



Hotellerie & Datenschutz

Datenschutzmanagement für die Hotellerie

DataSolution Thurmann

Stand 02'2007



Inhaltsverzeichnis

Datenschutz und IT-Sicherheit – Worum geht es?

1.	Bedeutung des Datenschutzes	3
2.	Welche Daten fallen unter das BDSG	4
3.	Rechtliche Grundlagen	6
4.	Prinzipien	8
5.	Datenschutzkontrollen	9
6.	Risiken	9

Datenschutz- und Datensicherheitsaufwendungen

1.	Organisation des Datenschutzes	10
2.	Aufbau und Pflege der Datenschutzorganisation	11
3.	Preisliste	13
4.	Leistungsverzeichnis	15

Datenschutz und IT-Sicherheit – Worum geht es?

Jedes Unternehmen, gleich welcher Rechtsform, muss sich heutzutage um den Datenschutz kümmern. Diese Verpflichtung ergibt sich aus dem Bundesdatenschutzgesetz (BDSG), den Landesdatenschutzgesetzen der Bundesländer, dem Teledienstschutzgesetz (TDDSG) und einer Reihe anderer Regelungen.



Unter Datenschutz wird nicht der Schutz der Daten, wie oft angenommen, verstanden, sondern der Schutz der Personen, über die personenbezogenen Daten erhoben, gespeichert, verarbeitet und genutzt werden. Der Datenschutz wahrt die Persönlichkeitsrechte von Kunden, Mitarbeitern und Lieferanten. Die Ergreifung von geeigneten organisatorischen und technischen Maßnahmen zum Schutz aller Daten im Unternehmen sind die Schwerpunkte der IT-Sicherheit.

Nach § 3 Absatz 1 BDSG sind personenbezogene Daten „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener).“ Der Begriff „Einzelangaben über persönliche oder sachliche Verhältnisse“ ist sehr weit zu verstehen. Persönliche Verhältnisse können Eigenschaften des Betroffenen sein, sachliche Verhältnisse Dinge, die dem Betroffenen zuzuordnen sind.

Beispiel 1 | Neben dem Namen des Gastes und dessen Anschrift erfassen viele Hotels zusätzliche Daten über den Gast, um die Servicequalität zu erhöhen. Zu ihnen gehören unter anderem Eigenschaften, wie Vorlieben, Abneigungen und Gewohnheiten. Aber auch E-Mail-Adressen, Rufnummern, Kfz-Kennzeichen und Firmenzugehörigkeiten, um nur einige zu nennen, gehören zur Sammelleidenschaft von Hoteliers.

„Einzelangaben“ liegen nicht mehr vor, wenn die Informationen nicht mehr auf eine Person zurückzuführen ist. Sie sind anonymisiert.

1. Bedeutung des Datenschutzes

Der Zweck des Datenschutzes besteht darin, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht auf informelle Selbstbestimmung beeinträchtigt wird. Datenschutz steht für die Idee, dass jeder Mensch grundsätzlich selbst entscheiden kann, wem wann welche seiner persönlichen Daten zugänglich sein sollen. Der Datenschutz will den so genannten „Gläsernen Menschen“ verhindern.

Die Bedeutung des Datenschutzes ist seit der Entwicklung der Digitaltechnik stetig gestiegen, weil Datenerfassung, Datenhaltung, Datenweitergabe und Datenanalyse immer einfacher werden. Technische Entwicklungen wie Internet, E-Mail, Videoüberwachung, Mobiltelefon und elektronische Zahlungsmethoden schaffen neue Möglichkeiten zur Datenerfassung.

Beispiel 2 | Beim Surfen im Internet sind viele Verbraucher auf „Access-Provider“ angewiesen, die den Zugriff auf das Internet ermöglichen. Dabei wird dem Computer des Verbrauchers für die Dauer des Zugriffs auf das Internet eine IP-Nummer zugewiesen. Die IP-Nummer ist ein Zahlencode, der zwischen vernetzten Rechnern wie eine postalische Adresse wirkt. Auf diese Art und Weise können Computer miteinander kommunizieren. Gleichzeitig kann eine IP-Nummer auch ein personenbezogenes Datum des Verbrauchers sein, wenn man die Zuweisung der IP-Nummer zu bestimmten Rechnern kennt oder ermitteln kann.

Interesse an personenbezogenen Informationen haben sowohl staatliche Stellen als auch private Unternehmen. Sicherheitsbehörden möchten beispielsweise durch Rasterfahndung und Telekommunikationsüberwachung die Verbrechensbekämpfung verbessern, Finanzbehörden sind an Banktransaktionen interessiert, um Steuerdelikte aufzudecken. Unternehmen versprechen sich von Mitarbeiterüberwachung (Arbeitnehmerdatenschutz) höhere Effizienz, Kundenprofile sollen beim Marketing helfen und Auskunfteien die Zahlungsfähigkeit der Kunden sicherstellen.



Beispiel 3 | Markt- und Meinungsforschungsinstitute sind häufig kommerziell ausgerichtete Unternehmen, die Verbraucherdaten sammeln und auswerten, um sie anderen Unternehmen oder auch Behörden zu verkaufen. Wenn die Angaben über Verbraucher anonym, also ohne Zuordnung zu einer bestimmten Person erhoben werden, liegen zwar statistische Angaben einer Gruppe vor, meistens aber keine personenbezogenen Daten.

Tipp | Spricht Sie ein Markt- oder Meinungsforschungsinstitut an, prüfen Sie sorgfältig, ob Sie Informationen über sich preisgeben wollen! Bei seriösen, Ihnen bekannten Instituten bestehen keine grundsätzlichen datenschutzrechtliche Bedenken. Nachfragen nach der weiteren Verwendung der Daten kann allerdings nicht schaden. Andere Institute erfragen von Ihnen Informationen zumeist nur, um sie als personenbezogene Daten weiterzuverkaufen. Diese Daten werden regelmäßig in vielfältiger Weise ausgewertet. Sie müssen damit rechnen, dass Sie künftig von Vertragspartnern der Institute zu Werbezwecken angesprochen werden.

Dieser Entwicklung steht eine gewisse Gleichgültigkeit großer Teile der Bevölkerung gegenüber, in deren Augen der Datenschutz keine oder nur geringe praktische Bedeutung hat.

Vor allem durch die weltweite Vernetzung, insbesondere durch das Internet, nehmen die Gefahren hinsichtlich des Schutzes personenbezogener Daten laufend zu. Datenschützer müssen sich deshalb zunehmend mit den grundlegenden Fragen des technischen Datenschutzes (IT-Sicherheit) auseinandersetzen, wenn sie Erfolg haben wollen.

2. Welche Daten fallen unter das BDSG

Relevante Verarbeitungsformen von personenbezogenen Daten sind nach dem BDSG die Datenerhebung, die Verarbeitung (Speicherung, Veränderung, Übermittlung, Sperrung, Löschung) und Nutzung. Unter Datenerhebung wird das Beschaffen von personenbezogenen Daten verstanden. Sie ist regelmäßig gegeben, wenn sich die Stellen Informationen aktiv beschaffen.



Beispiel 4 | Viele Hotels haben in ihrem Internetauftritt ein Online-Reservierungssystem integriert. Interessenten können hierüber Zimmer reservieren bzw. buchen. Hierzu geben sie personenbezogene Daten in ein Online-Formular ein, welche abschließend an das Hotel via Internet übermittelt werden.

Der datenschutzrechtliche Begriff Speichern entspricht dem allgemeinen Wortgebrauch. Er ist allerdings nicht auf ein Speichermedium beschränkt. Deshalb spricht das BDSG von „Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger“.

Beispiel 5 | Videoaufnahmen im Hotelbereich sind ebenso ein Speichern wie das Abspeichern von Gastdaten auf einem Computer.

Es ist dabei nicht erforderlich, dass die Speicherung dauerhaft erfolgt.

Verändern ist das „inhaltliche Umgestalten gespeicherter personenbezogener Daten“.

Beispiel 6 | Wenn ein Gast feststellt, dass von ihm falsche personenbezogene Daten gespeichert wurden, kann er vom Hotel deren Berichtigung verlangen.

Das Übermitteln ist das Weitergeben von personenbezogenen Informationen an einen Dritten. Diese Form der Datenverarbeitung ist bedeutsam, weil die Information den ursprünglichen Verwenderkreis verlässt. Damit findet eine Erweiterung des Kreises der Datenverarbeiter statt.

Beispiel 7 | Ein Hotel einer Hotelkette leitet die Daten seiner Gäste an eine zentrale Datenbank, welche das Mutterunternehmen administriert, weiter. Datenschutzrechtlich ist dieser Datentransfer als Datenübermittlung zu werten, der den allgemeinen Regeln zu folgen hat. Das Datenschutzrecht kennt kein Konzernprivileg.

Löschen ist das Unkenntlichmachen von gespeicherten personenbezogenen Daten. Ein Löschen liegt nur vor, wenn die Daten unwiederbringlich getilgt sind.

Beispiel 8 | Wenn Sie die „Löschfunktion“ in einem Textprogramm Ihres Rechners betätigen (delete – entf – o.ä.), beseitigt der Rechner lediglich den Datenzugriff (Zugriffspfad) und ermöglicht damit auch das Überschreiben des ursprünglichen Textes. Mit bestimmten Programmen sind die „gelöschten“ Texte aber wieder herstellbar. Unternehmen, die sensible Daten speichern, dürfen sich daher nicht damit begnügen, die Löschfunktionen zu verwenden.

Sperrungen bedeutet ein „Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken“. Gemeint ist folgendes: Es gibt Situationen, in denen an und für sich eine Löschung von personenbezogenen Daten erforderlich wäre. Andererseits kann es gute Gründe geben, z.B. weil es ein Gesetz verlangt, oder auch das Interesse des Betroffenen dafür spricht, dass die Daten weiterhin gespeichert werden. In diesem Fall bewirkt die Sperrung, dass die Daten zwar gespeichert werden, grundsätzlich aber nicht mehr verwendet werden dürfen.

Beispiel 9 | Eine Hotelkette hat ehemalige Gäste zu Werbezwecken angeschrieben. Ein Gast widerspricht der weiteren Nutzung seiner Daten. Nun kann es passieren, dass die Hotelkette erneut die Adresse des Gastes erhält. Wenn die Hotelkette alle Daten des Gastes gelöscht hat, kann es nicht mehr erkennen, dass er einen Widerspruch erklärt hat und keine Werbezuschriften wünscht. Hier hilft die Sperrung: die Adressdaten werden nur noch aufbewahrt, um zu verhindern, dass der Gast erneut zu Werbezwecken angesprochen wird.

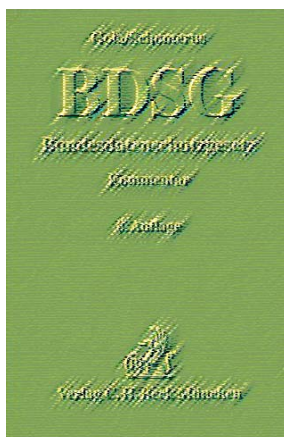
3. Rechtliche Grundlagen

Das erste deutsche Datenschutzgesetz wurde bereits 1977 verabschiedet. Im Rahmen der Volkszählung entschied 1984 das Bundesverfassungsgericht, dass es für jeden Einzelnen ein „Recht auf informelle Selbstbestimmung“ gebe. Das Bundesdatenschutzgesetz (BDSG) wurde im Jahr 2001 überarbeitet und in den letzten Jahren durch eine Vielzahl bereichsspezifischer Gesetze, wie das Teledienstschutzgesetz (TDDSG) ergänzt.

Mit dem "Ersten Gesetzes zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft", das am 26. August 2006 in Kraft getreten ist, erfolgte die letzte Änderung des Bundesdatenschutzgesetzes in vier Paragraphen.

1. Es ändert sich die generelle Pflicht der Ernennung eines Datenschutzbeauftragten (DSB). Diese Pflicht ist nun auf Unternehmen reduziert, die mindestens 10 (zuvor 5) Mitarbeiter mit der datentechnischen Erhebung, Nutzung und Verarbeitung von personenbezogenen Daten beschäftigen.
2. Dementsprechend entfällt auch die Meldepflicht für Unternehmen mit nicht mehr als 9 personenbezogenen Daten verarbeitenden Mitarbeitern.
3. Die erforderliche Fachkunde eines Datenschutzbeauftragten soll in Abhängigkeit vom konkreten Schutzbedarf der jeweils verantwortlichen Stelle bemessen werden.
4. Berufsgeheimnisträger wie Rechtsanwälte, Steuerberater und Ärzte dürfen jetzt ebenfalls einen externen Datenschutzbeauftragten bestellen.

Mit der Europäischen Datenschutzrichtlinie haben das Europäische Parlament und der Europäische Rat Mindeststandards für den Datenschutz der Mitgliedsstaaten festgeschrieben. Die Richtlinie gilt jedoch nicht für den Bereich der justiziellen und polizeilichen Zusammenarbeit, die so genannte Dritte Säule der Union.



In Deutschland wurde die Richtlinie im Jahr 2001 mit dem Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze in nationales Recht umgesetzt. Geregelt wird auch die Übermittlung von personenbezogenen Daten in Drittstaaten, die nicht Mitglied der EU sind: Gemäß Artikel 25 ist die Übermittlung nur dann zulässig, wenn der Drittstaat ein „angemessenes Schutzniveau“ gewährleistet.

Die Entscheidung, welche Länder dieses Schutzniveau gewährleisten, wird von der Kommission getroffen, die dabei von der so genannten Artikel - 29 - Datenschutzgruppe beraten wird. Aktuell wird gemäß Entscheidung der Kommission von folgenden Drittstaaten ein angemessenes Schutzniveau gewährleistet: Schweiz, Kanada, Argentinien, Guernsey, Isle of Man, sowie bei der Anwendung der vom US-Handelsministerium vorgelegten Grundsätze des „Safe Harbor“.

4. Prinzipien

Hauptprinzipien des Datenschutzes sind:

- Datenvermeidung und Datensparsamkeit,
- Erforderlichkeit,
- Zweckbindung.

Sind [dennoch] Daten einmal angefallen, so sind technisch-organisatorische Maßnahmen zur Gewährleistung des Datenschutzes zu treffen. Hierzu gehört insbesondere die Beschränkung des Zugriffs auf die Daten durch die jeweils berechtigten Personen. Für automatisierte Abrufverfahren (Online-Verfahren) sind besondere Regeln zu beachten.

Aus den Prinzipien der Datensparsamkeit und der Erforderlichkeit folgt, dass Daten zu löschen sind, sobald sie nicht mehr benötigt werden. Nicht mehr erforderliche Daten, die wegen gesetzlicher Aufbewahrungs- und Dokumentationspflichten (insb. im Steuerrecht bis zu 10 Jahren) nicht gelöscht werden dürfen, sind zu sperren.

Zu den grundlegenden Datenschutzerfordernissen gehören ferner die unabdingbaren Rechte der Betroffenen (insb. das Recht auf Auskunft über die zu der jeweiligen Person gespeicherten Daten) und eine unabhängige Datenschutzaufsicht.



5. Datenschutzkontrollen

Der Gesetzgeber hat Aufsichtsbehörden und Bundes- bzw. Landesdatenschutzbeauftragte installiert, die für die Belange von Betroffenen zuständig sind und Behörden und nicht-öffentliche Organisationen kontrollieren und überwachen.

Der Landesdatenschutzbeauftragte geht insbesondere Beschwerden von Personen nach, die begründet darlegen, dass eine Datenschutzvorschrift verletzt wurde. Des Weiteren überwacht er die Ausführung der Datenschutzgesetze, wenn hinreichende andere Anhaltspunkte dafür vorliegen, dass eine Vorschrift verletzt wurde und er überwacht die Ausführung der Datenschutzgesetze auch ohne Anlass, wenn personenbezogene Daten im Auftrag durch Dienstleistungsunternehmen verarbeitet oder zum Zweck der (auch anonym) Übermittlung gespeichert werden. Die Ergebnisse der Überprüfungen fasst der Landesdatenschutzbeauftragte in seinem Jahresbericht zusammen.

6. Risiken

Vielen ist offensichtlich nicht bewusst, dass der Geschäftsführer für einen Gesetzesverstoß im Bereich Datenschutz (der normalerweise als grob fahrlässig anzusehen ist) mit seinem Privatvermögen (gem. §43 GmbHG) persönlich unbegrenzt haftet.

Die Berufung vom Geschäftsführer, Hoteldirektor, Abteilungsleiter Personal, EDV bzw. Controlling und Administrator zum Datenschutzbeauftragten ist wegen des Interessenkonfliktes ungültig. Ein Konzerndatenschutzbeauftragter ersetzt nicht den eigenen betrieblichen Datenschutzbeauftragten, jedes konzernzugehöriges Hotel muss ebenfalls einen DSB bestellen.

Konsequenzen

1. Nicht- oder Scheinbestellung

Die Nicht- oder Scheinbestellung eines DSBs kann gem. § 43 BDSG mit einem Bußgeld von bis zu 25.000 Euro geahndet werden. Eine Scheinbestellung liegt dann vor, wenn der bestellte DSB nicht über die notwendige Fachkunde verfügt oder ein Interessenkonflikt.

2. Fahrlässiger Verstoß gegen § 43 II BDSG

Bereits ein fahrlässiger Verstoß gegen § 43 II BDSG (z.B. wer unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet) wird mit einer Geldbuße bis zu 250.000 Euro geahndet.

3. Vorsätzlicher Verstoß gegen § 43 II BDSG mit Bereicherungsabsicht

Erfolgt ein Verstoß gegen § 43 II BDSG vorsätzlich und mit einer Bereicherungsabsicht oder der Absicht einen anderen zu schädigen, so droht zusätzlich zum Bußgeld (bis zu 250.000 Euro) gem. § 44 BDSG eine Freiheitsstrafe von bis zu zwei Jahren.

4. Schadensersatzforderungen der Betroffenen

Oftmals werden die Folgen einer richterlichen Auseinandersetzung unterschätzt. Ein Verstoß gegen das Bundesdatenschutzgesetz, der durch den Betroffenen bei der Aufsichtsbehörde angezeigt wurde, kann schnell sehr hohe Strafen, z.B. aus Schadensersatzgründen, nach sich ziehen.

Datenschutz- und Datensicherheitsaufwendungen

1. Organisation des Datenschutzes

Den Einstieg in die Umsetzung der Anforderungen an die betriebliche Organisation zur Gewährleistung der aus datenschutzrechtlicher Sicht primär geforderten Schutz- und Sicherheitsstandards bildet die **allgemeine Datenschutzanalyse**. Hierzu wird eine Kurzbefragung durchgeführt, die unterschiedliche Themen des Datenschutzes näher betrachtet.

Zu diesen Themen gehören:

- Allgemeine datenschutzrechtliche Belange
- Umgang mit Kundendaten
- Rechte der Betroffenen
- Umgang mit Mitarbeiterdaten
- Umgang mit Daten von Lieferanten/Vertragspartnern
- Marketing
- Datenübermittlung
- Technische und organisatorische Belange



An Hand der Auswertung des Fragebogens können die nächsten Schritte festgelegt werden, um den Anforderungen des BDSG zu genügen, das Haftungsrisiko und die Wahrscheinlichkeit des Datenmissbrauchs zu reduzieren sowie das notwendige Vertrauen zum Gast zu stärken. Der Hotelier erhält eine Analyse zu allen relevanten Themen, die den aktuellen Datenschutzstand des Hotels widerspiegelt und Schwachstellen aufzeigt.

Darauf aufbauend wird eine detaillierte **Ist-Analyse** durchgeführt, die alle technischen und organisatorischen Datenschutzbelange tiefgründig betrachtet. Zum Aufbau einer nachhaltigen Datenschutzorganisation ist es notwendig, für das Hotel ein **Datenschutzkonzept** zu erarbeiten und entsprechende organisatorische Maßnahmen festzulegen. Die Erkenntnisse aus der Ist-Analyse fließen in das Datenschutzkonzept ein.

Für die Umsetzung des Datenschutzkonzeptes in die betriebliche Organisation empfiehlt es sich, entsprechende Maßnahmen in einer Richtlinie zum Datenschutz oder einem **Datenschutzhandbuch** für das Hotel festzulegen. Hierin sind zugleich Verantwortlichkeiten für die Einhaltung des Datenschutzes sowie die Umsetzung des Datenschutzkonzeptes zu regeln. Die mit der Umsetzung betrauten Personen benötigen neben einer Anweisung und Handlungsanleitung oft zusätzliche Hilfestellungen.

2. Aufbau und Pflege der Datenschutzorganisation

Sofern das Hotel zur **Bestellung eines Datenschutzbeauftragten** verpflichtet ist, muss geprüft werden, wie dieses erfolgen soll. Die Geschäftsleitung muss die Entscheidung treffen, ob ein eigener Mitarbeiter zum Datenschutzbeauftragten berufen wird. Hierzu muss er den Mitarbeiter über Schulungen qualifizieren und er darf nicht im Interessenskonflikt zur auszuführenden Tätigkeit stehen. Ein Interessenskonflikt besteht insbesondere bei der Bestellung der Geschäfts- bzw. Hotelleitung, des Personalleiters, Leiter Controlling und EDV zum Datenschutzbeauftragten.

Als zweite Variante kann die Bestellung des Datenschutzbeauftragten durch eine externe Firma realisiert werden. Dieses ist in der Regel kostengünstiger und der Hotelier greift auf das bereits vorhandene Expertenwissen sofort zu. Die

Realisierung der Datenschutzmaßnahmen findet effizienter und schneller statt. Auch eine Mischform ist denkbar. So ist eine Aufgabenteilung zwischen dem externen Datenschutzbeauftragten und einem internen Datenschutzverantwortlichen realisierbar. Die notwendige Fachkompetenz wird durch die Bestellung des externen Datenschutzbeauftragten erlangt. Der interne Datenschutzbevollmächtigte muss nicht geschult werden, er nimmt aber Aufgaben des Datenschutzbeauftragten in Abstimmung direkt vor Ort wahr.

In der Gegenüberstellung werden die Vorteile (+) und Nachteile (-) der Bestellung eines internen und eines externen DSB verglichen.

Interner Datenschutzbeauftragter	Externer Datenschutzbeauftragter
<ul style="list-style-type: none"> + kennt sich im Unternehmen aus + ist im Unternehmen bekannt - Kosten und Zeitaufwand zur Erfüllung der Aufgaben als DSB Neben den eigentlichen Tätigkeiten und Aufgaben - Kosten für Aus- und Weiterbildung zum DSB - innerbetriebl. Interessenskonflikte - besonderer Kündigungsschutz wie Betriebsrat - Kosten für Fachliteratur, Seminare - Bereitstellung eines geeigneten Arbeitsplatzes 	<ul style="list-style-type: none"> - muss sich erst mit den Unternehmensstrukturen vertraut machen - DSB ist im/dem Unternehmen zunächst unbekannt (gegenseitige Vertrauensbildung) + Effektive und zuverlässige Umsetzung der Aufgaben eines DSBs + Transparente Kostenplanung / kalkulierbare Kosten durch Beratervertrag + befristeter Vertrag + eigene Mitarbeiter können sich Ihren Hauptaufgaben widmen + Vermeidung von Risiken (z.B. Schadensersatz, Bußgeld durch Verstöße gegen das BDSG) + Unvoreingenommenheit + Synergieeffekt

Unter Einbindung des Datenschutzbeauftragten ist eine nachhaltige Datenschutzorganisation aufzubauen. Hierbei sind insbesondere folgende Bereiche zu beachten, die organisatorischer Regelungen bedürfen:

- Verarbeitung von Kunden-, Mitarbeiter- und Lieferantendaten
- Gewährleistung der Rechte der Betroffenen
- Marketingmaßnahmen
- Auftragsdatenverarbeitung und Datenübermittlung
- Technik und Organisation

Abgeleitet aus der Art der Bestellung zum Datenschutzbeauftragten und der Größe des Hotels muss die Hotelleitung zu entscheiden, in welchem Umfang die Datenschutzmaßnahmen realisiert werden. Hierzu können zum Grundmodul die Module 1 bis 3 mit beauftragt werden. Sie unterscheiden sich im Leistungsspektrum, angepasst an die Anforderungen der aufzubauenden Datenschutzorganisation.

3. Preisliste

Mit dem Baukastensystem kann sich jeder Hotelier sein individuelles Leistungspaket zusammenstellen. Es ist auf die unterschiedlichen Bedürfnisse der Hotelleitung ausgerichtet.

Sonderkonditionen für den Hotel- und Gaststättenverband e.V.							
	Preis* [€]	Anzahl Mitarbeiter					
		< 10	10 - 50	> 50	HK**		
Organisation des Datenschutzes	einmalig						
Allgemeine Datenschutzanalyse***	390,-	+	+	+	+	+	
Techn. und org. Bestandsanalyse	890,-	-	o	+	+	+	
Datenschutzkonzept	690,-	-	o	+	+	+	
Datenschutzhandbuch	890,-	o	+	+	+	+	
Aufbau und Pflege der Datenschutzorg.	monatlich						
Grundmodul – Datenschutzberatung	69,-	-	+	+	+	+	
Modul 1 – Coaching interner DSB****	119,-	-	-	o	o	o	
Modul 2 – Implementierung interner DSV	151,-	-	-	o	o	o	
Modul 3 – Umfassendes Datenschutzmanagement	79,- bis 270,-	-	+	+	+	+	

Legende:	+ notwendig	Abkürzung:	HK Hotelkette	* Preise zzgl. gesetzliche MWST.
	o empfohlen		DSB Datenschutzbeauftragte	** Preise pro Hotel
	- bei Bedarf		DSV Datenschutzverantwortliche	*** Für Mitglieder HoGa Berlin kostenfrei
				**** Voraussetzung: eigener DSB

Honorarsätze für Beratungsleistungen im Datenschutz (Stand 01.02.2006)

1. Zusätzliche Beratungsleistungen

Projektleitung / Managementberatung	1100,- € / Tag
IT-Consultant	800,- € / Tag
Mindestberechnung	0,5 Tag

2. Beratung im Ausland

auf Anfrage

3. Reisekosten

PKW-Fahrkosten	0,70 € / km
----------------	-------------

Fahrkosten innerhalb von Berlin und Potsdam sowie 50 km vom Standort der Geschäftsstelle **inklusive**.

Bei Entfernungen von mehr als 400 km steht es dem Berater frei, mit der Bahn oder dem Flugzeug zu reisen. Die Kosten für Benutzung eines Mietwagens oder Taxis vor Ort trägt der Auftraggeber.

Die tatsächlich entstandenen Kosten werden auf Nachweis berechnet.

4. Übernachtungskosten

Kosten für die Unterbringung im Hotel werden auf Nachweis berechnet.

5. Spesen

Es wird eine Spesenpauschale von 20,- € / Tag berechnet.



4. Leistungsverzeichnis

Organisation des Datenschutzes

Die **allgemeine Datenschutzanalyse** zur Ermittlung der datenschutzrechtlichen Belange gemäß BDSG beinhaltet nachfolgende Leistungen:

- Einführungsgespräch zu Datenschutz- und Datensicherheitsaspekten in Hotels
- Durchführung einer Kurzbefragung zur Analyse des aktuellen Datenschutzstandes
- Erstellung eines Maßnahmenkataloges aus der Kurzbefragung
- Einsichtnahme der Internetpräsenz
- Vorabkontrolle Kontaktformulare, Online-Buchungssystem, Newsletter, Impressum und der Datenschutzerklärung, soweit vorhanden
- Beratung zur Bestellung eines Datenschutzbeauftragten
- Prüfung Meldepflicht
- Recherchen zu kundenbezogene Regelungen
- Erhebung Basisdaten für öffentliches Verzeichnis und Datenschutzerklärung
- Risiko-/Wahrscheinlichkeitsanalyse
- Telefonische Beratung

Die Hotelleitung erhält im Ergebnis einen Bericht (ca. 10 Seiten) inklusive Netzwerkdiagramm zur Risiko-/Wahrscheinlichkeitsanalyse. Anhand dieses Berichtes können Entscheidungen zur weiteren Vorgehensweise getroffen werden.

Die Hotelleitung oder ihre Vertretung muss einen Zeitaufwand von ca. 2 Stunden zur Kurzbefragung einplanen.

In § 9 BDSG ist geregelt, dass jedes Unternehmen alle erforderlichen technischen und organisatorischen Maßnahmen treffen muss, um die Ausführungen der Vorschriften des BDSG zu gewährleisten. Die **technische und organisatorische Bestandsanalyse** baut auf die allgemeine Datenschutzanalyse auf. Alle behandelten Themen werden tiefgründig betrachtet.

- Durchführung der datenschutzrechtlichen Bestandsanalyse
- Durchführung der technisch-organisatorischen Bestandsanalyse
- Durchführung der IT-Sicherheitsanalyse
- Erstellung eines Maßnahmenkataloges aus der Ist-Analyse
- Anlegen einer elektronischen Datenschutzakte
- Vorarbeiten zur Erstellung einer internen Verarbeitungsübersicht
- Vorarbeiten zur Darstellung datenschutzrelevanter Geschäftsprozesse
- Prüfung von Formularen auf Datenschutzkonformität
- Prüfung von Verträgen Dritter, die Datenschutzkonformität verlangen
- Erstellung Übersicht aller Hotelreservierungsportale
- Vorabkontrolle der eingesetzten Hotelsoftware
- Prüfung weiterer automatisierter Verfahren mit personenbezogenen Daten
- Prüfung Datenübermittlung personenbezogener Daten
- Prüfung Marketingmaßnahmen im Rahmen des BDSG und Unlauteren Wettbewerbsgesetz (ULG)
- Analyse der Aktivitäten der EDV-Administration, insbesondere bei externer Administration via Fernwartung
- Recherchen zu kundenbezogene Regelungen
- Zusätzlicher Arbeitsaufwand für Abstimmungsgespräche

Die Hotelleitung erhält im Ergebnis eine Ist-Analyse, die alle datenschutzrechtlichen Aspekte beleuchtet. Anhand dieser Analyse wird eine ToDo-Liste mit allen Sofortmaßnahmen erstellt.

Die Hotelleitung oder ihre Vertretung muss einen Zeitaufwand von ca. 2 - 3 Arbeitstagen zur Bestandsanalyse einplanen.



Auf der Grundlage der Bestandsanalyse kann ein **Datenschutzkonzept** erstellt werden. Hier werden die Vorgehensweise und der Fahrplan der Umsetzungsmaßnahmen festgeschrieben. Kritische Punkte werden herausgearbeitet, Maßnahmepakete werden für einen Zeitraum von 3 Jahren festgelegt.

Die wichtigsten Themen, die ein Datenschutzkonzept betrachtet, sind:

- Anleitungen zur praktischen Umsetzung des Datenschutzes
- Verarbeitung von Kunden-, Mitarbeiter- und Lieferantendaten
- Gewährleistung der Rechte der Betroffenen
- Auftragsdatenverarbeitung und Datenübermittlung
- Marketingmaßnahmen
- Datenschutzgerechter Internetauftritt
- Notwendigkeit der Bestellung eines Datenschutzbeauftragten
- Benennung der Verfahren, für die Melde- und Informationspflicht besteht
- Angaben der zu erstellenden Verfahrensdokumentation
- Technische und organisatorische Maßnahmen
- DV-Sicherheitsmaßnahmen
- Umgang mit mobilen Datenträgern
- Relevante Datenschutzgesetze

Die Hotelleitung erhält im Ergebnis ein Datenschutzkonzept (ca. 50 Seiten), das alle datenschutzrechtlichen Aspekte beleuchtet. Es dient als Leitfaden zum Aufbau und zur Pflege einer nachhaltigen Datenschutzorganisation.

Die Ergebnisse werden der Hotelleitung im Anschluss der Erstellung des Konzeptes präsentiert und diskutiert.

Im **Datenschutzhandbuch** befinden sich alle Richtlinien, Dokumente und Informationen, die im Rahmen der Datenschutzmaßnahmen anfallen. Es ist der zentrale Ablageort für das Hotel und dient der Aufsichtsbehörde, um sich einen schnellen und umfangreichen Überblick über die Datenschutzmaßnahmen machen zu können.

Schwerpunktmäßig enthält das Datenschutzhandbuch die Rubriken:

- Gesetzliche Anforderungen
 - Erstellung des öffentlichen Verfahrensverzeichnis und der Datenschutzerklärung
 - Impressum, AGB und Haftungsausschluss
 - Schriftliche Bestellung zum Datenschutzbeauftragten sowie Erstellung der Stellenbeschreibung
 - Verpflichtungsschreiben zum Datenschutz
 - Zusammenstellung relevanter Gesetzestexte
 - Tätigkeitsberichte
- Hard- und Softwareumgebung
 - Erstellung Anlagenverzeichnis
 - Dokumentation von Standardanwendungen, Anwendungen zur Verarbeitung personenbezogener Daten und Internetanwendungen
- Verfahrensanweisungen
 - Umgang mit personenbezogenen Daten
 - Rechte der Betroffenen
 - Marketing
- Sicherheitsmaßnahmen
 - IT-Sicherheitskonzept gemäß § 9 BDSG (Anlage)
 - Backup-Konzept
 - Administration
 - Systemsicherheit
- Verarbeitungsübersicht
 - Hotelsoftware
 - Online-Buchungssystem und Hotelreservierungsportale
 - Bonusprogramme
 - Videoaufzeichnung
 - Lohnabrechnung

- Auftragsdatenverarbeitung
 - Übersicht Beauftragung Dritter
 - Musterverträge
- Schulung und Belehrung
 - Schulungsplan
 - Informationsschreiben an Mitarbeiter
 - Belehrungen (z.B. Sicherheitsbelehrung EDV)
- Dienstanweisungen
 - Nutzung Internetdienste
- Konzepte und Analysen
- Korrespondenz und Nachweise

Die Hotelleitung erhält im Ergebnis eine vollständige Dokumentation über alle Datenschutzmaßnahmen. Den gesetzlichen Verpflichtungen, die sich aus dem Bundesdatenschutzgesetz ergeben, wird durch die Erstellung des Datenschutzhandbuches nachgekommen.

Abschließende Anmerkungen

Alle aufgeführten Module sind einmalige Kosten im Rahmen einer umfassenden Analyse des aktuellen Datenschutzstandes und der Beratung der abzuleitenden Maßnahmen.

Die Erstellung des Datenschutzkonzeptes setzt die technische und organisatorische Bestandsanalyse voraus.

Für die Erstellung des Datenschutzhandbuches werden zahlreiche Informationen benötigt, die sich ebenfalls aus der technischen und organisatorischen Bestandsanalyse ergeben. Soweit notwendige Informationen nicht vorliegen, reduziert sich der Umfang des Datenschutzhandbuches.

Aufbau und Pflege der Datenschutzorganisation

Das Grundmodul beinhaltet insbesondere Beratungs- und Informationsleistungen zu allen datenschutzrechtlichen Belangen. Die Module 2 und 3 sind nur im Zusammenhang mit dem Grundmodul erhältlich. Der monatliche Beitrag für Modul 3 richtet sich nach der Anzahl der Mitarbeiter und der Komplexität der Datenschutzanforderungen. Der Preis wird in einem separaten Angebot nach der allgemeinen Datenschutzanalyse bestimmt.

Leistungsübersicht

	Grundmodul	Modul 1	Modul 2	Modul 3
Bestellung zum betrieblichen Datenschutzbeauftragten	-	-	√	√
Coaching interner betrieblicher DSB	-	√	-	-
Coaching interner Datenschutzverantwortlicher	-	-	√	-
Überwachung Datenverarbeitungsprogramme	-	-	-	√
Prüfung der Zulässigkeit der Datenverarbeitung	√	√	-	-
Sensibilisierung der Mitarbeiter für Datenschutz	-	-	√	√
Vorbereitung von Schulungsmaßnahmen	-	√	√	√
Schulung und Belehrungen der Mitarbeiter	-	-	√	√
Vorabkontrolle automatisierter Verarbeitungsverfahren	√	√	-	-
Führen des öffentlichen Verzeichnisses	-	-	-	√
Überwachung von Datenschutzmaßnahmen	-	-	-	√
Benachrichtigung und Auskunftserteilung Betroffener	-	-	-	√
Beratung über techn. und org. Maßnahmen	√	√	-	-
Beratung über relevante Rechtsvorschriften	√	√	-	-
Informationsvermittlung über gesetzliche. Veränderungen	√	√	-	-
Bearbeitung Datenschutzbeschwerden	-	-	√	√
Erstellung und Weiterentwicklung von Richtlinien	-	-	√	√
Verpflichtung auf das Datengeheimnis	-	-	-	√
Erstellung Dienstanweisungen	-	√	√	√
Vertretung bei Kontrolle der Aufsichtsbehörde	-	-	√	√
Erstellung Tätigkeitsbericht	-	-	√	√
Durchführung von Datenschutzaudits	-	√	√	√
Telefonische Beratungsleistungen	√	√	√	√
Anwesenheit vor Ort [Tage/Jahr]	1	6	5	11



GESELLSCHAFT FÜR DATENSCHUTZ
UND DATENSICHERUNG e.V.

Mitglied in der Gesellschaft für
Datenschutz & Datensicherung e.V.



Fördermitglied im
Hotel- und Gaststättenverband Berlin e.V.

DataSolution Thurmann

Datenschutz & Datensicherheit

Isarstr. 13

14974 Ludwigsfelde

Tel.: (0 33 78) 87 13 86

mail@hoteldatenschutz.de

www.hoteldatenschutz.de

