrift,
6. die Staatsangehörigkeiten oder das Herkunftsland.

Der Meldeschein ist für ein Jahr aufzubewahren; vor unbefugter Einsichtnahme zu sichern und nach Ablauf der Aufbewahrungsdauer zu vernichten.

Hieraus ergibt sich für den Hotelier:

- Er hat keine Prüfpflicht bzgl. der Angaben des Gastes; solange der Gast nicht angibt, Ausländer zu sein, kann die Vorlage eines Ausweises nicht verlangt werden.

- Es existiert keine Rechtsgrundlage für das **Kopieren von Ausweisen**. Dies verstößt gegen das Gebot der Datensparsamkeit (§ 3a BDSG) und stellt ggf. eine Ordnungswidrigkeit dar.

- Es gibt keine namentliche Meldepflicht für Ehegatten, Lebenspartner und Kinder

- Nach § 4 Abs. 3 BDSG besteht eine Hinweispflicht auf die Zweckbestimmung und auf die gesetzliche Grundlage der Erhebung der Meldedaten (hier: Meldegesetz).

Weiter gilt:

- Die Nutzung der Meldedaten für Vertragszwecke ist unproblematisch, der Hotelier kann also Angaben aus dem Meldeschein in die Hotelrechung übernehmen.

aber:
- Die Erhebung **weiterer Daten** beim Check-In erfolgt dann nicht mehr auf Grundlage des Meldegesetzes!

Dies gilt für die Frage nach:
- eMail-Adresse
- Festnetz-Nummer / Mobiltelefon-Nummer / Fax-Nummer
- Ausweis-Nummer / Ausstellungsdatum / Ausstellungsort
- Geburtsdatum Ehegatte / Kinder
- Geschlecht
- Firma
- Nächstes Reiseziel
- Vielfliegerprogramm
- Hobby / Freizeitbeschäftigungen
- Angabe Zahlungsmodalitäten

Grundlage dieser Datenerhebungen ist ausschließlich die **freiwillige Einwilligung** des Gastes (§ 4a BDSG). Diese setzt voraus:

- den **Hinweis auf Freiwilligkeit und Zweck** der Datenerhebung (§ 4 Abs. 3 Satz 2 BDSG)

- die **besondere Hervorhebung** / drucktechnisch **eindeutige Trennung von Pflichtangaben und freiwilligen Angaben** auf dem Meldeformular (vgl. § 4a Abs. 1 Satz 4 BDSG)

- die **Trennbarkeit von Pflichtangaben und freiwilligen Angaben** auf dem Meldeformular, etwa durch die Einfügung einer Perforation, um bei Einsichtnahme der Meldebehörde in den Meldeschein eine überschießende Information der Meldebehörde auszuschließen

- eine Möglichkeit, dass die nach dem Meldegesetz zu leistende Unterschrift und die Unterschrift im Rahmen der Einwilligung in weitere Datenerhebungen und –nutzungen auf jeweils **separaten Unterschriftenfeldern** geleistet werden. Ansonsten entfällt die Freiwilligkeit der Einwilligung.

2. Der Einsatz von Kreditkarten

Regelmäßig werden Hotelgäste beim Check-In aufgefordert, ihre Kreditkarte an der Rezeption „zum Zwecke der Erfassung“ vorzulegen.

Mit dieser Erhebung von personenbezogenen Daten werden verschiedene Ziele verfolgt. Zum einen wird die Kreditkarte erfasst, um im Falle einer Abreise des Gastes ohne (vollständige) Zahlung offene Forderungen befriedigen zu können. Die Erfassung der Kreditkarte dient also **Kautionszwecken**.
In anderen Fällen wird die Kreditkarte mit einem Minimalbetrag (z.B. 1 Cent) belastet, um zu prüfen, ob der Hotelgast Kredit genießt, hier geht es also um eine **Bonitätsprüfung**.

Unter datenschutzrechtlichen Aspekten ist hierbei zu beachten:

- Der Gast ist in jedem Falle über den **Zweck der Erfassung** der Kreditkarte **aufzuklären** (§ 4 Abs. 3 Satz 1 BDSG).

- Der Gast ist über die **Freiwilligkeit** der Erfassung der Kreditkarte **aufzuklären** (§ 4 Abs. 3 Satz 2).

- Der Gast ist über die **Folgen einer Verweigerung** von Angaben **aufzuklären** (§ 4 Abs. 3 Satz 3 BDSG); also über die andernfalls bestehende Notwendigkeit einer Barkaution bzw. Vorkasse.

Hiernach erforderliche Informationen sind dem Hotelgast in der Regel an der Rezeption zu geben; bewährt haben sich hier Hinweise in Gestalt von Aufstellern. Auf Wunsch sind diese Informationen dem Gast schriftlich zu überlassen.

Rechtswidrig wäre es, nur von Kreditkarteninhabern eine Kautionsleistung zu verlangen.

Hinweis: Die Belastung der Kreditkarte ohne Unterschrift des Kreditkarteninhabers widerspricht häufig den Nutzungsbedingungen des Kreditkarteninstituts.

3. Die Anfertigung von Kundenprofilen

Während seines Hotelaufenthalts wird der Hotelgast für den Hotelier nahezu zwangsläufig zum „gläsernen Kunden“. Der Hotelier erhält eine Vielzahl, häufig besonders sensibler Daten, etwa über Ess- und Trinkgewohnheiten, Begleitpersonen, Besucher, Gesundheitszustände, Behinderungen, sexuelle Orientierung, Freizeitverhalten usw. Hier ist äußerste Diskretion und Zurückhaltung beim Umgang mit diesen personenbezogenen Daten geboten, sonst drohen Vertrauensverlust beim Kunden und Reputationsschäden in der Öffentlichkeit (vgl. dazu die „Auszeichnung“ internationaler Hotelketten mit dem Big Brother Award 2007).

Aus datenschutzrechtlicher Sicht ist hierbei zu beachten:

- Zulässig ist die Erhebung und Speicherung aller Daten, die für die **Leistungserbringung und –abrechnung** im Rahmen des Beherbergungsvertrags benötigt werden (etwa: Konsum im Restaurant, Minibar, Pay-TV, Wellness-Leistungen). Grundlage für die Datenverarbeitung ist in diesem Falle § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Diese Daten dürfen auch für eigene Werbezwecke des Hotels genutzt werden (§ 28 Abs. 3 Satz 2 Nr. 1 BDSG).

- Daten über erbrachte **Leistungen, die nicht abgerechnet werden** – etwa die im Übernachtungspreis inbegriffene Nutzung des Pools, die kostenlose Abgabe einer Tageszeitung oder die kostenfreie Gewährung eines Internetzugangs – dürfen auf dieser Rechtsgrundlage nicht erfasst werden, denn dies wäre für die Durchführung des Beherbergungsvertrages nicht erforderlich. Hier kann nur die ausdrückliche, auf Basis einer klaren Zweckerklärung erfolgte Einwilligung des Hotelgastes eine Datenverarbeitung rechtfertigen.

- Die Nutzung eines so erstellten **Kundenprofils** für eigene Zwecke – etwa mit Blick auf zukünftige Aufenthalte – bedarf ebenfalls einer ausdrücklichen und informierten **Einwilligungserklärung** des Gastes. Bezieht sich die Erklärung auf **besonders schutzwürdige personenbezogene Daten** – also auf Angaben über politische Meinungen, religiöse Überzeugungen, über Gesundheit oder Sexualleben (§ 3 Abs. 9 BDSG) -, so muss sich die Einwilligungserklärung ausdrücklich auch auf diese Daten beziehen (§ 4a Abs. 3 BDSG). Die Einwilligungserklärung kann der Gast jederzeit und ohne Angabe von Gründen einschränken oder mit Wirkung für die Zukunft **widerrufen**. Sobald der Widerruf dem Hotel zugegangen ist, hat jegliche weitere Datennutzung zu unterbleiben; die Daten sind unverzüglich zu löschen bzw. zu sperren.

- Die **Weitergabe von Kundenprofilen an Dritte** – Privatpersonen, andere Gewerbetreibende oder an staatliche Stellen – bedarf jeweils einer einschlägigen (gesetzlich oder individuell erteilten) Ermächtigung (vgl. §§ 28 ff. BDSG), deren Vorliegen der Hotelier als verantwortliche Stelle im Einzelfall gegenüber dem Gast

bzw. gegenüber der Aufsichtsbehörde (§ 38 BDSG) nachweisen muss (vgl. § 4 Abs. 1 BDSG). Auch andere Häuser einer Hotelkette können Dritte sein, wenn sie jeweils rechtlich eigenständig sind, so dass auch in diesem Fall für die Weitergabe eine Ermächtigung erforderlich ist. Dabei sind insbesondere versteckte, in ihrer Bedeutung klar zuzuordnende Einwilligungserklärungen in die Datenweitergabe („im Kleingedruckten"/AGB) unzulässig (vgl. dazu § 4a Abs.1 Satz 4, § 28 Abs. 3a Satz 2 BDSG).

- In Zweifelsfällen wird dem Hotelier dringend angeraten, vor der Weitergabe von Kundendaten beim Gast oder der Datenschutzaufsichtsbehörde **nachzufragen**, ob gegen die Übermittlung Bedenken bestehen.

- In jedem Falle hat der Hotelier zu prüfen, wie lange er personenbezogene Daten seiner Gäste aufbewahrt. Sobald die Datenerhebung ihren Zweck erfüllt hat, sind **alle Daten unverzüglich zu löschen** (§ 35 Abs. 2 BDSG). Dabei sind, je nach Zweckbestimmung der Daten, häufig unterschiedliche Löschfristen zu beachten. Teilweise bestehen aber auch steuerliche und handelsrechtliche **Aufbewahrungspflichten**. In diesem Fall sind die Daten weiter zu speichern, dürfen für andere Zwecke aber nicht mehr genutzt werden (sog. Sperre).

Einen Überblick behält der Hotelier hier nur dann, wenn er schon bei Erhebung der Daten diese unterschiedlichen Kategorien zuordnet und – ggf. automatisierten – **Löschroutinen** unterwirft. Bewährt haben sich hier sog. Lösch- und Sperrkonzepte.

4. CRM (Customer-Relationship-Management)

a) Kundenzufriedenheitsbefragungen

Qualifizierte Kundenbefragungen sind Bestandteil eines effektiven Qualitätsmanagements. Werden sie durch den Hotelier selbst vorgenommen, können sie mit Einwilligung des Gastes, also **auf freiwilliger Basis** unter Hinweis auf die Zwecke der Befragung (§ 4 Abs. 3 Sätze 1 und 2 BDSG), durchgeführt werden.

Vorsicht ist allerdings bei der Art und Weise geboten, **wie der Gast angesprochen** wird. Unproblematisch ist es, wenn die Befragung persönlich erfolgt oder schriftlich im Hotel durchgeführt wird. Auch eine briefliche Kundenbefragung im nahen zeitlichen Zusammenhang mit einem Hotelaufenthalt begegnet keinen Bedenken (vgl. § 28 Abs. 3 Satz 2 Nr. 1 BDSG). Bei **telefonischen oder per E-Mail durchgeführten Zufriedenheitsbefragungen** ist allerdings § 7 Abs. 2 UWG zu beachten (vorherige ausdrückliche Einwilligung!) und es müssen die Vorgaben des TKG (Verbot der Rufnummernunterdrückung § 102 Abs. 2 TKG) beachtet werden; bei Verstößen drohen hohe Bußgelder bis 50.000 € (§ 20 UWG).

Setzt der Hotelier **Dienstleister** (z.B. Call Center / Marktforschungsinstitute) für eine Kundenzufriedenheitsbefragung ein, ist zu klären, ob der Dienstleister streng nach Weisung des Hoteliers handelt (dann liegt eine Auftragsdatenverarbeitung gem. § 11 BDSG vor). Verfährt hingegen der Dienstleister nach eigenen Maßgaben, ist eine Übermittlung der Kundendaten durch den Hotelier an den Dienstleister nur nach vorheriger Abwägung mit den eventuell entgegenstehenden schutzwürdigen Interessen des Gastes, nicht von Dritten auf die Vertragsbeziehung zum Hotelier angesprochen zu werden, zulässig (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG).

b) Kundenbindungsprogramme (insbes. Rabattsysteme)

Teil von CRM sind auch sog. Kundenbindungsprogramme, die sich als Kombination aus Prämien- und Rabattsystem einerseits und vertraglicher Werbeleistung per Newsletter, eMail oder Telefon andererseits darstellen. Dabei wird die Dokumentation des Reise- und Konsumverhaltens des Gastes für ein **zielgruppenspezifisches Marketing** genutzt.

Da im Rahmen solcher Kundenbindungsprogramme regelmäßig aussagekräftige Bewegungs- und Nutzungsprofile des Hotelgastes entstehen und zudem nicht selten die Weiterveräußerung dieses Kundenprofils an weitere Gewerbetreibende vorgesehen ist, kann eine solche Datenverarbeitung **nur auf ausdrücklicher und spezifischer vertraglicher Grundlage** erfolgen. Dabei ist insbesondere zu beachten, dass der Hotelgast sichere Kenntnis der vertraglichen Abreden erhält (dies kann bei der Nutzung von AGB zweifelhaft sein). Außerdem kann der Hotelgast seine Teilnahme an Kundenbindungsprogrammen jederzeit mit Wirkung für die Zukunft **widerrufen** und auf einer **Löschung** bzw. Sperrung seiner Daten bestehen.
Die so entstehenden **Datenbestände** sind in besonderer Weise vor dem **Zugriff Dritter** (Stichwort: Datenklau**) zu schützen** (vgl. unter 6. Datensicherheit).

5. Der Einsatz von Videoüberwachung

Der Einsatz von Videoüberwachungstechnik ist – auch in Hotels – weit verbreitet; dies bedeutet aber keineswegs, dass er immer zulässig ist und rechtmäßig erfolgt.

Für eine rechtmäßige Videoüberwachung ist insbesondere zu beachten:

- Das Betreiben einer Videoüberwachung im öffentlich zugänglichen Raum (Lobby, Flure, Außenanlagen, Tiefgarage etc.), ist nur gestattet (vgl. § 6b BDSG)

  - **zur Wahrung des Hausrechtes** oder
  - **zur Wahrnehmung berechtigter Interessen** für **vorab konkret festgelegte Zwecke**, insbesondere die Sicherheit der Gäste und der Einrichtung des Hotels,

  und keine Anhaltspunkte dafür bestehen, dass **schutzwürdige Interessen der Betroffenen** gegenüber dem Überwachungsinteresse überwiegen (§ 6b BDSG).

  Ein solches Überwiegen von Betroffeneninteressen ist anzunehmen bei einer Überwachung in Ruhe- und Wellnessbereichen, im Restaurant oder in Toilettenräumen. In nicht öffentlich zugänglichen Räumen, also in den Hotelzimmern sowie in allein den Mitarbeitern vorbehaltenen Bereichen kommt eine Videoüberwachung auf der Grundlage von § 6b BDSG ohnehin nicht in Betracht. Auch ist die **Videoüberwachung von Mitarbeitern** zu Zwecken der Verhaltens- oder Leistungskontrolle grundsätzlich **unzulässig**.

- Der Betreiber ist verpflichtet, mit **Hinweisschildern** (vgl. DIN 33450) auf die **Überwachung** und **die überwachende Stelle** (mit Adresse/Telefon-Nummer) hinzuweisen (§ 6b Abs. 2 BDSG); diese Hinweisschilder sind so anzubringen, dass die Betroffenen erkennen können, dass sie sich in einen überwachten Bereich hineinbegeben. Dies gilt auch für Nebeneingänge.

- Sicherheitsinteressen werden am besten durch ein **Monitoring** gewährleistet, das durch eingriffsbereites und geschultes Personal erfolgt. Soll zugleich eine **Aufzeichnung** stattfinden, so ist wegen der größeren Eingriffsintensität von Videoaufzeichnungen eine eigenständige Abwägung mit den widerstreitenden Interessen der Betroffenen vorzunehmen.

- Im Außenbereich installierte Kameras dürfen **nur das Hotelgelände** erfassen und **nicht den öffentlichen Verkehrsraum** überwachen.

- Die **maximale Speicherdauer** beträgt **48 Stunden**. Eine längere Speicherung ist nur im Ausnahmefall bei Vorliegen besonderer, zu dokumentierender Umstände zulässig. Die Daten sind unverzüglich zu löschen, wenn sie für die Erreichung des Zweckes nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegen stehen.

- Die **Weitergabe von Daten an Dritte** darf nur auf Grund von Rechtsvorschriften erfolgen. Das gilt auch gegenüber staatlichen Stellen; hier gilt: eine freundliche Anfrage ersetzt keinen richterlichen Beschlagnahmebeschluss.

- Außerdem ist zu beachten:
  - Mitarbeiter sind über die Videoüberwachung und deren Zwecke zu informieren,
  - existiert ein Betriebsrat, so ist dieser in die Planung und Durchführung der Überwachung einzubeziehen; ggf. ist nach dem BetrVG der Abschluss einer entsprechenden Betriebsvereinbarung geboten.
  - Kameras mit Audio-Funktion sind verboten.
  - Kameraattrappen unterfallen nicht dem BDSG, können jedoch wegen des ausgelösten Überwachungsdrucks das Persönlichkeitsrecht der Hotelgäste verletzen; zudem können sie ein falsches Sicherheitsgefühl vermitteln.
  - Der Einsatz von Webcams, deren Bilder unmittelbar ins Internet übertragen werden und dort abrufbar sind, unterfällt ebenfalls § 6b BDSG. Werden einzelne Personen identifizierbar und im Internet allgemein abrufbar abgebildet, so ist dies regelmäßig unzulässig.

- Vor Inbetriebnahme der Videoüberwachung ist ein **Verfahrensverzeichnis zu erstellen.**

In einem Verfahrensverzeichnis werden benannt:

- wer die Überwachung durchführt
- die genaue Zweckbestimmung der Überwachung
- die betroffenen Personengruppen
- die Art der erhobenen und gespeicherten Daten
- die Art der eingesetzten Datenverarbeitungs-Hardware und -Software
- technisch-organisatorische Maßnahmen (TOM) nach § 9 BDSG die festlegen, unter welchen Voraussetzungen z.B. Kameras installiert und betrieben werden dürfen, wer Zugriff auf die gespeicherten Daten hat, aus welchem Anlass auf die Daten zugegriffen werden darf und welche Daten weitergegeben werden dürfen und an wen. Es ist zu dokumentieren, wer, wann, aus welchem Anlass auf die Daten zugegriffen hat und was er mit den Daten machte, insbesondere an wen er sie weitergegeben hat.

- Dient die Videoüberwachung der Identifizierung von Personen, so ist vor ihrer Einrichtung eine **Vorabkontrolle durch einen betrieblichen Datenschutzbeauftragten** gemäß § 4d Abs. 5 und 6 BDSG vorzunehmen.

6. Datensicherheit (§ 9 BDSG, Anlage)

Der Hotelier verfügt mit den persönlichen Daten von Gästen, Mitarbeitern und Geschäftspartnern über einen „Datenschatz“, den er gut behüten muss. Einerseits vertrauen seine Gäste und Vertragspartner darauf, dass er mit ihren sensiblen Daten sorgsam umgeht, andererseits stellt dieser Datenschatz ein lohnenswertes Ziel für Hacker, Datendiebe und andere Kriminelle dar, die den wirtschaftlichen Wert der Daten abschöpfen wollen.

Zur Gewährleistung der hier angesprochenen Datensicherheit verpflichtet § 9 BDSG den Hotelier, alle „technischen und organisatorischen Maßnahmen zu treffen“, die erforderlich sind, um die rechtmäßige Nutzung der Daten zu gewährleisten.

Dazu muss er

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren (**Zutrittskontrolle**),
2. verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),
3. gewährleisten, dass die zur Nutzung Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (**Zugriffskontrolle**),
4. gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),
5. gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten erfolgt (**Weitergabekontrolle**),
6. gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),
7. gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**) und
8. gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden (**Trennungsprinzip**).

Dabei hat er insbesondere die dem Stand der Technik entsprechenden **Verschlüsselungsverfahren** einzusetzen.

Diese Grundsätze der Datensicherheit gelten nicht nur für die Computer des Hotelbetriebs selbst, sondern auch dann, wenn der Hotelier seinen Hotelgästen die Nutzung von **WLAN** ermöglicht.

Kommt es trotzdem zu Datendiebstahl oder Datenverlusten, so ist der Hotelier verpflichtet, den hiervon Betroffenen, also insbesondere den Hotelgästen, diese „**Datenpanne**“ anzuzeigen und Maßnahmen zu treffen, den hierdurch drohenden Schaden zu begrenzen; eine solche Anzeige ist auch der Datenschutz-Aufsichtsbehörde gegenüber abzugeben (§ 42a BDSG).

III. Tipps für Hotelgäste

Hoteliers, die sich ihrer Pflicht zum Schutz des informationellen Selbstbestimmungsrechts von Kunden und Mitarbeitern bewusst sind, tragen viel zum „gelebten Datenschutz“ bei. Genauso wichtig sind aber aufgeklärte und selbstbewusste Hotelgäste, die um den Wert ihrer Privatsphäre wissen und nicht in jede datenschutzrechtliche Zumutung blindlings einwilligen.

Hierzu die folgenden Tipps:

1. **Datensparsamkeit schützt.**
   Persönliche Daten, die ich dem Hotel nicht offenbare, können auch nicht zu meinem Nachteil verwendet werden. Das gilt auch für die Nutzung „kostenloser“ WLAN.

2. **Fragen hilft.**
   Wenn von mir Angaben verlangt werden, ohne dass gleichzeitig erläutert wird, auf welcher Grundlage gefragt wird und zu welchem Zweck die Daten erhoben werden, dann hilft nur die Nachfrage. Und das Bestehen auf eine Antwort.

3. **Streich mal wieder.**
   Nur weil ein vorgelegtes Formular viele Antwortfelder vorsieht, muss ich es noch lange nicht komplett ausfüllen. Fragen nach persönlichen Angaben, die ich nicht verstehe oder die ich nicht beantworten will, kann ich getrost streichen. Auf zwingend erforderliche Fragen wird der Hotelier mich hinweisen.

4. **Auskunftsrechte nutzen.**
   Das BDSG gibt dem betroffenen Gast umfangreiche Rechte gegenüber dem Hotel. Der Gast darf jederzeit und ohne Angabe von Gründen Auskunft über alle Informationen verlangen, die das Hotel über ihn gesammelt hat. Die Verweigerung der Auskunft kann sogar mit einem Bußgeld bestraft werden.

5. **Alles auf Anfang: Das Widerrufsrecht ausüben.**
   Auch wenn man früher mal eine Einwilligung zur Speicherung persönlicher Daten abgegeben hat, ein einfacher Widerruf lässt ganze Datensammlungen verschwinden. An eine einmal abgegebene Einwilligung ist man für die Zukunft nicht gebunden, ein formloser Widerruf verpflichtet den Hotelier, alle „Datenspuren“ zu beseitigen.

6. **Hilfsangebote nutzen.**
   Wenn man als Gast unsicher ist, wie man sich verhalten soll oder wenn man meint, der Hotelier geht mit den persönlichen Daten nicht korrekt um, dann hilft der Landesdatenschutzbeauftragte gerne weiter. Ein Anruf genügt.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit RLP
Hintere Bleiche 34 *Tel. 06131/208-2449*
55116 Mainz *E-Mail: poststelle@datenschutz.rlp.de*