



ARTIKEL

**Datenschutz und CRM/Marketing sind eng miteinander verbunden. Der Artikel gibt eine Übersicht über die verschiedenen Bereiche und die möglichen Auswirkungen, wenn der Datenschutz von Unternehmen vernachlässigt wird.**

# Gefahr durch den Datenschutz?

*Was Hotels beachten müssen*

von Diplom Betriebswirt Michael Toedt und  
Rechtsanwalt Dr. jur. Robert Selk

September 2007 © Toedt, Dr. Selk & Coll. GmbH  
Dieses Werk ist urheberrechtlich geschützt. Jede Verwertung außerhalb der Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung von TS&C unzulässig und strafbar.





## Artikel

März 2005

# Gefahr durch den Datenschutz?

- Was Hotels beachten müssen -

Von Michael Toedt und Dr. Robert Selk

Untersuchungen haben es bereits mehrfach belegt, der Datenschutz wird von der Deutschen Hotellerie sehr stiefmütterlich behandelt. Dieses Verhalten kann Unternehmen allerdings teuer zustehen kommen, denn auch in diesem Fall gilt der allgemein gültige Grundsatz: **„Unwissenheit schützt vor Strafe nicht“**. Geldbußen bis zu 250.000 € (vgl. § 43 BDSG) können letztlich die Existenz bedrohen. Es gibt also genügend Gründe, sich diesem Thema näher anzunehmen.

Neben den hohen Strafen ist ein weiterer Aspekt besonders wichtig: Einmal unrechtmäßig gespeicherte Daten können im Nachhinein nicht mehr rechtmäßig werden. Was bedeutet das? Hat ein Hotel beispielsweise ein System im Einsatz, in dem Kundendaten unrechtmäßig genutzt werden und dies wird bei einer Kontrolle festgestellt, reicht es nicht die vorhandenen Mängel zu beseitigen. Sofern keine nachträgliche „Legalisierung“ erfolgt, sind diese Daten, in der Regel das wichtigste Kapital der Sales- und Marketingabteilungen, unwiderruflich verloren und dürfen nicht mehr verwendet werden. Dies kann verheerende Folgen für viele CRM- (Customer Relationship Management) und Marketingprogramme haben, da hier besonders stark auf die Sammlung und Analyse von Kundendaten gesetzt wird. Solche Vorhaben kosten selbst bei Einzelhotels schnell fünfstelligen Beträge und bei Hotelketten oft mehrere Millionen Euro. Eine intensive Planung unter Einbeziehung

des Datenschutzes ist aus diesem Grund äußerst ratsam.

## Datenschutz ≠ Datensicherheit

Was allgemein unter „Datenschutz“ verstanden wird, muss in zwei Bereiche unterteilt werden: den Datenschutz im rechtlichen Sinne sowie die vorwiegend technisch zu sehende Datensicherheit. Beides wird von den Datenschutzgesetzen geregelt. Unter „Datenschutz“ versteht dabei das Gesetz allerdings nicht den Schutz der Daten, sondern den Schutz der Personen, über die die erhobenen oder gespeicherten Daten etwas aussagen können. Die einschlägigen Gesetze regeln dabei nicht nur das Datenmanagement in der Beziehung „Hotel – Kunde“, sondern auch die Beziehungen „Hotel – Lieferanten“ bzw. „Hotel – Mitarbeiter“. Bestimmte datenschutzrechtliche Vorgänge innerhalb eines Unternehmens sind laut Gesetz in einer sog. Verfahrensübersicht sowie einem Verzeichnis festzuhalten. Die Verfahrensübersicht kann dabei „jedermann“ zur Einsicht anfordern. Allerdings nur theoretisch, denn bei einer Untersuchung von Studenten der Fachhochschule München konnte keine der Befragten Hotelketten den vorgeschriebenen Informationspflichten nachkommen.



Das erste deutsche Datenschutzgesetz („Bundesdatenschutzgesetz“, BDSG) wurde bereits 1977 verabschiedet. Im Rahmen der Volkszählung entschied 1984 das Bundesverfassungsgericht, das es für jeden Einzelnen ein **„Recht auf informationelle Selbstbestimmung“** gebe. Dies besagt im Grundsatz, dass jeder selbst entscheiden können soll, wer, was, wann über einen selbst wie lange wissen darf.

Das BDSG wurde letztmals im Jahr 2001 überarbeitet und in den letzten Jahren durch eine Vielzahl bereichsspezifischer Gesetze, wie etwa das Teledienstedatenschutzgesetz (TDDSG), welches in Bezug auf das Internet besonders wichtig ist, ergänzt. Schutzbedürftig aus der Sicht der Datenschutzgesetze sind allerdings nur die so genannten **„personenbezogenen Daten“**: Hierbei dreht es sich um Daten, die einen Rückschluss auf eine Person zulassen, beispielsweise Name, Adresse, Telefon. Im Zuge von Service- und Marketingverbesserungen sammeln Hotels heute vermehrt Informationen über Interessen, Vorlieben oder Freizeitaktivitäten, oftmals jedoch ohne Beachtung der gesetzlichen Vorschriften. Weitestgehend verboten, sind dabei die Speicherung von „sensiblen Daten“, wie z. B. Daten zur Gesundheit, rassischer und ethnischer Herkunft, politische, religiöse oder philosophische Überzeugungen oder gar über das Sexualleben.

Grundsätzlich gilt im Datenschutzrecht das sog. **„Verbotsprinzip“**: Zunächst ist jede Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten verboten. Eine Ausnahme gilt nur, wenn entweder der Betroffene vorher eingewilligt hat oder das Gesetz eine Verwendung der Daten explizit erlaubt. Ein Gast muss somit vor der Datenverarbeitung seine Einwilligung geben. Am besten kann dies durch eine gut gestaltete Einwilligungserklärung oder auch eine Ergänzung der Allgemeinen Geschäftsbedingungen erfolgen, wobei dann besondere Voraussetzungen zu erfüllen sind. Eine Anpassung der Gast-Anmeldeformulare sowie der AGB's ist somit sehr empfehlenswert.

Zu beachten ist, dass Hotels gegenüber den Kunden regelmäßig gewisse und zum Teil sehr umfangreiche Informationspflichten erfüllen müssen, wie z. B. ein Hinweis auf die Freiwilligkeit der Angaben und das Widerrufsrecht, etwa zum Abmelden von zukünftigen Postsendungen etc.

Grundsätzlich ist für jede Übermittlung, unabhängig ob national oder international, eine Erlaubnis, entweder in Form einer Einwilligung oder einer gesetzlichen Regelung, erforderlich.

Dies gilt sogar für Übermittlungen innerhalb einer Unternehmensgruppe. Demnach müssen zwischen Mutter- und Tochtergesellschaften gesonderte Verträge geschlossen oder Regelungen gefunden werden, wenn man nicht Gefahr laufen möchte, gegen geltendes Recht zu verstoßen.

Bei **internationalen Geschäftsbeziehungen** gilt zudem, dass Daten nur in „sichere Länder“ übermittelt werden dürfen. Dies betrifft z. B. auch das Reservierungssystem. Da innerhalb der EU der Datenschutz mittlerweile harmonisiert ist, ist eine Übermittlung in diesem Falle deutlich einfacher, es bedarf jedoch auch hier einer Einwilligung oder gesetzlichen Erlaubnis. Ein Datentransfer in Staaten außerhalb der EU ist nur gestattet, wenn besondere Voraussetzungen erfüllt sind, beispielsweise so genannte „Datenschutz-Policies“ oder „codes of conducts“ geschaffen und als unternehmensweit verbindlich erklärt wurden.

Ausnahmen gelten beispielsweise hinsichtlich der Schweiz sowie Unternehmen in den USA, die Teil des so genannten **„Safe Harbor“** - Abkommens sind. Auf der Seite <http://www.export.gov/safeharbor> sind die (wenigen) zertifizierten Unternehmen gelistet, was zur Überprüfung bzw. Vorbereitung von internationalen Verträgen äußerst hilfreich ist. In diesem Zusammenhang ist zu erwähnen, dass selbst große amerikanische Unternehmen diesen gesetzlichen Vorgaben oftmals keine Beachtung schenken. Leidtragender und derjenige der letztlich für dieses Versäumnis haftet ist das Hotel, das Unternehmen in Deutschland.

Unternehmen müssen die Datensicherheit gewährleisten und haben eine **Auskunftspflicht** gegenüber den Kunden. Bei einer Überprüfung von drei führenden deutschen Hotelgruppen, war keine der Gesellschaften in der Lage, der Auskunftspflicht nachzukommen und eine Verfahrensübersicht der im Unternehmen verarbeiteten Daten zu übermitteln. Beides ist gesetzlich ganz klar geregelt und vorgeschrieben.

Für die Kontrolle der Einhaltung der Datenschutzgesetze innerhalb eines Unternehmens ist der **Datenschutzbeauftragte** verantwortlich, den jedes Unternehmen bestellen muss, wenn mehr als vier Personen mit der automatisierten Datenverarbeitung beschäftigt sind. Hat ein Hotel beispielsweise an der Rezeption mehr als vier Mitarbeiter, die Zugang zum Front Office System haben, ist die Bestellung eines Datenschutzbeauftragten zwingend notwendig. Die Stelle eines Datenschutzbeauftragten kann intern an Mitarbeiter oder extern vergeben werden. Wichtig

dabei ist, dass die erforderliche Fachkunde, gerade im komplexen rechtlichen Bereich, gegeben ist.

Besonders für kleine und mittlere Betriebe ist die Bestellung eines externen Datenschutzbeauftragten sinnvoll. Ab einer Unternehmensgröße von ca. 1000 Mitarbeiter dagegen ist – auch hier gibt es Ausnahmen – es in der Regel günstiger, einen fest angestellten Datenschutzbeauftragten einzusetzen.

Der Datenschutzbeauftragte sorgt nicht nur für die Einhaltung des Datenschutzes bezüglich des Marketings, sondern hat umfassende Überwachungsaufgaben, also auch hinsichtlich der eigenen Mitarbeiter, Vertragspartner etc. Zudem gibt es bestimmte Arten der Datenverarbeitungen, die **vor** ihrem Einsatz zwingend vom Datenschutzbeauftragten geprüft werden müssen. Generell sollte aufgrund der Spezialmaterie im Hotelbereich darauf geachtet werden, dass der externe Datenschutzbeauftragte auch mit den Besonderheiten der Hotellerie und des Direktmarketings vertraut ist.

Die **Kosten** der Einschaltung eines externen Datenschutzbeauftragten richten sich vorwiegend danach, wie groß zum einen der Hotelbetrieb ist (Anzahl der Mitarbeiter, Umfang der Werbeaktivitäten, Vorhandensein eines

Betriebsrates, länderübergreifender Datenverkehr etc.) sowie danach, wie viel Wissen bereits im Bereich Datenschutz vorhanden ist. Belässt man den – je nach Einzelfall sehr unterschiedlichen – Aufwand der erstmaligen Prüfung aller notwendigen Unterlagen sowie die Erstellung der gesetzlich vorgeschriebenen Verzeichnisse außer Betracht, betragen die laufenden Kosten eines externen Datenschutzbeauftragten pro Quartal ca. 300 € - 600 €, je nach Aufwand.

In Bezug auf personalisierte Werbung wird nachfolgend kurz auf **Email** und Briefwerbung an private Kunden eingegangen. Emails dürfen im Gegensatz zum klassischen Postweg grundsätzlich nur an Personen verschickt werden, die vorher ausdrücklich zugestimmt haben. Ein entsprechender Vermerk in den AGB's ist in diesem Zusammenhang nicht ausreichend. Ein Formular auf der hoteleigenen Webseite zur Sammlung von Emailadressen muss somit eine klar formulierte Einwilligungserklärung beinhalten, die der Ausfüller selber aktivieren muss. Sogenannte „Check-Boxes“ in Webformularen dürfen also nicht standardmäßig mit einem Haken versehen sein. Darüber hinaus ist als einziges Pflichtfeld die Emailadresse erlaubt, da der Grundsatz der Datensparsamkeit gilt und weitere Angaben lediglich freiwilliger Natur sein dürfen.

The image shows a screenshot of the Althoff Hotels & Residences website. At the top, there is a navigation menu with links: 'Hotels & Residenzen', 'Das Unternehmen', 'Service-Lounge', 'Beauty & Spa', 'Restaurants', and 'Business-Lounge'. The main header features the 'ALTHOFF HOTELS & RESIDENCES' logo. Below the logo, there is a section titled 'Regelmäßig informiert durch den Althoff Newsletter!'. This section contains a registration form with the following fields: 'Anrede' (with a dropdown menu), 'Vorname', 'Nachname', 'E-Mail', 'Firma', 'Straße', 'PLZ', 'Ort', and 'Land' (with a dropdown menu). Below the form, there is a checkbox with the text: 'Ja, ich bin damit einverstanden zukünftig über Neuigkeiten der Althoff Hotels & Residenzen per E-Mail informiert zu werden.' Below the checkbox, it says '\* benötigte Felder'. To the right of the form, there is a preview of the newsletter content, showing various articles and images. At the bottom of the page, there is a footer with links: 'Home', 'Kontakt', 'Impressum', 'Jobs', 'Partner', 'Presse', 'E-Mail', 'Newsletter', and 'Besuchen'.

Abbildung 1: vorbildliches Webformular - gesehen unter [www.althoffhotels.com](http://www.althoffhotels.com)



Bei der klassischen **Briefwerbung** muss der Empfänger den Absender und die verantwortliche Stelle klar erkennen können und die Möglichkeit haben, weitere Werbezusendungen zu verweigern. So ist es beispielsweise ratsam, im Sichtfenster auf der Couvert-Innenseite eine Kontaktstelle anzugeben, an die sich der Empfänger bei Fragen und Wünschen wenden kann.

Um gegen ein Unternehmen vorzugehen, das die gesetzlichen Bestimmungen missachtet und etwa weiterhin unerwünschte Werbung verschickt, kann die Konkurrenz oder eine betroffene Person mit zivilrechtlichen Schritten vorgehen. Als äußerst wirksam hat sich dabei zum Beispiel das **Wettbewerbsrecht** erwiesen. Einer wettbewerbsrechtlichen Abmahnung kann etwa eine einstweilige Verfügung und eine Unterlassungsklage folgen. Zudem sind in der Regel die Anwaltskosten der Gegenseite zu übernehmen.

Die Kunden haben neben dem Auskunftsrecht auch Beseitigungs-, Unterlassungs- und Schadensersatzansprüche. Probleme können aber ebenso direkt von staatlicher Seite kommen. So kann die **Datenschutzaufsichtsbehörde** von selbst aktiv werden. Auch Anzeigen durch verärgerte Kunden oder von Mitbewerbern können zu Kontrollen führen. Neben all den genannten rechtlichen Sanktionen sind auch mögliche **Imageschäden** durch negative Presseberichterstattungen oder durch Veröffentlichungen im Internet nicht zu unterschätzen.

Der „Datenschutz“ ist mittlerweile zu einem komplexen Thema geworden und Unternehmen sind gut beraten, sich dessen anzunehmen. Eine kurze Checkliste bzgl. des Datenschutzes finden Sie im Internet unter [www.ts-und-c.de/datenschutz.htm](http://www.ts-und-c.de/datenschutz.htm).

**Autoren:**



**Michael Toedt -**  
 Managing Director  
 Dipl.-Betriebswirt  
 Michael Toedt ist geschäftsführender Gesellschafter der Toedt, Dr. Selk & Coll. GmbH in München.  
 Das

Beratungsunternehmen ist spezialisiert auf die Bereiche CRM-Technologie, Marketing-Beratung und Datenschutz für Tourismusunternehmen. Neben seiner Tätigkeit bei Toedt, Dr. Selk & Coll. ist er Lehrbeauftragter an der Fachhochschule München zum Thema „CRM im Tourismus“.

Kontakt: [michael.toedt@TS-and-C.com](mailto:michael.toedt@TS-and-C.com)



**Dr. jur. Robert Selk**  
 - Rechtsanwalt, LL.M.

Rechtsanwalt Dr. Robert Selk ist Partner der Kanzlei Dr. Schmid, Dr. Selk & Hoffmann in München. Er promovierte Bereich des Internet- und

Datenschutzrechts und ist u.a. Mitglied der Arbeitsgruppe IT-Recht des deutschen Anwaltvereins, der deutschen Gesellschaft für Recht und Informatik (DGRI), der Gesellschaft für Datenschutz und Datensicherheit (GDD) sowie dem Deutschen Datenschutzverein (DVD). Dr. Robert Selk ist in verschiedenen Unternehmen als externer Datenschutzbeauftragter tätig, Gastdozent an der Universität Augsburg sowie der Akademie für Unternehmensführung der Handwerkskammer Oberbayern.

Kontakt: [robert.selk@TS-and-C.com](mailto:robert.selk@TS-and-C.com)





Toedt, Dr. Selk & Coll. GmbH  
Augustenstr. 79  
80333 München  
Tel.: 0 89/ 18 93 56 9 0  
Fax: 0 89/ 18 93 56 9 19

**Internet:**  
[www.TS-and-C.com](http://www.TS-and-C.com)