LEITFADEN

DAS NEUE DATENSCHUTZRECHT

INFORMATIONEN & PRAXISTIPPS

Impressum

Herausgeber:

Hotelverband Deutschland (IHA) e.V.
Am Weidendamm 1A
10117 Berlin

Telefon 030/59 00 99 690
Telefax 030/59 00 99 699
E-Mail office@hotellerie.de
Web www.hotellerie.de

Verfasser:

Laura-Sophie Franze
Justitiarin
Hotelverband Deutschland (IHA) e.V.
E-Mail franze@hotellerie.de

Verleger:

IHA-Service GmbH
Kronprinzenstraße 37
53173 Bonn

Telefon 0228/92 39 290
Telefax 0228/92 39 299
E-Mail info@iha-service.de
Web www.iha-service.de

Vorwort

Am 25. Mai 2018 tritt die EU-Datenschutzgrund-verordnung (DSGVO) in Kraft. Sie bildet künftig den maßgeblichen datenschutzrechtlichen Rahmen in allen Mitgliedstaaten der Europäischen Union. In Deutschland wird die DSGVO durch das neue Bundesdatenschutzgesetz an manchen Stellen noch verschärft.

Nicht nur entfaltet die DSGVO ab dem 25. Mai 2018 ihre volle Wirkung, ab diesem Tage ist auch eine Überprüfung der Einhaltung des Datenschutzes in Unternehmen durch Behörden möglich.

Die gute Nachricht vorweg: Die wesentlichen Regelungen der Datenschutzrichtlinie (95/46/EG) aus dem Jahr 1995, umgesetzt im alten Bundesdatenschutzgesetz (BDSG-alt), bleiben bestehen und bilden auch weiterhin die Basis des deutschen Datenschutzrechts. Hotels, die bereits unter dem BDSG-alt Daten konform verarbeitet haben, werden durch die Neuregelungen weniger Veränderungen erfahren, als es im ersten Moment den Anschein hat: Die durch die DSGVO getroffenen strengeren Vorschriften stellen vor allem die umfassenden Dokumentationspflichten in den Vordergrund. Sanktionen von bis zu 20 Millionen Euro oder 4% des Jahresgewinns sind ein scharfes Schwert in der Hand der Behörden.

Mit diesem IHA-Merkblatt geben wir der Branche einen auf die praktischen Bedürfnisse der Hotellerie ausgerichteten Leitfaden an die Hand, der mit Check-listen die Umsetzung der herausfordernden Materie im Alltag der Hotellerie erleichtern wird.

Ihr

Otto Lindner
Vorsitzender

Inhaltsverzeichnis

Einleitung

Datenschutz ist spätestens mit der Einführung der DSGVO ein Teamprojekt geworden, das die Zusammenarbeit von Geschäftsführung, Recht- und Compliance-Abteilung, IT-Sicherheit, Personalabteilung und Betriebsrat erfordert.

Das Ziel, gelebten Datenschutz Teil der Unternehmenskultur werden zu lassen, kann nur durch eine umfassende Analyse der betriebsinternen Prozesse und Neuausrichtung erreicht werden. Für eine Durchleuchtung aller datenrechtlich relevanten Prozesse, die manchem Verantwortlichen vielleicht aktuell noch nicht vollumfänglich bewusst sind, sind besonders die nachfolgenden Fragen von großer Bedeutung:

- Wie werden welche Daten innerhalb Ihres Hotels verarbeitet?
- Wo werden Daten gespeichert?
- Aufgrund welcher Rechtsgrundlagen werden Daten verarbeitet?
- Wie lange werden Daten aufbewahrt und warum?
- Wann werden Daten gelöscht?

Bei der praktischen Umsetzung des neuen Datenschutzrechts rücken vor allem die Dokumentationspflichten in den Mittelpunkt. Nur durch detaillierte Dokumentation aller Verarbeitungstätigkeiten, Schutzmaßnahmen und Rechtsgrundlagen kann es dem Hotelier der Nachweis gelingen, dass Datenschutz in seinem Betrieb ernst genommen wird: Die Beweislast, sich datenschutzrechtlich konform zu verhalten hat, trägt von nun an der Hotelier.

Das Ziel Datenschutzkonformität setzt ein alle Datenverarbeitungsvorgänge umfassendes Datenschutzkonzept voraus, das in den nächsten Monaten die Befassung mit den folgenden Aufgabenbereichen erforderlich machen wird:

- Erhebung des Status der derzeitigen Datenverarbeitung
- Verfassen interner Richtlinien zum Umgang mit personenbezogenen Daten
- Einrichtung eines Dokumentationssystems für alle Verarbeitungstätigkeiten
- Bestellung eines internen / externen Datenschutzbeauftragten bzw. Datenschutzverantwortlichen für den Fall, dass keine Pflicht zum Datenschutzbeauftragten besteht

- Errichtung eines internen Kontrollsystems und Festlegung von Verantwortlichkeiten unter den Mitarbeitern
- Überprüfung der bisher verwendeten Einwilligungserklärungen und Datenschutzbestimmungen
- Überprüfung der bisher verwendeten Formulare, Betriebsvereinbarungen und Vertragsklauseln (AGB)
- Überprüfung der Verträge mit Dritten, insbesondere Auftragsverarbeitern, Subunternehmern und Lieferanten
- Umsetzung von Datenschutz durch Anpassung technischer Geräte
- Organisation von Schulungen für Mitarbeiter

Dieses Merkblatt wird Ihnen die Umsetzung des neuen Datenschutzrechts erleichtern, indem insbesondere standardisierte und auf andere Bereiche übertragbare Konzepte zum Datenschutz präsentiert werden. Wenn an manchen Stellen erwähnt wird, wie Datenschutz im Optimalfall umgesetzt wird, dann soll dies nicht abschreckend wirken. Es sind vor allem die kleinen Schritte, die große Unterschiede im Hinblick auf den Datenschutz ausmachen können.

Im Folgenden sollen insbesondere die für die Hotellerie relevanten Fragenstellungen zum Datenschutzrecht mit all seinen Teilaspekten von Arbeitnehmerdatenschutz bis WLAN beantwortet werden. Umfangreiche Checklisten (siehe auch Anlage 1) zur Evaluierung des aktuellen Stands und der umzusetzenden Anforderungen schließen jedes Kapitel ab.

KAPITEL 1:

Regelungsbereich des Datenschutzrechts

Zunächst einige grundsätzliche Erklärungen zum Verständnis der von der DSGVO verwendeten Begrifflichkeiten.

1. An welche Personen richtet sich das neue Datenschutzrecht?

Die DSGVO sieht Regelungen vor, die sich an unterschiedliche Personen wenden und wie folgt abzugrenzen sind:

- Verantwortlicher: Natürliche oder juristische Person, die Daten verarbeitet oder deren Verarbeitung beauftragt. Verantwortlicher ist immer das Hotel, wenn Daten durch seine Angestellte verarbeitet werden.
- Auftragsverarbeiter: Natürliche oder juristische Person, die im Auftrag des Verantwortlichen Daten verarbeitet. Der Auftragsverarbeiter unterliegt den Weisungen des Verantwortlichen. Typisches Beispiel ist die Fernwartung einer Software durch ein IT-Unternehmen oder eine externe Buchhaltung. Keine Auftragsverarbeiter hingegen sind Steuerberater oder Rechtsanwälte, da hier eine sog. Funktionsübertragung vorgenommen wird. In diesem Fällen verarbeitet der Auftragnehmer die Daten nach eigener Verantwortung.
- Datenschutzbeauftragter: Der Datenschutzbeauftragte ist eine vom Verantwortlichen zu benennende natürliche Person, die gesetzlich vorgegebene Pflichten zu erfüllen hat.
- Datenschutzvertreter: Wird auch als EU-Vertreter bezeichnet und ist eine natürliche oder juristische Person, die von jedem Verantwortlichen, der auf dem europäischen Markt agiert, zu bestellen ist, wenn der Verantwortliche außerhalb der Union niedergelassen ist.
- Betroffener: Die natürliche Personen, deren Daten verarbeitet werden.

2. Wann liegt ein Verarbeiten vor?

Der Begriff der Verarbeitung ist denkbar weit, so dass im Zweifel immer vom Vorliegen auszugehen ist. Konkret umfasst „Verarbeiten“ das Erheben, Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung oder jede andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, das Löschen oder die Vernichtung von personenbezogenen Daten.

Die Verarbeitung kann erfolgen durch automatisierte Verfahren mittels IT-Systemen oder durch einen manuellen Vorgang, wenn die Daten in einem Dateisystem, bspw. Kundendatei, gespeichert sind oder gespeichert werden sollen. Dabei muss es sich nicht zwingend um ein digitales Speichersystem handeln: Daten, die nur in Papier- bzw. Aktenform vorhanden sind, fallen unter das neue Datenschutzrecht, wenn die Akten einem Ordnungssystem unterliegen. Dies ist der Fall, wenn bspw. eine systematische Erfassung nach Jahr der Verarbeitung oder eine alphabetische Ordnung besteht.

3. Welche Daten unterscheidet die DSGVO?

Nur wenn personenbezogene Daten verarbeitet werden, findet die DSGVO Anwendung. Die DSGVO unterscheidet hierbei personenbezogene Daten allgemeiner Art (Art. 4 Nr.1 DSGVO), sowie personenbezogene Daten besonderer Kategorien (Art. 9 DSGVO). Je nachdem welche Daten verarbeitet werden, bestehen unterschiedlich strenge Anforderungen hinsichtlich des Umfangs der Dokumentationspflichten und der Schutzmaßnahmen zur Gewährleistung der Integrität der Datenverarbeitung.

Nicht in den Anwendungsbereich der DSGVO fallen Daten, die anonym verarbeitet werden und somit keinen Rückschluss auf eine identifizierbare Person zulassen.

4. Welche Informationen sind personenbezogene Daten?

Die Legaldefinition in Art. 4 Nr. 1 DSGVO ist weit: Wenn sich über die Daten eine Person identifizieren lässt, also die Informationen einer Person in einer unspezifischen Form zugeordnet werden können, liegt ein ausreichender Personenbezug vor.

Folgende Informationen sind Beispiele für personenbezogene Daten allgemeiner Art:

- Name, Geburtsdatum, -ort, Wohnanschrift, Telefonnummer, E-Mail-Adresse, Staatsangehörigkeit
- Geschlecht, körperliche Merkmale (Körpergröße, Körperstatur, Haar-, Augen-, Hautfarbe)
- Konto-, Kreditkarteninformationen, Sozialversicherungsnummer
- Beruf, berufliche Position, Einkommen, Kfz-Typ, Autokennzeichen
- Charaktereigenschaften, Verhaltensauffälligkeiten, Auftreten, Vorlieben
- Tatsächliche und rechtliche Familienverhältnisse
- IP-Adresse

Als besonders sensible personenbezogene Daten im Sinne des Art. 9 DSGVO werden eingestuft:

- Religion, politische Einstellung, Weltanschauungen
- Zugehörigkeit zu Gewerkschaften, politischen Parteien
- Gesundheit, Krankengeschichte, Behinderungen, Krankheitsrisiken
- Sexualleben, sexuelle Orientierung
- Biometrische und genetische Informationen

Die DSGVO ist ein Verbotsgesetz mit Erlaubnisvorbehalt: Das Gesetz geht somit von dem Grundsatz aus, dass personenbezogene Daten nicht verarbeitet werden dürfen, es sei denn, eine gesetzliche Rechtsgrundlage für die Verarbeitung besteht. Ist dies nicht der Fall, so kann subsidiär die Verarbeitung auch auf eine Einwilligung des Betroffenen gestützt werden.

Da dem Verantwortlichen als die Daten verarbeitende Stelle die Pflicht obliegt, im Falle einer fehlenden gesetzlichen Rechtsgrundlage nachzuweisen, dass die betroffene Person in die Verarbeitung ihrer Daten eingewilligt hat, ist es angeraten, sich die Einwilligung des Gastes stets schriftlich geben zu lassen und zu dokumentieren. Auf die Anforderungen an eine rechtswirksame Einwilligung wird in Detail im Kapitel 3.3 eingegangen.

Tipp für die Praxis

Ob personenbezogene Daten in Ihrem Hotel gespeichert werden dürfen, kann in der Mehrheit der Fälle anhand der Fragen entschieden werden:

- Ist die Information für die Erfüllung einer gesetzlichen Verpflichtung erforderlich? Ja, wenn eine vertragliche oder gesetzliche Obliegenheit besteht.
- Ist dies nicht der Fall: Möchte der Gast die Information hinterlegt haben? Ja, wenn er in die Verarbeitung eingewilligt hat.

5. Was sind geeignete technische und organisatorische Maßnahmen im Sinne der DSGVO?

Die DSGVO spricht an vielen Stellen davon, dass Datenschutz in den Unternehmen durch geeignete technische und organisatorische Maßnahmen (TOM) gewährleistet werden soll.

Bisher waren die TOM in der Anlage zu § 9 BDSG-alt in die Bereiche Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags-, Verfügbarkeits- und Trennungskontrolle untergliedert. Die Untergliederung wurde immer wieder kritisiert, weil eine so starke Ausdifferenzierung wenig pragmatisch ist. In Art. 32 DSGVO wird im Prinzip unterschieden zwischen Maßnahmen zur Vertraulichkeit, Integrität und Verfügbarkeit von Daten unterschieden. Hinzu kommen Maßnahmen, um sicherzustellen, dass Daten auch nur weisungsgemäß verarbeitet werden.

Anlage zu § 9 BDSG-alt Art. 32 DSGVO

• Zutritts- und Zugangskontrolle • Zugriffs-, Eingabe- und Weitergabekontrolle • Auftragskontrolle • Verfügbarkeits- und Trennungskontrolle	• Maßnahmen zur Vertraulichkeit • Maßnahmen zur Integrität • Maßnahmen zur Verfügbarkeit von Daten • Maßnahmen zur weisungsgemäßen Verarbeitung

Die DSGVO legt somit nicht fest, welche konkreten Maßnahmen zu ergreifen sind. Vielmehr obliegt es dem Verantwortlichen zu ermitteln, welches Schutzniveau im Einzelfall die von ihm verarbeiteten Daten bedürfen und welche Maßnahmen zum Schutz geeignet und erforderlich sind.

Die TOM nach § 9 BDSG-alt haben sich in der Vergangenheit bewährt und entsprechen den Anforderungen der DSGVO, sind nun aber leicht verändert kategorisiert.

Typische TOM entsprechend der Untergliederung im Sinne des Art. 32 DSGVO:

Vertraulichkeit von Daten

	Zutrittskontrolle: Verhinderung eines unbefugten Zutritts zu Datenverarbeitungsanlagen Zugangskontrolle: Verhinderung unbefugter Systembenutzung Zugriffskontrolle: Verhinderung unbefugten Lesens, Kopierens, Veränderns oder Entfernens Trennungskontrolle: Sicherstellung einer getrennten Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden durch Pseudonymisierung.

Integrität von Daten

	Maßnahmen, um sicherzustellen, dass nachvollzogen werden kann, dass und wer Daten verändert hat und dass Daten beim Transport gegen Zugriff und Manipulation geschützt sind.

Verfügbarkeit von Daten

	Maßnahmen, mit denen sichergestellt wird, dass Daten nicht ungewollt verloren gehen und im Falle eines Verlusts möglichst schnell wiederhergestellt werden könnten.

Überprüfung von Daten

	Maßnahmen, mit denen sichergestellt wird, dass z. B. Auftragnehmer, Daten nur weisungsgemäß verwenden. Ebenso Maßnahmen zur regelmäßigen Evaluierung von Auftragnehmern.

Die TOM sind die Grundlage für das für den datenverarbeitenden Betrieb erforderliche Datenschutzkonzept. Je nach Sensibilität und Schutzbedürftigkeit der personenbezogenen Daten, sind die TOM nach den folgenden Kriterien auszuwählen:

- Die Maßnahmen müssen dem aktuellen Stand der Technik entsprechen: technische Maßnahmen, die aktuell zur Verfügung stehen, sich in der Praxis bewährt haben und einen ausreichenden Sicherheitsstandard gewährleisten.
- Die Kosten der Anschaffung dürfen berücksichtigt werden: Implementierung und Instandhaltung sollen in einem angemessenen Verhältnis zu erforderlichen Schutzniveau der Daten stehen.
- Die Maßnahme muss geeignet sein, Schutz im Hinblick auf Art, Umfang, Umstände und Zweck der Verarbeitung zu gewährleisten. Dabei ist die objektive Eintrittswahrscheinlichkeit des Risikos und die Schutzwürdigkeit der Daten andererseits zu berücksichtigen.

Tipp für die Praxis:

Sobald der Status quo in der Datenverarbeitung Ihres Betriebs ermittelt ist (Welche Abteilung verarbeitet welche Daten aus welchem Anlass?), muss im Folgeschritt als interne Richtlinie festgelegt werden, welche konkreten TOM als zumutbare Schutzmaßnahmen im Betrieb standardmäßig anzugwenden sind. Die Dokumentation der Datenverarbeitung und angewendeten Schutzmaßnahmen erfolgt im Verzeichnis der Verarbeitungstätigkeiten, welches die interne Richtlinie zu den zu ergreifenden Schutzmaßnahmen als Anlage beizufügen ist.

6. Checkliste zu personenbezogenen Daten

- ☐ Gibt es in Ihrem Hotel ein Bewusstsein für die Wichtigkeit von Datenschutz und Datenschutzrisiken?
- ☐ Bestehen bereits datenschutzrechtliche Konzepte, bspw. interne Datenschutzleitlinien, Dokumentation von Datenschutzzielen, Verantwortlichkeiten und Datenschutzrisiken, auf die Sie ggf. aufbauen können?
- ☐ Sind den einzelnen Abteilungen bekannt, welche technisch-organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes bisher vorhanden sind?
- ☐ Wer ist in der Abteilung zuständig für die zukünftige Umsetzung von TOMs?
- ☐ Sind Mitarbeiter geschult, im Arbeitsalltag personenbezogene Daten zu erkennen?
- ☐ Welche Hotelabteilungen verarbeiten personenbezogene Daten?
- ☐ Hat jede Abteilung eine Übersicht über die Verarbeitungstätigkeiten hinsichtlich personenbezogener Daten?

KAPITEL 2:

Fragen rund um Datenverarbeitung

Der Hotelbetrieb ist ohne die Erhebung von Daten nicht möglich. Die DSGVO geht grundsätzlich davon aus, dass die Verarbeitung von Daten nicht gestattet ist. Vielmehr bedarf es eines Erlaubnistatbestandes, dessen Voraussetzungen für die Datenverarbeitung seitens der Hotels vorliegen müssen.

1. Wann dürfen Daten verarbeitet werden?

Personenbezogene Daten dürfen in den folgenden Fällen verarbeitet werden:

- Das Datenschutzrecht sieht eine Rechtsgrundlage für die Datenverarbeitung vor.
- Der Betroffene hat wirksam seine Einwilligung erklärt.
- Das Recht zur Datenverarbeitung ergibt sich aus einem anderen Gesetz, bspw. Melderecht, Steuer- oder Handelsrecht.
- Es besteht ein überwiegendes berechtigtes Interesse des datenverarbeitenden Unternehmens.

2. Wann erlaubt das Datenschutzrecht die Verarbeitung von Daten?

Die DSGVO regelt einige Fälle, in denen Daten verarbeitet werden dürfen:

- Daten, die zur Vertragserfüllung erforderlich sind: Alle Daten, auf die das Hotel Zugriff haben muss, um der Verpflichtung aus dem Beherbergungsvertrag, dem Dienstleistungsvertrag oder anderen Verträge, die vor, während oder nach dem Hotelaufenthalt geschlossen werden, nachkommen zu können.
- Daten, die zur Erfüllung einer sonstigen rechtlichen Verpflichtung erforderlich sind: Für alle Daten, die für das ordnungsgemäße Ausfüllen des Meldescheins erforderlich sind, ist das Hotel berechtigt und verpflichtet zu erheben. Ebenso alle Daten, die das Hotel aus steuer- oder handelsrechtlicher Sicht benötigt.

- Schutz lebenswichtiger Interessen
- Erfüllung öffentlicher Aufgaben
- Privilegierung der Zweckänderung: Alle Daten, die aufgrund einer vorhandenen Einwilligung des Betroffenen verarbeitet werden, dürfen auch für einen anderen Zweck verarbeitet werden, wenn dieser vom dem ursprünglichen Zweck umfasst ist. Die zweckgebundene ursprüngliche Einwilligung muss somit etwas weitergehen, als der neue Zweck, für den die Daten genutzt werden sollen.
- Wahrung berechtigter Interessen: Alle Daten, bei denen das Interesse an der Verarbeitung im Rahmen einer Abwägung die gegenläufigen Interessen des Verantwortlichen zugunsten des Verantwortlichen überwiegen. Hierauf kann z. B. die Videoüberwachung in der Hoteltiefgarage gestützt werden, wenn diese nur präventiv darauf abzielt, die Ordnung und Sicherheit der Gäste zu wahren.

Die Weitergabe von konform verarbeiteten Daten innerhalb eines Konzerns kann im Einzelfall unter Wahrung berechtigter Interessen fallen, wenn das Abwägungsergebnis zugunsten einer zulässigen Weitergabe ausfällt. Allerdings werden Konzernunternehmen datenschutzrechtlich wie Dritte behandelt, entsprechend ist der Tatbestand sehr eng auszulegen.

Zu dem Sonderfall der Direktwerbung siehe Kapitel 2.9.

3. Wann ist eine Einwilligung datenschutzrechtlich konform?

Eine rechtswirksame Einwilligung hat folgende Voraussetzungen zu erfüllen:

- Freiwilligkeit: Fehlt, wenn der Abschluss des Vertrages von der Erteilung der Einwilligung zur Datenverarbeitung abhängig gemacht wird oder Nachteile bei Verweigerung der Einwilligung angekündigt werden. Auch bei Bestehen eines wirtschaftlichen Abhängigkeitsverhältnisses denkbar.
- Konkreter Zweck: Fehlt bei pauschal erklärter Einwilligung in die Verarbeitung. Setzt Erkennbarkeit voraus, wer welche personenbezogenen Daten zu welchem Zweck wie lange verarbeitet und an wen weitergibt.

- Informierte Handlung: Fehlt, wenn Informationen nicht verständlich und transparent bereitgestellt werden. Setzt genaue Angaben statt allgemeiner Beschreibungen voraus.
- Unmissverständlichkeit: Fehlt, wenn die Einwilligung als solche nicht eindeutig erkennbar ist.

An einer Einwilligung fehlt es in den folgenden Konstellationen:

- Mit der Veröffentlichung einer Postadresse oder E-Mail-Adresse im Internet ist nicht die Einwilligung in die Zusendung von Werbung verbunden.
- Standardmäßig angekreuzte Einwilligung auf Internetseiten („Bitte Häkchen entfernen, wenn keine Zustimmung erklärt werden soll“) ist unzulässig und anstatt dessen ein „Double-Opt-In“ erforderlich, indem durch Aktivierung eines Links die Einwilligung bestätigt wird.
- Verstoß gegen das Kopplungsverbot (siehe Kapitel 2.5)

4. Dürfen Hotels Daten von Kindern verarbeiten?

Nach DSGVO steigt das Mindestalter für die Abgabe einer rechtswirksamen Einwilligung in die Verarbeitung personenbezogener Daten auf 16 Jahre. Von der Möglichkeit der Senkung der Altersgrenze auf 13 Jahre hat der deutsche Gesetzgeber keinen Gebrauch gemacht.

Die Eltern müssen ausdrücklich in die Verarbeitung der Daten ihrer Kinder einwilligen. Aufgrund der Beweislast sollten Hotels, die Daten von Kindern erheben, auf einer schriftlichen Einwilligung bestehen. Um den Vorwurf der Umgehung des Datenschutzrechtes zu vermeiden, sollte die Einwilligung der Eltern für ihre Kinder separat, bspw. durch eigene Zeile und erneute Unterschrift, erfolgen. Von einer pauschalen Einwilligung für die gesamte reisende Familie ist aus Klarstellungsgründen abzuraten.

5. Wie wirkt sich das Kopplungsverbot bei Gewinnspielen und sonstigen angebotenen Vorteilen aus?

Das Kopplungsverbot besagt, dass der Erhalt von beliebigen Vorteilen nicht mit der Bedingung verknüpft werden darf, dass in die kommerzielle Nutzung der abgegebenen personenbezogenen Daten eingewilligt wird. Diese Regelung beeinflusst maßgeblich die Ausgestaltung von Gewinnspielen und Teilnahme an Rabattaktionen etc. Die Einwilligung zur kommerziellen Nutzung der Daten ist unwirksam, wenn die Einwilligung nicht separat erklärt bzw. verweigert werden kann.

Dies wirkt sich auch auf die häufig eingesetzten Anreize wie Rabatte etc. für Verbraucher zur Eintragung von E-Mail-Adressen in Newsletter und E-Mail-Verteilern aus. Die Formulierung „Abonnieren Sie unseren Newsletter und erhalten Sie 5% Rabatt auf Ihre nächste Zimmerbuchung in unserem Hotel.“ stellt eine unzulässige Kopplung dar und macht die Einwilligung in den Erhalt des Newsletters unzulässig.

6. Wie ist die Einwilligung für einen E-Mail-Verteiler auszugestalten?

Da der Versand von digitalen Newslettern nur bei bestehender Einwilligung des Empfängers zulässig ist und der Verantwortliche die Beweislast hierfür trägt, ist die Dokumentation der Einwilligung essentiell. Behauptet ein Empfänger des Newsletters, dass die Einwilligung nicht erteilt wurde, dann wird der Hinweis darauf, dass generell das Double-Opt-In-Verfahren zur Anwendung kommt, von den Gerichten nicht als ausreichend anerkannt. Viel mehr ist zu dokumentieren, wann und wie die Einwilligung erteilt wurde. In der Praxis ist die Dokumentation weniger kompliziert als es klingt: Die für die Verwaltung von Newsletter-Abonnementen verwendeten Softwarelösungen gespeicherte Information, wann die Einwilligung per E-Mail erteilt wurden, ist in regelmäßigen Abständen zu archivieren.

Des Weiteren sind folgende Punkte bei Newslettern zu beachten:

- Erfolgt die Anmeldung zum Newsletter online, dann ist zwingend das Double-Opt-In-Verfahren einzusetzen. Aktuelle Softwareprogramme für

News-letter sehen dieses standardmäßig vor. Im Double-Opt-In-Verfahren erhält der Gast nach der Eintragung der E-Mail-Adresse eine kurze E-Mail mit dem Hinweis, seine Einwilligung per Klick auf einen Bestätigungslink endgültig zu bestätigen. Erst mit dem Anklicken des Links ist die Eintragung abgeschlossen und der Gast darf in den E-Mail-Verteiler aufgenommen werden.

- Da nur der Inhaber des E-Mail-Kontos auf die Bestätigungsmail Zugriff hat, wird durch das Double-Opt-In Verfahren die Einwilligung beweisbar und sollte als solche archiviert werden. Hat der Betroffene den Newsletter abbestellt, so muss die Adresse aus dem Verteiler genommen werden.
- Es ist bereits bei der Eintragung der E-Mail-Adresse in den Verteiler und in jedem Newsletter der Hinweis erforderlich, dass der Verwendung der E-Mail-Adresse jederzeit nachträglich widersprochen und der Newsletter abbestellt werden kann. Dies ist unkompliziert umzusetzen, indem im Newsletter ein Link zur Abmeldung zur Verfügung gestellt wird.
- Es sind keine unmittelbaren Vorteile wie Rabatte, Gutschein, etc. für das Newsletter-Abonnement anzubieten. Sobald der Empfänger sich für das Abonnement entscheiden hat, dürfen im Newsletter selbst Vorteile wie Rabatte gewährt oder exklusive Sonderangebote beworben werden.

7. Kann eine Einwilligung auch im Rahmen von Allgemeinen Geschäftsbedingungen (AGB) eingeholt werden?

Eine Einwilligung zur Datenverarbeitung im Rahmen von Allgemeinen Geschäftsbedingungen ist unter folgenden Voraussetzungen möglich:

- Am Textanfang der Allgemeinen Geschäftsbedingungen ist darauf hinzuweisen, dass eine datenschutzrechtliche Einwilligungserklärung enthalten ist.
- Die Einwilligungserklärung ist in den AGB drucktechnisch besonders hervorgehoben und als solche leicht erkenn- und abgrenzbar. Dies gelingt durch eine gesonderte Überschrift („Datenschutzrechtliche Einwilligung“), Fettschrift, Abgrenzungslinien oder farbliche Absetzungen.

- Die Einwilligung zur Datenverarbeitung setzt einen aktiven Mausklick oder das Leisten der Unterschrift voraus. Vorangekreuzte Kästchen erfüllen die Voraussetzungen der unmissverständlichen Abgabe einer Einwilligungserklärung nicht.

Allgemeine Geschäftsbedingungen liegen immer dann vor, wenn eine Klausel für eine Vielzahl von Verträgen vorformulierte, also nicht im Einzelnen ausgehandelte Vertragsklauseln, die eine Vertragspartei der anderen bei Vertragsschluss stellt. Dies ist bspw. bei einem Formular der Fall, das Meldeschein und Fragebogen zu weiteren personenbezogenen Daten kombiniert.

Tipp für die Praxis:

Für die Zusendung von Werbung ist stets eine gesonderte Einwilligungserklärung erforderlich, da das allgemeine Einverständnis in die Datenverarbeitung nicht den Erhalt von Werbung umfasst. Die Einwilligung, den digitalen Newsletter zugeschickt zu bekommen, kann somit nicht in AGB „versteckt“ werden.

8. Welche Bedeutung hat das Widerrufsrecht?

Die betroffene Person muss vor Abgabe der Einwilligungserklärung über ihr Recht zum Widerruf in Kenntnis gesetzt werden. Hierfür ist einerseits in den Datenschutzbestimmungen ein erklärender Hinweis aufzunehmen, darüber hinaus auch schon bei der Erklärung der Einwilligung auf die Widerrufsmöglichkeit hinzuweisen.

Zum Widerruf ist folgendes zu beachten:

- Auf das Widerrufsrecht ist ausdrücklich hinzuweisen.
- Der Widerruf muss jederzeit möglich sein.
- Für die Wirksamkeit des Widerrufs bedarf es keiner Begründung.
- Die Ausübung des Widerrufsrechts darf nicht erschwert werden, sondern ist so einfach wie die Abgabe der Einwilligung zu gestalten. So darf keine

schriftliche Widerrufserklärung per Post verlangt werden, wenn die Einwilligungserklärung online oder per E-Mail erfolgte.

Die bis zum Widerruf erfolgte Datenverarbeitung bleibt vom Widerruf unberührt.

Die von Ihnen bislang verwendeten Formulierungen zur Einwilligung in Vertragstexten sind auf ihre Verständlichkeit und Rechtskonformität zu überprüfen. Gleiches gilt für den Hinweis auf das Widerspruchsrecht in Ihren Datenschutzbestimmungen, der lauten könnte:

„Sie haben zu jeder Zeit und ohne Angabe von Gründen die Möglichkeit, der Verarbeitung Ihrer Daten zu widersprechen und deren Löschung zu verlangen. Die Löschung werden wir umgehend vornehmen. Sollte eine Löschung aufgrund gesetzlicher Vorgaben des Steuer- und Handelsrechts nicht möglich sein, werden Ihre Daten nur für die sich für uns aus den Gesetzen ergebenden Pflichten verarbeitet. Eine Verarbeitung zu kommerziellen Zwecken findet nach einem Widerspruch nicht mehr statt.“

9. Kann die Verarbeitung von personenbezogenen Daten auf berechtigte Interessen des Hotels an der kommerziellen Nutzung gestützt werden?

Bei der Nutzung von Daten zu Werbezwecken sieht die DSGVO zwei Wege vor: die Einwilligung des Betroffenen oder eine zum Vorteil des werbenden Unternehmers ausfallende Interessenabwägung.

Im Erwägungsgrund 47 der DSGVO heißt es: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.“ Die DSGVO geht somit davon aus, dass Unternehmen personenbezogene Daten für die Direktwerbung auch ohne Einwilligung des Betroffenen nutzen können.

Sie ahnen das Aber: Das deutsche Recht sieht im Gesetz gegen den unlauteren Wettbewerb (UWG) eine strengere Regelung vor und die Rechtsprechung wendet die Vorgaben des Datenschutzes und des Wettbewerbsrechts einheitlich an. Demnach muss eine Einwilligung in Werbung auch die Vorgaben des UWG erfüllen, die eine ausdrückliche vorherige Einwilligung fordert.

§ 7 Abs. 3 UWG nennt kumulativ folgende Voraussetzungen, die sehr eng angewendet werden müssen:

- ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat,
- der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet,
- der Kunde der Verwendung nicht widersprochen hat und
- der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann.

Bei alten Datenbeständen (bspw. E-Mail-Adressen ehemaliger Gäste) wird es häufig an der letztgenannten Voraussetzung fehlen, da der Gast auf die Verwendung der Daten zu Werbezwecken ausdrücklich hingewiesen worden sein muss.

10. Welche Aufklärungs- und Informationspflichten treffen den Verantwortlichen grundsätzlich hinsichtlich der Einwilligung?

Die Aufklärungs- und Informationspflichten umfassen folgende Angaben:

- Umfang der Datenverarbeitung
- Zweck der Datenverarbeitung
- Hinweis auf das Widerrufsrecht

Die Informationen müssen dem Betroffenen bereits bei Eingabe der personenbezogenen Daten (bspw. E-Mail-Adresse für Newsletter) verfügbar sein. Musterbeispiel für die Gestaltung der Newsletter-Anmeldung:

Anmeldung für den [Hotel]-Newsletter

Ja, ich möchte den Newsletter des [Hotel] mit auf mich zugeschnittenen Informationen über Produkte [ggf. spezifizieren] und Aktionen des [Hotel] und [Hotel]-Partnerunternehmen abonnieren:

Geben Sie hier Ihre E-Mail-Adresse ein

ZUM NEWSLETTER ANMELDEN

Diese Einwilligung können Sie jederzeit, z.B. hier [Mit Link zur Newsletter-Abmeldung versehen] oder am Ende jedes Newsletters widerrufen, was zu

einer Löschung der erhobenen Nutzerdaten führt.

Weitere Informationen finden Sie in unseren Datenschutzbestimmungen [Mit Link zu den Datenschutzbestimmungen versehen].

11. Dürfen personenbezogene Daten aus Meldescheinen vom Hotelier zu kommerziellen Zwecken verarbeitet werden?

Die Rechtslage bleibt durch die DSGVO unverändert: Die bereits vorausgefüllten oder vom Gast eingetragenen Daten sind nach § 30 Abs. 4 Bundesmeldegesetz (BMG) für den Zeitraum von einem Jahr aufzubewahren und bei Aufforderung den Meldebehörden auszuhändigen. Die Daten sind somit ausschließlich für die Meldebehörden bestimmt.

Es ist anerkannt, dass der Hotelier dem Meldeschein all die Daten zur Verarbeitung entnehmen darf, die zur Erfüllung vertraglicher Pflichten erforderlich sind. Für andere Zwecke dürfen die Daten zunächst nicht weiter verarbeitet werden.

Aus der Perspektive des Hoteliers kann der Moment, in dem der Gast den Meldeschein ausfüllt günstig sein, um sich auch die Einwilligung des Gastes in die weitere Verarbeitung geben zu lassen, sowie zusätzliche Daten, wie bspw. die E-Mail-Adresse, zu erlangen.

Hierbei sind folgende Punkte zu beachten:

- Es besteht die Möglichkeit, auf dem Meldeblatt optisch klar abgetrennt, den Gast durch ein Häkchen oder eine weitere Unterschrift in die Verarbeitung der Daten durch das Hotel einwilligen zu lassen. Um die Freiwilligkeit zu gewährleisten, bedarf es einer räumlich-optischen Unterscheidbarkeit zwischen den Daten, die aufgrund einer gesetzlichen Verpflichtung abgegeben werden, und solchen, die für das Hotelmarketing verwendet werden. Es ist bereits auf dem Formular darauf hinzuweisen, dass ein Widerruf der Einwilligung zu jedem späteren Zeitpunkt möglich ist.

- Der Gast darf auf dem Meldeschein aufgefordert werden, Angaben zu machen, die über den Umfang des § 30 Abs. 2 Bundesmeldegesetz hinausgehen. Dies ist insbesondere der Fall bei Fragen nach der E-Mail-Adresse und personenbezogenen Daten der Mitreisenden. Wichtig ist hierbei, dass der Gast leicht wahrnehmen kann, dass er zu diesen weiteren Angaben nicht gesetzlich verpflichtet ist und diese auch verweigern kann. Eine optische Abgrenzung durch gut sichtbare Kennzeichnung der verpflichtenden Angaben, oder Unterlegung der Textfelder mit unterschiedlicher Farbe ist denkbar. Darüber hinaus ist der Gast auf den Zweck der Verarbeitung ausdrücklich hinzuweisen.

- Vom Gast zusätzlich zur Verfügung gestellte Daten dürfen den Meldebehörden nicht zugänglich gemacht werden. Dies erzeugt einen Konflikt mit der Verpflichtung des Hoteliers, die Meldescheine der Behörde nach Aufforderung zu übergeben. Eine einfache Lösung könnte sein, dass die zusätzlichen Angaben auf dem unteren Abschnitt des Meldescheins gemacht werden, der anschließend abgetrennt werden kann (bspw. erleichtert durch eine Perforierung). Wichtig ist hierbei, dass der melderechtliche Teil, sowie der Teil mit den zusätzlichen Angaben jeweils unterschrieben sind.

12. Dürfen Daten aus alten Beständen, die mit Einwilligung des Betroffenen erhoben wurden, weiterverwendet werden?

Es ist nicht erforderlich, dass die Betroffenen ihre Einwilligung erneut erteilen. Dabei muss aber die Einwilligung bereits in der Vergangenheit den Anforderungen der DSGVO entsprochen haben. Dies könnte insbesondere im Hinblick auf das Kopplungsverbot fraglich sein, wenn Newsletter-Abonnements mit Gewinnspielen verknüpft wurden und die Teilnahme unter der Bedingung der Einwilligung in die Nutzung der Daten zu kommerziellen Zwecken stand. Ein Verstoß gegen das Kopplungsgebot liegt nur dann nicht vor, wenn das Einverständnis in die Datenverarbeitung mit einer separaten Einwilligung erklärt oder verweigert werden konnte.

Wurde in der Vergangenheit vom Betroffenen freiwillig und in Kenntnis des kommerziellen Charakters, bspw. Werbung, in die Datenverarbeitung eingewilligt, so dürfen die Daten auch zukünftig weiter verwendet werden. Die Aufsichtsbehörden gehen nach eigenem Bekunden davon aus, dass Einwilligungen, die unter dem alten BDSG konform erklärt wurden, auch der DSGVO entsprechen.

Zwar bleibt eine einmal abgegebene und nicht widerrufene Einwilligung wirksam. Die Einwilligungswirkung einer in der Vergangenheit erklärten Einwilligung entfällt jedoch, wenn die Kontaktaufnahme, in die eingewilligt wurde, mehr als ein Jahr zurückliegt. Aus diesem Grund sollten Newsletter wenigstens einmal im Jahr versendet werden.

13. Wie geht man mit Daten um, die in der Vergangenheit zwar datenschutzkonform erhoben wurden, jedoch die Einwilligung heute nicht mehr nachgewiesen werden kann?

Diese Situation stellt ein Dilemma dar: Einerseits sind die Daten konform verarbeitet worden und dürften auch zukünftig verwendet werden, andererseits

obliegt dem Verwender als Verantwortlicher die Nachweispflicht, dass Daten berechtigt verarbeitet werden.

Wenn der Nachweis nicht mehr möglich ist und der Betroffene ggf. bestreitet, die Einwilligung erteilt zu haben, dann muss von der Unzulässigkeit der Verwendung ausgegangen werden.

Wenn Sie entsprechende Daten nutzen, wird folgendes Vorgehen empfohlen:

- Markieren Sie in Ihrer Datenbank alle Datensätze, bei denen eine Einwilligung tatsächlich vorlag, Sie aber nicht mehr nachweisen können, dass die Einwilligung eingeholt wurde.
- Legen Sie einen Vermerk oder Eintrag im Verzeichnis der Verarbeitungstätigkeiten (siehe Kapitel IX) an, in dem Sie schildern, wie, wann, wo und durch wenn die Daten auf Grundlage der Einwilligung verarbeitet wurde. So könnte der Betroffene im Rahmen einer Tourismusmesse seine Visitenkarte überreicht und den bislang zugesendeten Newslettern nicht widersprochen haben. Ist keine Dokumentation mehr möglich, dann können die Daten nicht mehr verwendet werden und die Einwilligung ist neu einzuholen.
- Rechnen Sie damit, dass Sie zukünftig von einem geringen Prozentsatz der Betroffenen Nachfragen bekommen, warum sie angeschrieben werden. Bereiten Sie für diesen Fall eine Standardantwort vor:

„Sehr geehrte Frau X / sehr geehrter Herr X,

Sie erhalten unseren Newsletter per E-Mail zugeschickt, da Sie in unserer Datenbank als ehemaliger Gast oder Interessent an den Angeboten unseres Hotels geführt werden.

Sollte bei Ihnen mittlerweile kein Interesse mehr an besonderen Angeboten und aktuellen Informationen unseres Hotels bestehen, dann löschen wir selbstverständlich Ihre E-Mail-Adresse umgehend aus unserer Datenbank.“

14. Wie geht man mit Datenbanken um, die teilweise nicht konform sind?

Datenbanken, die Datensätze enthalten, die ohne Rechtsgrundlage oder unter Verstößen gegen das Datenschutzrecht, bspw. Kopplungsverbot, verarbeitet wurden, sollten zeitnah bereinigt werden und die Datensätze entfernt werden.

Dies gilt jedenfalls für Kontaktdatenbanken. Die Weiterverwendung solcher Daten in einer PMS-Datenbank kann hingegen auf ein berechtigtes Interesse gestützt werden.

Sollten die nicht konformen Daten nicht mehr aus der Datenbank gefiltert werden können, stellt das ein Dilemma dar, welches anhand einer Risikoabwägung bewertet werden sollte. Ist der Anteil von nicht konformen Datensätzen gering, dann spricht einiges dafür, das Risiko der Weiterverwendung einzugehen. Dokumentieren Sie hierfür Ihre Abwägung.

Sollten Datenbanken bereinigt werden müssen, dann sind der beabsichtigte Löschvorgang und seine Umsetzung im Verzeichnis der Verarbeitungstätigkeiten aufzunehmen.

15. Was gilt es bei Kundenzufriedenheitsbefragungen zu beachten?

Kundenzufriedenheitsbefragungen können ein effektives Mittel zur Verbesserung der Hoteldienstleistungen sein. Sollte der Gast nicht beim Check-in oder separat auf dem Meldeschein zur Abgabe weiterer Daten aufgefordert worden sein, könnte eine Kundenzufriedenheitsbefragung am Ende eines angenehmen Aufenthalts ein optimaler Zeitpunkt zur Erhebung von Daten sein. Im Rahmen der Befragung bietet es sich ggf. auch an, sich die Einwilligung des Gastes für den Newsletter geben zu lassen. Datenschutzrechtlich ist dabei folgendes zu beachten:

- Sollen personenbezogene Informationen aus dem Bogen zur Kundenzufriedenheit, bspw. Angabe des Namens oder eine Kombination aus Zimmernummer und Datum, E-Mail-Adresse, verarbeitet werden, dann ist hierfür an sich eine Einwilligung erforderlich.

- Werden die zur Befragung verwendeten Papierbögen auf dem Zimmer ausgelegt, dann müssen diese vom Housekeeping eingesammelt werden, bevor ein neuer Gast das Zimmer bezieht. Sollten personenbezogene Daten angegeben worden sein, so dürfen diese nicht Dritten zugänglich gemacht werden, was der Fall wäre, wenn beispielsweise ein ausgefüllter

Bogen auf dem Zimmer vom Housekeeping vergessen und vom nächsten Gast gelesen wird.

- Wird die Befragung erst nach der Abreise bspw. per Post oder E-Mail zugeschickt, dann ist dies rechtlich immer als Werbung zu werten und die Vorgaben aus § 7 Abs. 3 UWG (siehe Kapitel 2.9) müssen eingehalten sein. Empfehlenswert ist es, den Kunden spätestens beim Check-out (schriftlich) zu fragen, ob er mit der Zusendung eines Bogens zur Kundenzufriedenheit einverstanden ist.

16. Dürfen dem Gast Geburtstagsgrüße per E-Mail verbunden mit Werbung geschickt werden?

Geburtstagsgrüße sind ein besonders aufmerksames Mittel der Kontaktpflege und Kundenbindung. Voraussetzung hierfür ist die datenschutzkonforme Verarbeitung von Kontaktdaten und Geburtsdatum. Da es sich dabei um personenbezogene Daten handelt, ist eine Einwilligung des Gastes erforderlich: Lassen Sie sich die Einwilligung in die Verarbeitung der Daten schriftlich geben und weisen Sie daraufhin, dass der Verwendung zu jedem späteren Zeitpunkt widersprochen werden kann. Auch wenn all dies umständlich erscheint, so wird der Gast den verantwortungsbewussten Umgang mit seinen Daten ebenso schätzen wie eine Glückwunschkarte zum Geburtstag.

17. Dürfen personenbezogene Daten, erhoben für den Newsletter des Hotels, auch für andere Marketingzwecke, bspw. hoteleigenes Bonusprogramm, eingesetzt werden?

Die Einwilligung des Betroffenen kann nur zweckgebunden eingeholt werden. Die Einwilligung in die Verwendung der personenbezogenen Daten für einen Newsletter schließt eine anderweitige Verwendung regelmäßig aus. Eine Weiterverarbeitung der Daten außerhalb des ursprünglichen Zwecks ist nur zulässig,

- wenn sie mit dem ursprünglichen Zweck vereinbar ist und
- dies zur Wahrung berechtigter Interessen erforderlich ist und

- kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Zusätzlich sind bei der Verwendung von Daten von Gästen die Voraussetzungen des § 7 Abs. 3 UWG (siehe Kapitel 2.9) zu beachten, da ein Bonusprogramm werbenden Charakter hat.

Für Nicht-Kunden, die in die Zusendung von Newsletter eingewilligt haben, ist die Einwilligung so weit zu verstehen, dass damit auch eine Einwilligung in die Werbung für das eigene Bonusprogramm erteilt wurde. Nicht umfasst wäre aber jedoch die Aufnahme in das Bonusprogramm und das Anlegen eines Nutzerprofils, ohne dass der Betroffene, gleich ob ehemaliger Gast oder nicht, darin ausdrücklich eingewilligt hat.

18. Ist Profiling zulässig?

Profiling im Sinne des Art. 22 DSGVO ist jede Art der automatisierten Verarbeitung personenbezogener Daten, um sie im Hinblick auf bestimmte Aspekte zu bewerten. Zu diesen Bewertungskriterien können gehören

- Arbeitsleistung und wirtschaftliche Verhältnisse
- Gesundheit
- persönliche Vorlieben und Interessen
- Charaktereigenschaften (bspw. Zuverlässigkeit) und Verhalten
- Aufenthaltsort bzw. vergangene oder zukünftige Ortswechsel.

Diese Kriterien dienen dazu, eine Person zu analysieren oder bestimmte Vorhersagen zu treffen. Zum Einsatz kommen solche Profile in der Hotellerie für Marketingzwecke (gruppenspezifische Angebote) oder in der Personalabteilung beim Abgleich einer Stellenbeschreibung mit einem Bewerberprofil.

Grundsätzlich dürfen aus rechtmäßig erhobenen Daten Rückschlüsse bspw. auf die finanzielle Situation der Person gezogen werden. Nicht zulässig ist eine automatisierte Verarbeitung zur Bewertung der wirtschaftlichen Verhältnisse oder Arbeitsleistung, wenn sich aus dem Ergebnis rechtliche Konsequenzen ergeben. Nicht zulässig wäre somit das Auslesen des Schließsystems zur

Ermittlung der Pausenzeiten von Mitarbeitern oder die Auswertung von Aufnahmen aus der Videoüberwachung, um ein Verhalten von Arbeitnehmern zu analysieren.

19. Checkliste zur Datenverarbeitung

- Analysieren Sie, welche Arten von personenbezogenen Daten in Ihrem Hotel verarbeitet werden. Sind personenbezogene Daten besonderer Kategorien darunter? Werden personenbezogene Daten von Kindern verarbeitet?
- Auf welchen Grundlagen werden Daten in Ihrem Hotel verarbeitet?
- Wie war die bisher verwendete Einwilligung formuliert?
- Bestehen Datensätze, die aufgrund einer nicht konformen Einwilligung verarbeitet wurden? Gab es in der Vergangenheit Verstöße gegen das Kopplungsverbot?
- Bietet Ihr Hotel einen Online-Newsletter an? Wie wurden die E-Mail-Adressen erhoben?
- Aktualisieren Sie das Anmeldeformular für den Newsletter: Ist ein Hinweis auf das Widerrufsrecht enthalten?
- Wird das Double-Opt-In Verfahren für die Registrierung benutzt?
- Ist die Unterseite der Webseite, die das Anmeldeformular enthält, verschlüsselt (https-Protokoll)?
- Enthalten von Ihnen verwendete AGB Einwilligungen in die Datenverarbeitung? Wenn ja, ist die Einwilligung leicht wahrnehmbar? Vorangekreuzte Einwilligungen sind unwirksam.
- Enthalten die Datenschutzbestimmungen einen ausdrücklichen Hinweis auf das Widerrufsrecht?
- Kommen Sie Ihren Aufklärungs- und Informationsrechten betreffend der Verarbeitung personenbezogener Daten auf der Webseite nach?

KAPITEL 3:

Hoteltypische Sonderfälle der Datenerhebung

Zum Schutz der Gäste und des Hotelbetriebs können Sicherungsvorkehrungen angezeigt sein, die mit der Verarbeitung sensibler personenbezogener Daten einhergeht. Besondere Vorkehrungen sind insbesondere beim Einsatz von Überwachungskameras zu treffen.

1. Was ist bei der Videoüberwachung von Hotellobby, Fluren und der Parkgarage zu beachten?

Werden öffentlich zugängliche Räume wie die Hotellobby überwacht, so ist eine Datenschutz-Folgenabschätzung notwendig. Die Datenschutz-Folgenabschätzung ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken. Dazu im Detail siehe Kapitel 6.

Hinweise zum Einsatz von Videoüberwachung:

- Auf die Videoüberwachung ist durch sichtbare Hinweisschilder hinzuweisen.
- Da die Erklärung einer ausdrücklichen Einwilligung des Gastes in die Videoaufzeichnung bei Betreten der Lobby nicht praktikabel ist, kann die Verarbeitung auf berechtigten Interessen des Verantwortlichen gestützt werden, wenn diese die Interessen oder Grundrechte der Betroffenen überwiegen.
- Die Interessenabwägung ist im Rahmen der Datenschutz-Folgenabschätzung zu dokumentieren.
- Es bedarf einer internen Regelung, wer die Aufnahmen zu welchem Anlass einsehen darf.
- Die Videoaufnahmen müssen passwortgeschützt aufbewahrt und die Zugangsberechtigung geregelt werden.
- Nachdem der Zweck der Videoaufzeichnung erreicht wurde, sind die Daten zu löschen. Ein Löschkonzept, in welchen Abständen Videoaufzeichnungen gelöscht werden, ist in das Verzeichnis der Verarbeitungstätigkeiten aufzunehmen.

2. Darf die Information gespeichert werden, dass ein Gast eine Straftat begangen hat?

Reist ein Gast ab, ohne die Rechnung bezahlt zu haben, oder wurde im Nichtraucherzimmer geraucht, so ist es ein berechtigtes Interesse des Hotels, den Gast jedenfalls mit einem Hinweis in der Gästedatenbank zu speichern.

Dabei ist Folgendes zu beachten: Speichern Sie zu dem Gast keine konkreten Informationen zu dem Vorwurf, sondern verwenden Sie ein Symbol zur Kennzeichnung. Die jeweilige Bedeutung der Symbole sollte nur der Reservierungsabteilung und Geschäftsführung, nicht aber der gesamten Belegschaft bekannt sein.

KAPITEL 4:

Fragen zur Auftragsverarbeitung

Ein Auftragsverarbeiter übernimmt im Auftrag des Verantwortlichen bestimmte Datenverarbeitungen. In der Hotellerie handelt es sich hierbei klassischerweise um die externe Buchhaltung, ein Rechenzentrum, den Cloud-Provider oder ein Softwareunternehmen, welches Fernwartungen übernimmt.

1. Muss die Einwilligung die Datenweitergabe an einen Auftragsverarbeiter umfassen?

Die Einwilligung des Betroffenen muss sich nicht auf die Weitergabe der personenbezogenen Daten an einen Auftragsverarbeiter beziehen, denn rechtlich verlassen die Daten das Hotel als verantwortliches Unternehmen nicht. Das Hotel als Auftraggeber und Verantwortlicher entscheidet allein, wie der Empfänger die Daten zu verwenden hat, mithin ist der Auftragsverarbeiter eine nur ausgelagerte Stelle des Verantwortlichen.

Allerdings bedeutet dies auch, dass das Hotel weiter verantwortlich ist, dass die empfangende Stelle die Daten entsprechend den Vorschriften der DSGVO behandelt. Dies macht es zwingend erforderlich, dass die laufenden und zukünftig abzuschließenden Verträge mit Auftragsverarbeitern Klauseln zum Datenschutz enthalten. Der Verantwortliche muss sich von seinem Auftragsverarbeiter eine datenschutzkonforme Handhabung der übermittelten Daten zusichern lassen.

2. Welche Neuerungen bringt die DSGVO für die Beauftragung von Auftragsverarbeitern?

Auch wenn die DSGVO nicht vorsieht, dass der Verantwortliche seine Auftragsverarbeiter regelmäßig kontrollieren muss, so bleibt es auch weiterhin dabei, dass der Verantwortliche nachweisen können muss, dass

- der Auftragsverarbeiter sorgfältig ausgewählt wurde und
- der mit dem Auftragsverarbeiter geschlossenen Vertrag diesen verpflichtet, dass er technisch-organisatorische Maßnahmen zum Schutz der weitergegebenen Daten anwendet und
- dies seitens des Auftragsverarbeiters ausreichend dokumentiert wird.

Viele Buchhalter und Software-Unternehmen sind mit dem Datenschutzrecht vertraut. Da das Hotel als übermittelnde Stelle weiter in der Verantwortlichkeit ist, muss der Verantwortliche sich aber mindestens hinsichtlich der folgenden Punkte absichern:

- Externe Buchhaltung bewahrt Unterlagen in abgesperrten Aktenschränken auf. Zugangsberechtigung zu den Schränken bzw. Räumen, in denen sich die Schränke befinden, nur für das Personal, das den Zugriff auf die Daten zwingend benötigt.
- Keine Weitergabe der Daten durch den Auftragsverarbeiter an Dritte. Ausgenommen es besteht eine gesetzliche oder vertragliche Pflicht zur Weitergabe, bspw. Übermittlung von Daten an die Finanzämter.
- Bestehende und zukünftig abzuschließende Verträge müssen zwingend klare Regelungen enthalten, wie der Auftragsverarbeiter mit den Daten umzugehen hat.
- Bei der künftigen Wahl von Auftragsverarbeitern ist zu berücksichtigen, ob diese von sich aus Garantien für einen verantwortungsvollen Umgang mit übermittelten Daten geben werden und technisch-organisatorische Maßnahmen im Betrieb des Auftragsverarbeiters implementiert wurden.

3. Was sind die Mindestangaben, die ein Vertrag mit Auftragsverarbeitern hinsichtlich des Datenschutzes enthalten muss?

Den inhaltlichen Umfang legt Art. 28 Abs. 3 DSGVO fest:

- Beschreibung der konkreten Verarbeitungstätigkeit
- Festlegung des Zeitraums der Verarbeitung
- Festlegung des Zweck der Verarbeitung
- Art der personenbezogenen Daten

- Kategorien der Betroffenen
- Verpflichtung des Auftragsverarbeiters technisch-organisatorische Maßnahmen zur Datensicherung vorzunehmen
- Verpflichtung des Auftragsverarbeiters zur Vornahme einer Datenschutz-Folgenabschätzung
- Verpflichtung des Auftragsverarbeiters zur unverzüglichen Meldung von Datenschutzpannen an die Meldebehörden und den Verantwortlichen
- Verpflichtung des Auftragsverarbeiters, keine Daten an Dritte bspw. Subunternehmer weiterzugeben, es sei denn, eine Weisung seitens des Verantwortlichen liegt vor
- Verpflichtung des Auftragsverarbeiters, keine Daten außerhalb der Europäischen Union zu verarbeiten (es sei denn, es besteht eine rechtliche Pflicht bspw. Steuerrecht)
- Regelung von Löschpflichten seitens des Auftragsverarbeiters nach Abschluss der Verarbeitung
- Pflichten und Rechte des Verantwortlichen, der die Daten weitergegeben hat

Wichtig: In den auf dem bisherigen Datenschutzrecht basierenden Verträgen waren Sie als das Daten weitergebende Hotel verpflichtet, den Auftragsverarbeiter regelmäßig zu kontrollieren. Durch die DSGVO ist diese Pflicht nun so modifiziert worden, dass der beauftragte Auftragsverarbeiter nun selbst Haftungsverantwortung trägt. Bestehende Vertrag sollten nun dahingehend verändert werden, dass sich die Kontrollpflicht reduziert auf

- die sorgfältige Auswahl des Auftragsverarbeiters
- sowie die einmalige Einholung der Zusicherung, dass der Auftragsverarbeiter technisch-organisatorische Maßnahmen zum Datenschutz vorgenommen hat. Hierfür lassen Sie sich die entsprechende Dokumentation seitens des Auftragsverarbeiters aushändigen.

Alle Vereinbarungen und Weisungen an den Auftragsverarbeiter sind zwingend in Ihr Verzeichnis der Verarbeitungstätigkeiten aufzunehmen: Zwar haftet der Auftragsverarbeiter für Verstöße ebenfalls mit einem Bußgeld bis zu 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes, die Haftungsrisiken bestehen beim Auftraggeber jedoch fort, da er dem Auftragsverarbeiter Weisungen gibt.

Durch eine Dokumentation aller Vereinbarungen und Weisungen an den Auftragsverarbeiter gelingt es Ihnen gegebenenfalls nachzuweisen, dass Sie gesetzeskonform gehandelt haben und eine Haftung ausgeschlossen ist.

4. Gibt es weitere Verträge, die aufgrund der DSGVO überarbeitet werden müssen?

Es ist empfehlenswert, alle bestehenden Verträge unter dem Aspekt des neuen Datenschutzrechts einer kurzen Revision zu unterziehen, denn Datenschutz spielt auch eine Rolle bei Geschäftsbeziehungen, deren Vertragsgegenstand keine Datenverarbeitung ist.

Bitten Sie jeden Ihrer Vertragspartner, eine verträgliche Zusatzvereinbarung zu akzeptieren, in der sich bspw. Ihre Lieferanten dazu verpflichten, keine Daten an Dritte weiterzugeben. Gleiches gilt, wenn bspw. das Housekeeping an ein externes Unternehmen ausgelagert wurde. Lassen Sie sich schriftlich zusichern, dass das Reinigungspersonal im Umgang mit Daten geschult ist und keine Daten an Dritte wie bspw. den Subunternehmer als Arbeitgeber weitergibt.

Tipp für die Praxis:

Die folgenden Vertragsinhalte sind keine sich aus der DSGVO neu ergebenden Pflichten, sondern wurden auf Grundlage des alten BDSG eingeführt. Nutzen Sie die Revision Ihrer Verträge, um sicherzustellen, dass diese Vorgaben spätestens jetzt erfüllt sind:

- Der Auftragsverarbeiter ist nur berechtigt, Personen bei der Verarbeitung einzusetzen, die zur Verschwiegenheit vertraglich oder gesetzlich verpflichtet sind.
- Der Auftragsverarbeiter hat alle sich jetzt aus Art. 32 DSGVO ergebenden erforderlichen technisch-organisatorischen Maßnahmen zu ergreifen

- Daten sind nach Ende des Auftrags nach Wahl des Auftraggebers zurückzugeben oder zu vernichten. Ausnahme: Pflicht zur Speicherung zum Beispiel nach Steuer- oder Handelsrecht seitens des Auftragsverarbeiters
- Dem Auftraggeber sind alle Informationen zur Durchführung von Kontrollen zur Verfügung zu stellen und Kontrollen müssen durch den Auftragsverarbeiter ermöglicht und unterstützt werden.
- Verstöße gegen das Datenschutzrecht müssen der Datenschutzaufsichtsbehörde des Bundeslandes, in dem das Hotel sich befindet, unverzüglich nach dem Bekanntwerden gemeldet werden. Eine Liste aller Datenschutzaufsichtsbehörden findet sich im Internet in der Infothek der Bundesbeauftragten für den Datenschutz und die Informationssicherheit: www.bfdi.bund.de.

5. Checkliste zur Auftragsverarbeitung

- ☐ Sind Externe mit der Verarbeitung personenbezogener Daten als Auftragsverarbeiter betraut?
- ☐ Auf welcher Grundlage werden die Auftragsverarbeiter für Sie tätig?
- ☐ Sind Verträge hinsichtlich datenschutzrechtlicher Vorgaben aktualisiert worden und enthalten diese Mindestangaben gemäß Art. 28 Abs.3 DSGVO?
- ☐ Gab der Auftragsverarbeiter bislang die Gewähr für einen vertraulichen Umgang mit den übermittelten personenbezogenen Daten?
- ☐ Sprechen Sie Ihre Auftragsverarbeiter auf das neue Datenschutzrecht an und lassen Sie sich schriftlich zusichern, dass sich Ihre Auftragsverarbeiter schulen lassen.
- ☐ Dokumentieren Sie Ihre Weisungen an den Auftragsverarbeiter.
- ☐ Schließen Sie mit allen Ihren sonstigen Vertragspartnern Zusatzvereinbarungen zum datenschutzkonformen Umgang mit personenbezogenen Daten.
- ☐ Die Europäische Kommission plant, Musterverträge zur Einhaltung datenschutzrechtlicher Vorgaben zur Verfügung zu stellen. Ziehen Sie aus Gründen der Rechtssicherheit diese Vorlagen heran, sobald diese veröffentlicht sind.

KAPITEL 5:

Fragen zum Datenschutzbeauftragten

Der Datenschutzbeauftrage sollte dem Hotel als kompetenter Ansprechpartner bei der Erstellung und Umsetzung eines Datenschutzkonzepts zur Seite stehen. Sollte für ein Unternehmen die Pflicht zur Benennung eines Datenschutzbeauftragten nicht bestehen, wird dennoch empfohlen, eine für Datenschutz verantwortliche Person intern festzulegen, da die Einhaltung des Datenschutzgesetzes unabhängig von der Pflicht zur Benennung eines Datenschutzbeauftragten besteht.

1. Welche Hotels brauchen einen Datenschutzbeauftragten?

Die DSGVO sieht einen Datenschutzbeauftragten verpflichtend vor, wenn die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht,

- welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke einen umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen oder
- die in der umfangreichen Verarbeitung besonders sensibler Daten gemäß Art. 9 DSGVO besteht.

In Deutschland wird die Verpflichtung erweitert, indem die bisherigen Regelungen des BDSG erhalten bleiben: Das BDSG verlangt die Bestellung eines Datenschutzbeauftragten, **wenn mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind**. Anknüpfungspunkt ist somit nicht die Betriebsgröße oder Art der Anstellung (Teilzeit / Vollzeit).

In der Hotellerie sind Mitarbeiter der Rezeption, Buchhaltung und Personalabteilung ständig mit der Verarbeitung personenbezogener Daten betraut.

Besteht aufgrund der Art der Datenverarbeitung die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (siehe dazu Kapitel 6.4), so ist stets ein Datenschutzbeauftragter verpflichtend.

2. Wie benennt man einen Datenschutzbeauftragten?

Eine Form und bestimmte Dauer für die Bestellung besteht nicht. Die Bestellung sollte aus Nachweisgründen in Textform erfolgen (siehe Anhang 2 Muster Bestellung eines Datenschutzbeauftragten). Der Bestellung ist eine detaillierte Beschreibung der Aufgaben des Datenschutzbeauftragten beizufügen.

Die Kontaktdaten des Datenschutzbeauftragten sind in den Datenschutzbestimmungen der Hotelwebseite zu veröffentlichen und sind der jeweiligen Landesdatenschutzbehörde zu übermitteln. Auf den meisten Behördenwebseiten finden sich Formulare zur Meldung des Datenschutzbeauftragten.

Tipp für die Praxis:

Welche konkreten Aufgaben der Datenschutzbeauftragte in Ihrem Betrieb zu übernehmen hat, sollte schriftlich niedergelegt werden. Treffen Sie insbesondere Regelungen, an welche Person in der Geschäftsleitung der Datenschutzbeauftragte zu berichten hat und legen Sie hierfür die zeitlichen Abstände fest. Im Idealfall führt der Datenschutzbeauftrage auch regelmäßig Mitarbeiterschulungen durch.

3. Wen sollte ein Hotel als Datenschutzbeauftragten bestellen?

In Betracht kommt ein interner oder externer Datenschutzbeauftragter. Nicht bestellt werden darf eine Person, die in einen Interessenkonflikt geraten könnte. Ein solcher ist denkbar bei Mitgliedern der Unternehmensleitung, Personalleitern sowie IT- Administratoren.

Ein Datenschutzbeauftragter muss das folgende Fachwissen haben:

- Kenntnis der für das Hotel relevanten datenschutzrechtlichen und spezialgesetzlichen datenschutzrechtlichen Vorschriften
- Kenntnisse der Informations- und Telekommunikationstechnologie und der Datensicherheit

- Kenntnisse zum Führen des Verzeichnis der Verarbeitungstätigkeiten, zur Umsetzung von Löschkonzepten und Vornahme von Datenschutz-Folgenabschätzungen

Eine Zertifizierung als Datenschutzbeauftragter muss nicht nachgewiesen werden, ist jedoch zu empfehlen.

Aufgrund der sich aus der Stellung des Datenschutzbeauftragten ergebenden Aufgaben ist es wohl für die Mehrheit der Hotels zu empfehlen, einen externen Datenschutzbeauftragten zu bestellen. Hierfür sprechen die folgenden Punkte:

- Der Datenschutzbeauftragte ist in alle datenschutzrechtlichen Fragen jeder Abteilung einzubinden. Zur Aufgabenerfüllung sind jährliche Fortbildungen erforderlich (zeitlicher und finanzieller Aufwand).
- Der Datenschutzbeauftragte hat Einblick in die sensibelsten Bereiche des Hotels, insbesondere Buchhaltung und Personalabteilung (Zugang zu allen personenbezogenen Daten zu gewähren).
- Bei seiner Tätigkeit als Datenschutzbeauftragter unterliegt er keinen Weisungen und berichtet unmittelbar der Hotelleitung als Verantwortlichen (Weisungsunabhängigkeit).
- Der interne Datenschutzbeauftragte darf während dieser Tätigkeit und nach deren Beendigung für ein weiteres Jahr nicht gekündigt werden. Die Kündigung aus wichtigem Grund ist weiter möglich (Besonderer Kündigungsschutz).

4. Wie ist ein Datenschutzbeauftragter in den Betriebsablauf einzubinden?

Der Datenschutzbeauftragte sollte für alle Hotelmitarbeiter als Ansprechperson bei Fragen mit Datenbezug zur Verfügung stehen. Ein jährliches Treffen des Führungspersonals der einzelnen Abteilungen mit dem Datenschutzbeauftragten sollte für Rückfragen und Beratung zur abteilungsübergreifenden Umsetzung des Datenschutzes genutzt werden.

Die an den Datenschutzbeauftragten gestellten Fragen, sollten inklusive der Antwort, als Nachweis für die Bemühungen, Datenschutz umfassend im

Hotelbetrieb umzusetzen, dokumentiert werden. Dies gilt insbesondere für den Fall, wenn keine befriedigende Lösung für eine Fragestellung gegeben werden kann.

Für eine koordinierte Umsetzung des Datenschutzes ist insbesondere bei einem externen Datenschutzbeauftragten empfehlenswert, eine weitere hotelinterne Ansprechperson zu bestimmen. So werden gegebenenfalls existierende Hemmschwellen abgebaut, die Mitarbeiter von Rückfragen bei einem externen Datenschutzbeauftragen abhalten.

5. Checkliste zum Datenschutzbeauftragten

- Verfügt Ihr Hotel über einen Datenschutzbeauftragten? Wenn nein, warum nicht? Dokumentieren Sie Ihre Erwägungsgründe.
- Werden in Ihrem Hotel sensible, also personenbezogene Daten besonderer Kategorien verarbeitet? Sind mindestens zehn Mitarbeiter ständig mit der Verarbeitung personenbezogener Daten vertraut? Sie benötigen in diesen Fällen einen Datenschutzbeauftragten.
- Wenn Sie keinen Datenschutzbeauftragten benötigen, wer ist dann in Ihrem Betrieb für die Überwachung der Einhaltung des Datenschutzes verantwortlich?
- Wenn Sie in Kürze einen Datenschutzbeauftragten benennen werden: Berücksichtigen Sie die Erwägungen für und gegen einen internen Datenschutzbeauftragten.
- Ist ein interner Datenschutzbeauftragter als solcher zertifiziert? Wenn nein, wie ist der Datenschutzbeauftragte anderweitig qualifiziert?
- Ist der Datenschutzbeauftragte der Aufsichtsbehörde gemeldet worden?
- Sind die Mitarbeiter geschult, wann der Datenschutzbeauftragte einzubeziehen ist?
- Findet eine jährliche Schulung der Mitarbeiter durch den Datenschutzbeauftragten statt?
- In welchen Abständen berichtet der Datenschutzbeauftragte der Geschäftsleitung über seine Tätigkeit?
- Wird die Zusammenarbeit mit dem Datenschutzbeauftragten dokumentiert?

KAPITEL 6:

Fragen zu Verzeichnis der Verarbeitungstätigkeiten und Datenschutz-Folgenabschätzung

Das Verzeichnis der Verarbeitungstätigkeiten wird künftig der Nachweis für die Bemühungen zur datenschutzkonformen Datenverarbeitung sein. Der Erstellung des Verzeichnisses geht die Erhebung des Status quo der Datenverarbeitung (Welche Abteilung erhebt auf welcher Grundlage welche Daten?) und ein an der Schutzbedürftigkeit der personenbezogenen Daten ausgerichteter Katalog an zu ergreifenden TOM voran. Die Datenschutz-Folgenabschätzung ist hingegen nur in Einzelfällen erforderlich, wenn die Datenverarbeitung ein „voraussichtlich hohes Risiko“ für die Freiheiten und Rechte der Betroffenen bedeuten kann.

1. Was ist ein Verzeichnis von Verarbeitungstätigkeiten?

Das Verzeichnis von Verarbeitungstätigkeiten ist eine systematische Dokumentation aller Verarbeitungsvorgänge. Es bildet die Grundlage für die Tätigkeit des Datenschutzbeauftragten und dient zum Nachweis der Pflichterfüllung des Verantwortlichen gegenüber Aufsichtsbehörden, die auf Anfrage Einsicht verlangen dürfen.

Die Pflicht, ein solches Verzeichnis zu führen, gilt grundsätzlich für Unternehmen mit mehr als 250 Mitarbeitern. Beschäftigt ein Unternehmen weniger als 250 Mitarbeiter, muss ein Verzeichnis von Verarbeitungstätigkeiten geführt werden, wenn

- die Verarbeitungen personenbezogener Daten ein Risiko für die Rechte und Freiheiten der betroffenen Personen, bspw. Videoüberwachung von öffentlich zugänglichen Räumen, birgt oder
- die Verarbeitungstätigkeit nicht nur gelegentlich, sondern regelmäßig erfolgt, bspw. Lohnbuchhaltung, Kundendatenverwaltung, oder

- die Verarbeitungstätigkeit sensible, personenbezogene Daten besonderer Kategorien umfasst (insbesondere Gesundheitsdaten von Hotelgästen, Religionszugehörigkeit der Arbeitnehmer in der Lohnbuchhaltung, usw.)

Für die Erforderlichkeit des Verzeichnisses kommt es anders als bei der Datenschutz-Folgenabschätzung nicht darauf an, dass es sich voraussichtlich um ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen handelt. Da jedes Risiko für die Rechte und Freiheiten durch die Verarbeitung genügt, ist das Erstellen des Verzeichnisses stets geboten.

2. Wie führt man ein Verzeichnis von Verarbeitungstätigkeiten?

Das Verzeichnis sollte so aufgebaut sein, dass jederzeit Auskunft gegeben werden kann, welche Daten von wem und zu welchem Zweck auf welcher Grundlage im Hotel verarbeitet und an wen weitergegeben werden. So kann der Beweislast, also dem vom Hotel zu erbringenden Nachweis, dass datenschutzkonform gehandelt wird, Genüge getan werden.

Auch gelingt es so Rechenschaft über folgende Grundsätze zu geben, die zu den Kernelementen des BDSG-alt und der DSGVO zählen:

- Rechtmäßigkeit der Datenverarbeitung
- Zweckbindung der verarbeiteten Daten
- Transparenz der Datenverarbeitung
- Datenminimierung
- Richtigkeit der Datenbestände
- Begrenzung der Speicherung von Daten
- Integrität und Vertraulichkeit der Datenverarbeitung

Des Weiteren stellt das Verzeichnis die Grundlage für Risikoabschätzungen und zu ergreifende Sicherungsmaßnahmen dar.

Das Verzeichnis ist schriftlich oder elektronisch zu führen und kann auch mit einer Software erfolgen. Es muss zumindest die sich aus Art. 30 DSGVO ergebenden Pflichtangaben enthalten. Darüber hinaus kann es sinnvoll sein, Zusatzinformationen freiwillig hinzuzufügen, wenn diese geeignet sind, im

Zweifelsfall eine weitere Nachweismöglichkeiten der Datenschutzkonformität zu bieten.

Pflichtangaben des Verzeichnisses von Verarbeitungstätigkeiten:

- Name und Kontaktdaten des Verantwortlichen, seines Vertreters sowie des etwaigen Datenschutzbeauftragten
- Konkrete Benennung aller Datenverarbeitungstätigkeiten in den jeweiligen Abteilungen
- Nennung aller Zwecke der Datenverarbeitungen
- Beschreibung der Kategorien betroffener Personen, bspw. Mitarbeiter und Gäste
- Beschreibung der Kategorien personenbezogener Daten, bspw. Kontaktdaten, Nutzungsdaten
- Beschreibung der Kategorien von Empfängern, bspw. interne Abteilungen, externe Dienstleister, Auftragsverarbeiter
- Bei Übermittlungen personenbezogener Daten an ein Drittland: Benennung des Drittlands und Beschreibung der Kategorien von Empfängern mit Kontaktdaten und Kategorien der übermittelten Daten
- Fristen für die Löschung der verschiedenen Datenkategorien
- Allgemeine Beschreibung der einzelnen technischen und organisatorischen Maßnahmen: Im Idealfall besteht ein allgemeines Sicherheitskonzept auf das im Verzeichnis der Verarbeitungstätigkeiten Bezug genommen werden kann. Sind stärkere Schutzmaßnahmen erforderlich, insbesondere bei der Verarbeitung personenbezogener Daten besonderer Kategorien, bspw. Gesundheitsdaten, dann sind die im Einzelfall angewendeten Maßnahmen mit höherem Schutzniveau ausdrücklich zu nennen.

Fakultative und im Falle behördlicher Überprüfung sehr hilfreiche Zusatzangaben:

- Woraus ergibt sich die Rechtmäßigkeit der verarbeiteten Daten: Benennung der Rechtsgrundlage / Verarbeitungszweck und Kompatibilität bei Zweckänderung / Ausgestaltung der Einwilligung / Ausgestaltung des Widerspruchs / Interessensabwägung: welche Interessen werden berücksichtigt und Ergebnis der Abwägung

- Gewährleistung von Informations- und Benachrichtigungspflichten: Verweis auf Datenschutzhinweise, Vertragsformulare, Betriebsvereinbarungen
- Sicherheitskonzept mit allen angewendeten technischen und organisatorische Maßnahmen: Ergebnis der Risikobewertung / Möglichkeiten der Pseudo- oder Anonymisierung / Abstände der Risikoüberprüfung inklusive Datum der letzten Überprüfung / Ergriffene Maßnahmen zur Datenminimierung durch angepasste Grundeinstellungen an technischen Geräten (privacy by design / privacy by default)
- Dokumentation der Risikoabschätzung zur Klärung, ob eine Datenschutz-Folgenabschätzung erforderlich ist: Prüfung der Erforderlichkeit dieser Risikobewertung und Ergebnis, ggf. Ausführungen zum Risikomanagement

Tipp für die Praxis:

Da die Hotelleitung in der Pflicht ist, den Nachweis der konformen Datenverarbeitung zu erbringen, ist die Aufnahme der zusätzlichen Informationen in das Verzeichnis eigentlich zwingend. Ob die Informationen zur Einwilligung bzw. Berechtigung nun im Verzeichnis der Verarbeitungstätigkeiten oder an anderer Stelle dokumentiert werden, ist letztlich gleich, da in jedem Fall eine Dokumentationspflicht besteht. Die Aufnahme aller zu dokumentierenden Informationen in das Verzeichnis ermöglicht eine strukturierte und kompakte Dokumentation.

3. Wie könnte ein Verzeichnis der Verarbeitungstätigkeiten für einen Hotelbetrieb aussehen?

Im Verzeichnis der Verarbeitungstätigkeiten muss jede einzelne Verarbeitungstätigkeit dokumentiert werden, da je nach verarbeitender Abteilung die betroffenen Personengruppen, Zwecke der Datenverarbeitung, usw. variieren können. Gleichgelagerte Verarbeitungsvorgänge können jedoch zusammengefasst werden. Im Anhang finden Sie ein Musterblatt der Bayerischen Landesdatenschutzbehörde zum Verzeichnis der Verarbeitungstätigkeiten (Anlage 3) mit einer Ausfüllhilfe.

4. Was ist unter einer Datenschutz-Folgenabschätzung zu verstehen?

Die Datenschutz-Folgenabschätzung (Art. 35 und 36 DSGVO) löst die bisherige Vorabkontrolle des BDSG-alt ab. Die Datenschutz-Folgenabschätzung ist eine Prognose hinsichtlich der Belastung der Rechte und Freiheiten einzelner durch alle bestehenden und zukünftigen Datenverarbeitungsvorgänge.

Eine Datenschutz-Folgenabschätzung ist immer dann durchzuführen, wenn im Rahmen einer Risikoabschätzung erkennbar wird, dass die Verarbeitung von Daten „voraussichtlich ein hohes Risiko“ für die Rechte und Freiheiten natürlicher Personen zur Folge hat. In zeitlicher Hinsicht ist die Folgenabschätzung immer dann durchzuführen, wenn die Verarbeitung zum ersten Mal vorgenommen oder grundlegend verändert wird.

Die Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung liegt bei dem für die Datenverarbeitung Verantwortlichen, also dem Hotelbetreiber. Eine vertragliche Übertragung auf den internen oder externen Datenschutzbeauftragten ist möglich. Achten Sie darauf, dass die Folgenabschätzung ausdrücklich dem Tätigkeitsfeld und Verantwortungsbereich des Datenschutzbeauftragten zugeordnet wird.

Die DSGVO enthält keine Definition, was unter einem „voraussichtlich hohen Risiko“ zu verstehen ist, nennt aber in Art. 35 Abs. 3 DSGVO einzelne Beispiele:

- automatisiertes Profiling
- Verarbeitung von Daten besonderer Kategorien wie Gesundheitsdaten
- systematische Überwachung öffentlich zugänglicher Bereiche durch Videokameras

Eine Datenschutz-Folgenabschätzung ist somit immer nötig, wenn Flächen, die allen Gästen im Allgemeinen zugänglich sind - bspw. Hotellobby, Flure zu den Hotelzimmern, Fahrstühle, Restaurants oder der Wellnessbereich - mit Videoüberwachung ausgestattet sind.

Ein weiterer Anhaltspunkt für die Erforderlichkeit einer Datenschutz-Folgenabschätzung sind die zukünftig von den Aufsichtsbehörden nach Art. 35 Abs.4 DSGVO zu führenden Positiv- bzw. Negativlisten. In der Positivliste sind

alle Verarbeitungen aufgeführt, die stets eine Folgenabschätzung erfordern. Ist eine Verarbeitung nicht genannt und besteht keine Negativliste (verbindliche Festlegung der Behörde, dass die konkrete Verarbeitung keine Datenschutz-Folgenabschätzung auslöst), so muss im Einzelfall geprüft werden, ob eine Datenschutz-Folgenabschätzung nötig ist. Bislang liegen allerdings noch keine Positiv- oder Negativlisten vor.

5. Wie erfolgt die Dokumentation einer Datenschutz-Folgenabschätzung?

Der Dokumentationsprozess ist sehr ernst zu nehmen: Die Nichtdurchführung der Datenschutz-Folgenabschätzung erfüllt bereits einen Bußgeldtatbestand.

Zunächst ist eine Risikoabschätzung erforderlich:

- Analyse für jeden einzelnen bzw. die zusammengefassten Datenverarbeitungsvorgänge: Besteht ein Risiko für die Freiheiten und Rechte einzelner durch die jeweilige Datenverarbeitung? Für die Beurteilung zu berücksichtigende Kriterien sind Art, Umfang, begleitende Umstände und Zwecke der konkreten Datenverarbeitung.
- Wie hoch sind die Eintrittswahrscheinlichkeit und die Schwere des zu erwartenden Risikos unter Berücksichtigung der eben genannten Kriterien?
- Gibt es keinen hohen Risikoerwartungswert, so ist eine Datenschutz-Folgenabschätzung nicht nötig. Das Ergebnis dieser Prüfung ist als Nachweis gegenüber den Aufsichtsbehörden zu dokumentieren.

Ist eine Datenschutz-Folgenabschätzung notwendig, dann sind für alle Datenverarbeitungsvorgänge folgende Informationen zu dokumentieren:

- Kategorisieren Sie alle bestehenden gleichartigen Datenverarbeitungsvorgänge anhand des Verzeichnisses der Verarbeitungstätigkeiten des Hotels und nehmen Sie auch alle zukünftig geplanten Datenverarbeitungsvorgänge auf. Es ist nicht erforderlich, für jede einzelne Verarbeitung eine Folgenabschätzung zu erstellen.

- Analysieren Sie, warum Daten in der von Ihnen gewählten Form, trotz hoher Risiken, verarbeitet werden (müssen) und eine für die Rechte einzelner weniger intensive Datenverarbeitung nicht in Betracht kommt.
- Notieren Sie alle Erwägungen, die das Interesse an Ihrem konkreten Vorgehen stützen.
- Dokumentieren Sie detailliert alle technischen und organisatorischen Maßnahmen, die Sie vornehmen, um das Risiko tatsächlich gering zu halten. Es kann nicht von Ihnen verlangt werden, dass Sie Risiken komplett ausschließen können. In der Hotellerie fallen risikobehaftete Datenverarbeitungen zwangsläufig an, bspw. bei der Aufbewahrung von Kreditkarteninformationen. Stellen Sie jedoch sicher, dass alle zumutbaren Schutzmaßnahmen ergriffen werden. Im eben genannten Beispiel ist nur Mitarbeitern der Buchhaltung Zugang zu den in abzusperrenden Schränken abgelegten Kreditkatendaten zu gewähren.
- Bei der Änderung von Datenverarbeitungsverfahren zu einem späteren Zeitpunkt analysieren Sie, ob die neue Form der Verarbeitung mehr oder weniger intensiv für die Rechte und Freiheiten einzelner wirkt. Liegt eine intensivere Belastung vor, muss erneut eine Folgenabschätzung durchgeführt werden.
- Bei Zusammenarbeit mit einem Auftragsverarbeiter hat auch dieser ein Verzeichnis aller durch ihn erfolgenden Verarbeitungstätigkeiten zu erstellen und die Folgenabschätzung durchzuführen.

Tipp für die Praxis:

Die Aufsichtsbehörden stehen als Ansprechpartner für komplizierte Einzelfälle zur Verfügung. Sollten Sie sich nicht sicher sein, ob ein Verarbeitungsvorgang eine Datenfolgenabschätzung erforderlich macht, dann lassen Sie sich von der Aufsichtsbehörde Auskunft geben. Dokumentieren Sie, wann und an wen die Anfrage gestellt wurde, welche Informationen Sie erhalten haben und wie Sie anschließend weiter vorgegangen sind.

6. Checkliste Verzeichnis der Verarbeitungstätigkeit und Datenschutz-Folgenabschätzung

- ☐ Besteht bereits ein Verarbeitungsverzeichnis? Wenn ja, prüfen Sie, ob es um die Anforderungen des Art. 30 DSGVO gegebenenfalls erweitert werden kann.
- ☐ Besteht für Ihr Hotel die Pflicht, ein Verzeichnis zu führen? Wenn nicht, wie wird der dennoch bestehenden Dokumentationspflicht nachgekommen?
- ☐ Wer ist im Betrieb dafür zuständig, das Verzeichnis zu führen und zu aktualisieren?
- ☐ Enthält das Verzeichnis alle Pflichtangeben?
- ☐ Werden fakultative Angaben im Verzeichnis aufgenommen? Falls nicht, wie erfolgt die Dokumentation alternativ?
- ☐ Wurde eine Risikoabschätzung durchgeführt? Ist das Ergebnis dokumentiert?
- ☐ Besteht aufgrund des Ergebnisses der Risikoabschätzung die Pflicht zur Datenschutz-Folgenabschätzung?
- ☐ Wer ist zuständig für die Datenschutz-Folgenabschätzung?
- ☐ Gibt es bislang nicht angewendete und zumutbare technisch-organisatorische Maßnahmen, die Risiken für verarbeitete Daten weiter reduzieren?
- ☐ Gibt es die Möglichkeit technische Grundeinstellungen von Geräten datenschutzärmer zu konfigurieren (privacy by design)?

KAPITEL 7:

Fragen rund um Hotel-Webseiten und Hotel-WLAN

Das folgende Kapitel behandelt die spezifischen Auswirkungen des Datenschutzrechts auf Webseiten. Da die Webseite für jedermann einsehbar ist, sollten datenschutzrechtliche Vorgaben im Rahmen der Datenschutzbestimmungen (siehe Kapitel 7.1) und Einwilligungserklärung für den Newsletter (siehe Kapitel 2.6) besonders aufmerksam und zeitnah umgesetzt werden.

1. Welche Veränderungen bringt das neue Datenschutzrecht für die Datenschutzbestimmungen auf Hotelwebseitenseiten?

Die Hotelwebseite muss eine von jeder Unterseite auffindbare Datenschutzerklärung zur Verfügung stellen. Hierfür genügt ein Link am Ende der Seite.

In der Datenschutzerklärung ist der Nutzer der Webseite in allgemeinverständlicher Form zu unterrichten, wer personenbezogener Daten wie, zu welchem Zweck und in welchem Umfang erhebt und verwendet.

Im Internet finden sich mehrere Webseiten, sog. Datenschutzbestimmung-Generatoren, die bei der Erstellung von Datenschutzbestimmungen herangezogen werden können. Ein überwiegend kostenloses Angebot finden Sie bspw. auf www.e-recht24.de.

Folgende Angaben müssen in den Datenschutzbestimmungen stets enthalten sein:

- Kontaktdaten des Verantwortlichen (Hotelbetriebsgesellschaft)
- Kontaktdaten des Datenschutzbeauftragten
- Alle Zwecke, zu denen personenbezogene Daten verarbeitet werden
- Rechtsgrundlage für die Datenverarbeitung
- Ggf. berechtigte Interessen, die mit der Datenverarbeitung verfolgt werden
- Speicherdauer

- Betroffenenrechte: Hinweis auf Auskunftsrecht und Widerrufsrecht der Betroffenen (siehe Kapitel 8.2 und 8.3)
- Benennung von Dritten innerhalb und außerhalb der EU, an die ggf. Daten übermittelt werden

Abhängig von der Verwendung bestimmter Applikationen, sind auch folgende Angaben in die Datenschutzerklärung einzubinden:

- SSL-Verschlüsselung der Webseite
- Einbindung von verschlüsselten Formularen zur Eingabe personenbezogener Daten
- Hinweis auf Verwendung von Daten für Newsletter
- Hinweis auf Verwendung von Google Dienstleistungen, bspw. Google Maps
- Hinweis auf Social Media-Plugins, bspw. Verwendung des Facebook „Like"-Buttons, Twitter, Instagram, etc.
- Umgang mit Webformularen zur Bestellung eines Newsletters, Kontaktformulare, etc.
- Verwendung von Cookies (hier insbesondere Informationen zu Zweck, Empfänger der Daten etc.) (Wichtig: Hier werden durch die ePrivacy-Verordnung voraussichtlich im Jahr 2020 Veränderungen kommen).
- Verwendung von Analyse-Tools (wie Google Analytics, Piwik oder etracker)

Die Liste ist nicht abschließend.

2. Wann darf die Unternehmenswebseite Cookies auf dem Endgerät des Nutzers setzen?

Aktuell sind die Hinweise zur Verwendung von Cookies in den Datenschutzerklärungen und die Opt-Out Möglichkeiten (aktiver Widerspruch gegen die Verwendung von Cookies) noch ausreichend.

Aller Wahrscheinlichkeit nach muss zukünftig die ausdrückliche Einwilligung zur Verwendung von Cookies eingeholt werden. Dies soll nur für solche Cookies nicht gelten, die zwingend erforderlich sind, um einen Dienst auf der Webseite in Anspruch zu nehmen. Somit sind Cookies für Konfigurationszwecke, die von Hotelwebseiten regelmäßig gesetzten Session-Cookies und für die Waren-

korbfunktion beim Online-Shopping weiterhin ohne ausdrückliche Einwilligung des Webseitenbesuchers erlaubt.

3. Dürfen die IP-Adressen der Webseitenbesucher gespeichert werden?

Bei IP-Adressen handelt es sich um personenbezogene Daten, die zwar gespeichert werden dürfen, aber im Verzeichnis der Verarbeitungstätigkeiten mit dem Zweck der Speicherung aufzuführen sind. In den Datenschutzbestimmungen muss auf die Verarbeitung der IP-Adressen hingewiesen werden.

Die für Hotelseiten verwendeten Content Management Systeme (CMS) bieten standardmäßig die Grundeinstellung an, statt der IP-Adressen der Webseitenbesucher nur den Hash-Wert zu speichern. Hierbei handelt es sich um eine anonymisierte Darstellung der IP-Adresse, die lediglich Rückschluss auf die geographische Lokalisation des Webseitennutzers zulässt.

Tipp für die Praxis:

Sollte in dem für Ihre Hotelwebseite verwendeten CMS bislang noch IP-Adressen gespeichert werden, dann stellen Sie es auf die „datenärmere“ Darstellung des Hash-Werts um („privacy by default“).

4. Darf auf der Unternehmenswebseite automatisch ein Nutzerprofil angelegt werden?

Das Anlegen von Nutzerprofilen auf Webseiten ist nur nach vorheriger ausdrücklicher Zustimmung des Betroffenen zulässig. Hiermit ist nicht das Kundenprofil in der Kundendatei gemeint, sondern ein auch für den Betroffenen sichtbares Nutzerprofil auf der Webseite.

5. Dürfen personenbezogene Daten über den Gast durch das Hotel-WLAN verarbeitet werden?

Nach dem Telemediengesetz dürfen Hotels auf freiwilliger Basis die Nutzer ihres Hotel-WLAN identifizieren, eine Passworteingabe verlangen oder andere

freiwillige Maßnahmen ergreifen. Behörden dürfen Hotels zur Verarbeitung und insbesondere der Speicherung der Daten nicht verpflichten.

Entscheidet sich ein Hotel zur Vergabe von Zugangsdaten, die den Nutzer unmittelbar oder mittelbar identifizieren lassen, dann findet die DSGVO Anwendung und verpflichtet das WLAN-betreibende Hotel zur Aufnahme der Datenverarbeitung in das Verzeichnis der Verarbeitungstätigkeiten und in die Datenschutz-Folgenabschätzung, sowie zu umfänglichen Informationspflichten.

6. Sollten Hotels ihr WLAN weiter mit Passwörtern sichern?

Zwar gilt seit April 2017 nicht mehr die allgemein gefürchtete Störerhaftung in der bisherigen Ausgestaltung, die WLAN-Betreiber aus Sorge vor einer Haftung wegen Rechtsverstöße davon abhielt, ihre Internetzugänge einem unbestimmten Personenkreis freizuschalten. Diese Bedenken sind nach der Änderung des Telemediengesetzes nicht mehr begründet, soweit dargelegt werden kann, dass weitere Personen Zugang zum WLAN hatten. Die Haftung für Hotspot-Betreiber ist vollständig entfallen.

Jedoch sollten auch zukünftig unverschlüsselte WLAN nicht ohne Zugangsbarrieren zur Verfügung gestellt werden, da die Verpflichtung zur Absicherung des WLAN mit Passwörtern sich aus dem Katalog zum § 109 Abs. 1 Telekommunikationsgesetz (TKG) ergibt.

Bei der Wahl der Passwörter sollte nicht auf personenbezogenen Daten der Gäste zurückgegriffen (bspw. Nachname des Gastes bei einer individualisierten Zugangsberechtigung) und den allgemeinen Passwortstandards hinsichtlich Länge und Komplexität entsprochen werden. Werden Passwörter vergeben, die mit Ende des Aufenthaltes des Gastes unwirksam werden, kann ausgeschlossen werden, dass die Daten an Dritte weitergegeben werden, die diese über den Besuch hinaus weiternutzen.

Tipp für die Praxis:

Aus Gründen des Datenschutzes sollten die Zugangsdaten zum WLAN keinen Rückschluss auf den Gast zulassen. Dies wäre der Fall, wenn die Zugangsdaten bspw. Zimmernummer oder Familienname des Gastes enthält.In dem Fall handelte es sich bei den Log-in-Daten um personenbezogene Daten.

Im Optimalfall verwenden Sie einen Passwortgenerator, der eine anonyme Benutzerkennung bzw. anonymes Passwort generiert, dessen Gültigkeit nur den Aufenthaltszeitraum des jeweiligen Gastes umfasst. Wahlweise vergeben Sie dieselben Standardzugangsdaten für alle Gäste.

7. Checkliste Sicherheit von Hotel- Webseiten und Hotel-WLAN

- ☐ Steht den Mitarbeitern ein Ansprechpartner für IT-Sicherheit im Hotel oder extern zur Verfügung?
- ☐ Sind die Gerätesoftware der Laptops, Tablets, Smartphones etc. der Mitarbeiter aktualisiert?
- ☐ Wird auf jedem der Geräte regelmäßig ein Malware-Scanner eingesetzt?
- ☐ Sind die WLAN-Netze für Mitarbeiter und Hotelgäste getrennt?
- ☐ Werden auf der Hotelwebseite automatische Nutzerprofile angelegt? Liegt eine Einwilligung der Betroffenen vor?
- ☐ Sind alle Unterseiten der Hotelwebseite, die Eingabeformulare für personenbezogene Daten enthalten, verschlüsselt?
- ☐ Sind die Mitarbeiter über die Bedeutung von Warnungen der Browser bei SSL-Problemen (unverschlüsselte Internetseiten) geschult?
- ☐ Ist das WLAN mit einem Passwort gesichert? Wird ein einheitliches Passwort regelmäßig geändert?
- ☐ Wird das Passwort durch personenbezogene Daten generiert? Wenn ja, warum ist dies erforderlich? Dokumentation im Verzeichnis der Verarbeitungstätigkeiten erforderlich.
- ☐ Sind die Datenschutzbestimmungen (inklusive der Informationspflichten) der Webseite aktualisiert?
- ☐ Sind die Datenschutzbestimmungen und Nutzungsbedingungen für WLAN-Zugänge aktualisiert?

KAPITEL 8:

Fragen zur Übermittlung von Daten an Dritte

Die Anforderungen der DSGVO an die Datenübermittlung an Dritte sind sehr einzelfallspezifisch. Das folgende Kapitel soll nur Grundzüge dieses Themenbereichs vermitteln, um die Frage der Betroffenheit Ihres Betriebs zu klären. Sollten Sie Daten innerhalb eines Konzerns, dem Sie angehören oder an ein nicht verbundenes Unternehmen in das außereuropäische Ausland weitergeben, dann ist eine Beratung durch einen Spezialisten sehr zu empfehlen.

1. Wer braucht einen EU-Datenschutzvertreter?

Diese Frage betrifft nur Hotels, die Daten an Dritte weitergeben, die ihren Sitz außerhalb der EU haben. Dritter in diesem Sinne wäre ein Konzern, dessen Hauptsitz oder datenverarbeitende Abteilungen außerhalb der EU angesiedelt sind und an den von angehörenden Hotels Daten weitergeben werden.

Die Existenz des EU-Vertreters hängt eng mit dem Marktortprinzip der DSGVO zusammen, wonach das europäische Datenschutzrecht nicht nur für in der Europäischen Union niedergelassene Unternehmen gilt, sondern Anwendung findet, sobald sich ein Angebot an einen bestimmten nationalen Markt in der EU richtet oder die Datenverarbeitung der Beobachtung des Verhaltens von Personen in der EU dient. Der EU-Datenschutzvertreter ist schriftlich zu bestellen und muss in einem Mitgliedsstaat niedergelassen sein.

Allein die Existenz eines EU-Vertreters im empfangenden Unternehmen, bedeutet nicht, dass Daten an das Unternehmen übermittelt werden dürfen. Auch hier gilt, dass ein Erlaubnistatbestand gegeben sein muss, der die Weitergabe der Daten erlaubt. Darüber hinaus sind die Betroffenen vor der Weitergabe ihrer Daten außerhalb der EU zu informieren.

2. Dürfen Daten an zentrale Abteilungen des Hotelunternehmens weitergeben werden?

Die Weitergabe von Daten innerhalb eines Konzerns, der nicht außerhalb der EU niedergelassen ist, wird durch das nun in der DSGVO verankerte kleine Konzernprivileg für Unternehmensgruppen unkomplizierter möglich. Die DSGVO führt an, dass ein berechtigtes Interesse an der Weitergabe von personenbezogenen Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, bestehen kann.

Unternehmensgruppe ist definiert als „Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht“. Ein Unternehmen „herrscht“, wenn es „aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann“. Dies ist auch der Fall, wenn ein Unternehmen die Verarbeitung personenbezogener Daten in einem ihm angeschlossenen Unternehmen kontrolliert.

Diese Situation ist regelmäßig in einem Konzern im Sinne des Aktiengesetzes (AktG) gegeben. Aber auch bei anders ausgestalteten Zusammenschlüssen von Hotels sind die Voraussetzungen gegeben, wenn

- der Verantwortliche Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen ist, die einer zentralen Stelle zugeordnet werden und
- personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, übermittelt werden.

Eine Unternehmensgruppe genießt folgende Privilegierungen:

- Möglichkeit eine gemeinsamen Datenschutzbeauftragten („Konzerndatenschutzbeauftragten“) zu bestellen
- Abwägung der berechtigten Interessen weiter erforderlich, aber Verwaltungszwecke können als legitime Zwecke gelten.

3. Checkliste zur Übermittlung von Daten an Dritte

- ☐ Werden Daten an Dritte außerhalb der EU weitergeleitet? Wenn ja, hat die empfangende Stelle einen Datenschutzvertreter? Sind Kontaktdaten dieser Person im Verzeichnis der Verarbeitungstätigkeiten genannt? Erfolgte eine Beratung durch einen Spezialisten?
- ☐ Wenn Daten an Dritte innerhalb oder außerhalb der EU weitergeleitet werden, auf welcher Rechtsgrundlage ist die Weiterleitung erlaubt? Ist die Rechtsgrundlage im Verzeichnis der Verarbeitungstätigkeiten genannt?
- ☐ Werden Daten an zentrale Abteilungen innerhalb eines Konzerns weitergegeben? Sind Ansprechpersonen im Verzeichnis der Verarbeitungstätigkeiten genannt?

KAPITEL 9:

Fragen rund um Anfragen von Behörden, Verbänden und Dritten

Das von der DSGVO statuierte Transparenzgebot verpflichtet Betriebe zur Information über die Verarbeitung von personenbezogenen Daten. Der Umfang der zu übermittelnden Informationen hängt davon ab, ob eine Behörde oder Betroffene selbst die Anfrage gestellt hat.

1. Wer darf Auskunft über die Datenverarbeitung verlangen?

Die Datenschutzbeauftragten der Länder sind eine eigenständige Behörde in allen Bundesländern und sind zu Auskunftsanfragen sowie zur Verhängung von Sanktionen und von sanktionslosen Verwarnungen berechtigt. Neben der Privatperson, deren Daten verarbeitet wurden, gibt die DSGVO auch Verbänden die Möglichkeit, aus eigenem Recht Anfragen an Unternehmen zu richten. Es bedarf somit keiner Aufforderung oder Beschwerden seitens des Verbrauchers für ein Tätigwerden.

Die Verbraucherschutzverbände dürfen aus eigenem Recht in allen Fällen kommerzieller Nutzung von Daten tätig werden, insbesondere bei nicht datenschutzkonformer Nutzung der Daten zu Werbezwecken, unberechtigt angelegter Profile oder Adressweitergabe. Sie sind neben der Durchsetzung von Auskunftsansprüchen auch berechtigt, Schadensersatzforderungen von Verbrauchern einzuklagen. Die DSGVO sieht allerdings kein eigenes Auskunftsrecht für Verbraucherschutzverbände vor.

Tipp für die Praxis:

Sichern Sie sich ab und geben Sie am Telefon keine Auskunft zu verarbeiteten Daten. Sollte es zu einer telefonischen Anfrage einer Behörde oder Verbraucherschutzverbands kommen, wird Missbrauch verhindert, indem Sie auf ein schriftliches Auskunftsersuchen mit Angabe der Rechtsgrundlage für die Auskunft bestehen.

2. Was ist unter dem Informationsrecht nach der DSGVO zu verstehen?

Die DSGVO unterscheidet zwei Ansprüche auf Information:

- Vorabinformation: welche Daten für welchen Zweck und auf welcher Rechtsgrundlage verarbeitet werden sowie
- Nachträglicher Informationsanspruch: welche Daten für welchen Zweck und auf welcher Rechtsgrundlage verarbeitet wurden.

Letzterer besteht nur, solange die Daten beim Verarbeiter gespeichert werden und setzt eine schriftliche Anfrage der Betroffenen voraus. Die Vorabinformation ist den Betroffenen in den Datenschutzbestimmungen auf der Webseite bzw. im Rahmen des zu schließenden Vertrages zu gewähren.

3. Welche Daten müssen im Falle einer Anfrage übermittelt werden?

Auf Nachfrage kann der Betroffene erfahren, welche Daten zu seiner Person im Hotel verarbeitet wurden. Das Informations- bzw. Auskunftsrecht umfasst nur personenbezogene Daten des Anfragenden. Es dürfen somit keine Daten übermittelt werden, die sich auf eine weitere Person beziehen. So sind einem Anfragenden nicht die verarbeiteten Daten zu der Person, mit der bspw. ein Hotelzimmer geteilt wurde, mitzuteilen. Dass die Gäste möglicherweise verheiratet oder verwandt sind, ändert daran nichts.

Der Verantwortliche hat folgende Informationen zur Verfügung zu stellen:

- Welche Daten wurden verarbeitet?
- Wie wurden Daten verarbeitet?
- Zu welchem Zweck wurden Daten verarbeitet?
- Woher stammen die verarbeiteten Daten?
- Werden Daten an einen Dritten übermittelt? Wenn ja, an wen?

Das Auskunftsrecht umfasst alle Daten, die im Zeitpunkt der Anfrage noch verarbeitet werden und kann sich auf alte Sachverhalte beziehen (vor dem Inkrafttreten der DSGVO). Nicht mitgeteilt werden muss auf welche Rechtsgrundlage die Verarbeitung der Daten gestützt wird.

Die Daten sind in einem gängigen, maschinenlesbaren Format (bspw. in einem Word- oder Excel-Dokument) innerhalb von einem Monat nach Eingang der Anfrage zu übermitteln. Die durch die Anfrage verursachten Kosten können dem Anfragenden nicht in Rechnung gestellt werden, da die DSGVO einen Anspruch auf eine kostenlose Auskunft über die verarbeiteten Daten vorsieht.

Tipp für die Praxis:

Anfragen von Gästen zu verarbeiteten personenbezogenen Daten müssen ernst genommen werden. Da Sie bislang womöglich nicht abschätzen können, wieviele Anfragen zu verarbeiteten Daten Sie ab dem 25. Mai 2018 erreichen, ist es empfehlenswert, zunächst Anfragen händisch zu beantworten. So kann besser eingeschätzt werden, ob sich die Kosten einer Softwarelösung hier rentieren.

4. Wie wird sichergestellt, dass der Anfragende tatsächlich die Person ist, als die er sich ausgibt?

Personenbezogene Daten dürfen nur an den Betroffenen selbst übermittelt werden. Die Weitergabe an eine sich lediglich als der Betroffene ausgebende Person würde bedeuten, dass ohne Einwilligung des Betroffenen Daten an

einen Dritten weitergeben werden. Dennoch sieht das Gesetz nicht vor, dass der Anfragende sich ausweist.

Sie müssen sich hinsichtlich der Identität des Anfragenden nur rückversichern, wenn es Anhaltspunkte für ein missbräuchliches Vorgehen gibt. Zur Wahrung der Privatsphäre Ihrer Gäste sollten Sie keine mündlichen Auskunftsanfragen akzeptieren.

5. Checkliste zu Auskunfts- und Informationsrechten

- ☐ Sind die Datenschutzbedingungen auf der Hotelwebseite aktualisiert? Sind die Datenschutzbedingungen von jeder Unterseite der Webseite aufrufbar?
- ☐ Wird das Informationsrecht der Betroffenen auf Vorabinformation, welche personenbezogene Daten zu welchem Zweck verarbeitet werden, auf der Webseite und in Vertragsdokumenten erfüllt?
- ☐ Werden Betroffene leicht verständlich auf ihr Recht zu Auskunft, Widerspruch und Löschen in Verträgen und auf der Webseite hingewiesen?
- ☐ Ist der Datenschutzbeauftragte als Ansprechperson in den Datenschutzbestimmungen genannt?
- ☐ Wer ist im Hotelbetrieb verantwortlich für die Beantwortung etwaiger Anfragen und Bearbeitung von Widersprüchen gegen die Verarbeitung von Daten?
- ☐ Ist auf der Webseite eine Ansprechperson für Betroffene genannt, die Auskunft über bereits verarbeitete personenbezogene Daten (nachträglicher Informationsanspruch) geben kann?
- ☐ Ist der verantwortliche Mitarbeiter geschult, welche Daten unter welchen Umständen übermittelt werden dürfen?
- ☐ Bestehen standardisierte Vorlagen zur schnellen und umfassenden Beantwortung von Anfragen Betroffener?
- ☐ Ist den regelmäßig personenbezogene Daten verarbeitenden Mitarbeitern eine Ansprechperson bei der Aufsichtsbehörde bekannt?
- ☐ Ist sichergestellt, dass der Aufsichtsbehörde im Falle einer Anfrage, unverzüglich das Verzeichnis der Verarbeitungstätigkeiten oder eine andere Form der Dokumentation übermittelt werden könnte?

KAPITEL 10:

Fragen zum Löschen von Daten

Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten jederzeit widersprechen und die Löschung verlangen („Recht auf Vergessen“). Wird die Löschung begehrt, stellt sich für den Hotelier die Frage, ob die Daten tatsächlich gelöscht werden können oder lediglich eine Sperrung der Daten für die kommerzielle Nutzung in Betracht kommt.

1. Inwieweit muss der Aufforderung zur Sperrung oder zum Löschen nachgekommen werden?

Wenn dem Betroffenen nach einer Anfrage die verarbeiteten Daten übermittelt werden, muss nicht gleichzeitig die Sperrung der Daten angeboten werden. Sollte der Betroffene in einer anschließenden Mitteilung an das Hotel zum Sperren oder Löschen auffordern, ist zu differenzieren:

- Der Betroffene darf die Löschung seiner Daten aus E-Mail-Verteilern und Datenbanken zu Werbezwecken jederzeit verlangen.
- Eine vollständige Löschung aller Daten scheidet aus, wenn Vorschriften aus dem Handels- und Steuerrecht entgegenstehen. So sind bspw. Kaufverträge und die sich aus ihnen ergebenden Daten für 10 Jahre aufzubewahren. Eine Verwendung der Daten für einen anderen Zweck ist dann selbstverständlich ausgeschlossen und wird durch einen Sperrvermerk in der Datenbank sichergestellt.
- Die weitere Verarbeitung der Daten ist nicht erlaubt, außer es kommt bspw. eine Anonymisierung in Betracht: Die Eingaben einer Kundenzufriedenheitsbefragung könnten somit weiterverarbeitet werden, jedoch müssen die Kontaktdaten des Gastes gelöscht werden.
- Wurden die personenbezogenen Daten an Dritte weitergegeben, so muss der weitergebende Verantwortliche auch diese Stellen informieren, dass die Daten gesperrt oder gelöscht werden sollen.

Darüber hinaus sind Daten unabhängig von einer Aufforderung seitens des Betroffenen zu löschen, wenn die Rechtsgrundlage der Verarbeitung nicht mehr fortbesteht. Zur systematischen Erfassung, wann welche Datensätze zu löschen sind, bedarf es eines Löschkonzepts, welches Bestandteil des Verzeichnisses der Verarbeitungstätigkeiten ist.

2. Wie erarbeitet man ein Löschkonzept?

Das Löschkonzept ist einer der größten Herausforderungen des neuen Datenschutzrechts. In der Regel richtet sich die Löschung nach dem Zweck der Datenerhebung und -nutzung. Daten sind somit in folgenden Fällen zu löschen:

- Der Zweck der Datenverarbeitung ist erfüllt.
- Der Betroffene verlangt die Löschung seiner Daten.
- Spezialgesetzliche Aufbewahrungspflichten, zum Beispiel aus dem Steuerrecht oder sonstigen branchenspezifischen Rechtsvorschriften, sind abgelaufen.

Die Erstellung und Umsetzung eines Löschkonzeptes stellt die Hotellerie in der Praxis vor mehrere große Herausforderungen:

- Das Hotel kann Daten aufgrund mehrerer unterschiedlicher Zwecke verarbeitet werden. Vor der Löschung sollte geprüft werden, ob tatsächlich alle Zwecke der Datenverarbeitung erfüllt sind. Dies gelingt durch die präzise Dokumentation aller Verarbeitungszwecke und frühesten Zeitpunkte zum Löschen im Verzeichnis der Verarbeitungstätigkeiten. Hierfür müssen alle datenverarbeitenden Hotelabteilungen wie etwa IT, Human Resources, Recht, Sales, Marketing und interne Revision, evaluieren, welche Daten sie verarbeiten und wann der Datensatz gelöscht werden kann.
- Das Löschen eines Datensatzes aus einer Datenbank entfernt die Daten nicht aus dem Backup-System. Eine Löschung eines einzelnen Datensatzes aus dem Backup-System ist regelmäßig nicht möglich, da derartige Datensicherungssysteme bislang gerade darauf ausgerichtet sind, vollständige Inhalte der Datenverarbeitungen zu sichern. Die DSGVO verpflichtet Unternehmen widersprüchlicher Weise sogar die Verfügbarkeit personenbezoge-

ner Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wieder herzustellen, was nur durch Backups technisch möglich sein wird.

- Im Verzeichnis der Verarbeitungstätigkeiten sollten alle absehbare Verarbeitungszwecke dokumentiert werden. Zu denken ist insbesondere an die Wahrung berechtigter Interessen des Unternehmens: Personenbezogene Daten können bspw. zur Geltendmachung oder Verteidigung von Rechtsansprüchen im Arbeitsverhältnis erforderlich sein und eine lange Speicherdauer rechtfertigen.

Als Teil des Verzeichnisses der Verarbeitungstätigkeiten sollten die Löschfristen bei jeder Dokumentation von Verarbeitungstätigkeiten bereits am Anfang festgelegt werden. Die längsten Fristen mit zehn Jahren Dauer sind vom Handels- und Steuerrecht vorgesehen.

Bei Fristen ist die Vorhalte- und Aufbewahrungsfrist zu unterscheiden. Die Vorhaltefrist bezieht sich auf die Zeit, in der die Daten aus betrieblichen Gründen noch in dem betreffenden Verfahren vorgehalten werden müssen. Die Aufbewahrungsfrist bezieht sich auf die Zeit, in der Daten aus gesetzlichen oder vertraglichen Gründen im Unternehmen verfügbar gehalten werden müssen. Hierdurch müssen Daten mitunter aus einzelnen Verfahren frühzeitiger gelöscht werden, während dieselben Daten an anderer Stelle zum Zwecke der Aufbewahrung langfristig abgelegt werden müssen. Das Löschkonzept organisiert die unterschiedlichen Löschfristen je nach Zweck der Speicherung.

3. Checkliste zum Löschen von Daten

- ☐ Sind die ggf. unterschiedlichen Aufbewahrungs- und Löschfristen (abhängig vom jeweiligen Verarbeitungszweck) für alle Datenkategorien dokumentiert und auf regelmäßige Wiedervorlage gesetzt?
- ☐ Besteht eine interne Richtlinie (Löschkonzept), wann Daten nach Wegfall des Zwecks der Datenerhebung gelöscht werden?
- ☐ Sind die Zuständigkeiten für den Löschvorgang geregelt?
- ☐ Wie werden nach Widerspruch des Betroffenen gegen die Verwendung der Daten Sperrvermerke in der Datenbank umgesetzt?
- ☐ Wenn Betroffene die Löschung ihrer personenbezogenen Daten verlangt und die personenbezogenen Daten zuvor an Dritte weitergegeben wurden, ist dann ein Verfahren vorgesehen, wie der weitergebende Verantwortliche auch diese Stellen informieren, dass die Daten gelöscht werden sollen?

KAPITEL 11:

Umgang mit Datenschutzverletzungen

Die DSGVO verpflichtet den Verantwortlichen innerhalb 72 Stunden nach Bekanntwerden der Panne die Datenschutzverletzung der Aufsichtsbehörde zu melden.

1. Was ist unter einer Datenschutzverletzung bzw. Datenpanne zu verstehen?

Eine Verletzung des Datenschutzes bzw. eine Datenpanne nach dem Verständnis der DSGVO liegt vor, wenn im Macht- und Verantwortungsbereich des Verantwortlichen alternativ

- Daten verloren gehen
- Daten unberechtigt verändert wurden
- unberechtigten Personen bekannt gegeben wurden
- unberechtigten Personen Zugang gewährt wurde

Ob die Datenrechtsverletzung versehentlich oder mit Wissen des Verantwortlichen geschah, ist unerheblich. Relevant ist dabei lediglich, dass es sich bei den verletzten Daten um solche personenbezogener Art handelt.

Sollte es in einem Unternehmen zu einer Verletzung des Datenschutzrechts kommen, ergeben sich daraus für den Datenschutzbeauftragten oder Verantwortlichen folgende Verpflichtungen:

- Meldepflichten gegenüber der Aufsichtsbehörde und den Betroffenen
- Dokumentationspflichten über Art, Umfang der Datenpanne
- Behebung des Datenlecks und Maßnahmen zur Schadensbegrenzung
- Überarbeitung der Datenschutzinfrastruktur und Dokumentation der Änderungen

2. Wie ist der Meldepflichten gegenüber der Aufsichtsbehörde und Betroffenen nachzukommen?

Sollte es im Betrieb oder bei einem Auftragsverarbeiter zur Datenpanne gekommen sein, ist dies der zuständigen Aufsichtsbehörde unverzüglich, d.h. ohne schuldhaftes Zögern, zu melden. Die DSGVO geht hierfür von einem Zeitfenster von maximal 72 Stunden nach Bekanntwerden der Verletzung aus.

Sollte die Meldung zu einem späteren Zeitpunkt erfolgen, ist eine Begründung für die Verzögerung zu empfehlen, da ein Verstoß gegen die Meldepflicht für die Höhe möglicher Bußgelder maßgeblich ist.

Besteht auch ein hohes Risiko für die persönlichen Rechte oder Freiheiten der Betroffenen, bspw. Vermögen, so sind auch diese direkt zu benachrichtigen oder bei einem großen Betroffenenkreis durch öffentliche Bekanntmachung in Kenntnis zu setzen.

Eine Meldung an die Aufsichtsbehörde oder die Betroffenen sollte folgende Informationen umfassen:

- Kontaktinformationen des Datenschutzbeauftragten und des Unternehmensinhabers
- Konkretisierung der Art der Datenschutzverletzung
- Angabe der Kategorien der verletzen Daten
- Angabe der Anzahl der betroffenen Personen (Schätzwert ausreichend)
- Angabe der Zahl der betroffenen Datensätze (Schätzwert ausreichend)
- Beschreibung des wahrscheinlichen Folgerisikos durch die Panne
- Beschreibung der Maßnahmen zur unmittelbaren Behebung oder Abmilderung der Datenpanne
- Konkretisierung der bereits erfolgten oder vorgesehenen Überarbeitung der Datenschutzinfrastruktur

Eine Meldung an die Behörden ist nicht erforderlich, wenn aller Voraussicht nach durch die Datenpanne kein Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Für die Beurteilung ist eine Risikobewertung anhand folgender Kriterien vorzunehmen:

- Sind verschlüsselte oder unverschlüsselte Daten betroffen?
- Sind Abhilfemaßnahmen ergriffen worden, die das Risiko auf ein vernachlässigbares Restrisiko reduzieren konnten?
- Risiko von Straftaten durch die verletzten Daten (bspw. Betrug, Identitätsdiebstahl)
- Finanzieller Schaden zu Lasten der Betroffenen
- Persönlichkeitsverletzung durch besonders sensible Informationen (bspw. Imageverlust, Rufschädigung)

Die Risikobewertung ist als gegebenenfalls später hilfreicher Nachweis gegenüber den Behörden zu dokumentieren.

3. Checkliste Umgang mit Datenschutzverletzungen

☐ Wer ist im Hotel zuständig, Datenschutzverletzungen an die Aufsichtsbehörden zu melden?

☐ Ist gewährleistet, dass eine Meldung innerhalb von 72 Stunden nach Kenntnis von der Datenpanne erfolgt?

☐ Wurde im Hotel ermittelt, an welchen Stellen der Datenverarbeitung ein beachtliches Risiko für Datenschutzverletzungen besteht?

☐ Gibt es geeignete Methoden, Datenpannen im Hotel zeitnah aufzuspüren?

☐ Sind Mitarbeiter geschult, wie sie sich bei Datenschutzverletzungen zu verhalten haben?

KAPITEL 12:

Fragen zum Arbeitnehmerdatenschutz

Im Arbeitsrecht bringt das neue Datenschutzrecht nur einige wenige Veränderungen. Maßgeblich sind hier nicht die DSGVO, sondern die konkreteren und präziseren Vorschriften des BDSG-neu.

1. Welche Daten dürfen von Mitarbeitern erhoben werden?

Das Datenschutzrecht sieht drei Konstellationen vor, die den Arbeitgeber zur Verarbeitung von Daten ermächtigen:

- Erlaubnis aufgrund eines Gesetzes
- Einwilligung des Betroffenen
- Tarif-, Betriebs- und Dienstvereinbarungen
- Interessensabwägung, wobei berechtigte Interessen des Arbeitnehmers nicht entgegenstehen dürfen.

Gemäß § 26 BDSG-neu darf der Arbeitgeber alle Daten der Beschäftigten erheben, die für die Entscheidung

- über die Begründung eines Beschäftigtenverhältnisses oder nach Begründung des Beschäftigungsverhältnisses
- für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

Dies umfasst insbesondere alle Informationen zu

- Qualifizierung inklusive Arbeitszeugnisse
- Daten zur Identifizierung (z.B. Personalausweisnummer, Geburtsdatum) und Personenstand

2. Welche Anforderungen muss eine Einwilligung im Arbeitsverhältnis erfüllen?

Eine weitergehende Datenverarbeitung ist mit Einwilligung des betroffenen Arbeitnehmers möglich. Besonders zu beachten ist hier das Erfordernis der Freiwilligkeit, da sich der Arbeitgeber in einem Abhängigkeitsverhältnis zum Arbeitgeber befindet.

Freiwilligkeit darf immer unterstellt werden, wenn durch die Datenverarbeitung für den Arbeitnehmer ein rechtlicher oder wirtschaftlicher Vorteil erlangt wird oder Arbeitgeber und Arbeitnehmer gleichgelagerte Interessen vertreten. Eine Einwilligung, die nur einseitig dem Arbeitgeber dient, ist unwirksam.

Hinsichtlich der Formalien der Einwilligung gelten im Arbeitsverhältnis strengere Vorschriften: Die Einwilligung muss schriftlich eingeholt werden. Darüber hinaus ist der Arbeitgeber verpflichtet, den Arbeitnehmer über den Zweck der Datenerhebung und das Widerrufsrecht aufzuklären.

Personenbezogene Daten besonderer Kategorien (siehe Kapitel 1.3) dürfen nur erhoben werden, wenn dies zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht notwendig ist. Dies ist der Fall, wenn Daten zur Gewährleistung des Gesundheitsschutzes des Arbeitnehmers erforderlich sind.

3. Wann sind Daten von ausgeschiedenen Mitarbeitern oder abgelehnter Bewerber zu löschen?

Die Unterlagen abgelehnter Bewerber muss der Verantwortliche für drei bis sechs Monate aufbewahren, um Ansprüche aus dem Allgemeinen Gleichbehandlungsgesetz abwehren zu können.

Für arbeitsrechtliche Unterlagen ehemaliger Mitarbeiter gilt die allgemeine Aufbewahrungspflicht von 10 Jahre. Es handelt sich hierbei um Steuerunterlagen, die von der Finanzverwaltung und sonstigen Sozialträgern noch geprüft werden können müssen.

Die Daten sind in beiden Fällen so aufzubewahren, dass Dritte, insbesondere auch andere Mitarbeiter, keinen Zugang zu den Daten haben.

4. Welche Auswirkungen hat der Datenschutz im Rahmen von Bewerbungsverfahren?

Viele Hotels nutzen ihre Webseite zur Mitarbeitergewinnung. Eine Kontaktformular oder die Angabe der Kontaktdaten der HR-Abteilung bspw. E-Mail-Adresse sind die gängige Form. Dabei sind folgende Punkte zu beachten:

- Achten Sie darauf, dass Unterseiten mit Kontaktfeldern zur Eingabe von personenbezogenen Daten verschlüsselt sind.
- Bieten Sie bereits auf der jeweiligen Unterseite einen Link zu den Datenschutzinformationen an. Alternativ senden Sie dem Bewerber nach Erhalt der Bewerbungsunterlagen Ihre Datenschutzbestimmungen zum Umgang mit Bewerberdaten zu.
- Informieren Sie den Bewerber, welche Daten wie lange auch nach Abschluss des Bewerbungsverfahrens gespeichert werden. Die Speicherung der Daten von Bewerbern, mit denen kein Arbeitsvertrag eingegangen wurde, ist dabei ebenso erforderlich, um Ansprüche nach dem Allgemeinen Gleichbehandlungsgesetz abzuwehren.

5. Darf der Arbeitgeber Videokameras zur Überwachung der Arbeitsleistung der Arbeitnehmer sowie zur Verhinderung von Straftaten, begangen durch Arbeitnehmer, einsetzen?

Der deutsche Gesetzgeber hat sich die vorhandene Öffnungsklausel der DSGVO zu Nutze gemacht und für die Videoüberwachung in öffentlichen Bereichen in § 4 BDSG verschärfte Grenzen gesetzt. Demnach ist die Videoüberwachung von Arbeitsplätzen in öffentlich zugänglichen Räumen, bspw. solchen von Servicekräften im Restaurant oder Rezeptionisten in der Hotellobby, zulässig, wenn dies der Wahrnehmung

- des Hausrechts oder
- berechtigter Interessen für konkret festgelegte Zwecke

dient. Schutzwürdige Interessen der Arbeitnehmer und Gäste dürfen das Interesse des Arbeitgebers dabei nicht überwiegen:

- Vor der Installation der Videokameras ist eine Datenschutz-Folgenabschätzung vorzunehmen. Insbesondere die Zugriffsberechtigung auf die gespeicherten Aufzeichnungsdaten ist zu regeln.
- Die Videoaufzeichnungen ist eine Datenverarbeitung und ist im Verzeichnis der Verarbeitungstätigkeiten zu führen.
- Auf die Videoüberwachung ist durch geeignete Schilder in den öffentlichen Räumen hinzuweisen.

Wichtig: Videokameras dürfen nicht zur Überwachung der Arbeitsleistung des Arbeitnehmers eingesetzt werden. Erlaubt wäre lediglich eine Überwachung der Einrichtung zur Erfassung der Arbeitszeit durch Videokameras zur Betrugsprävention.

Datenerhebung zur Aufdeckung und Verhinderung von Straftaten ist dem Arbeitgeber nur erlaubt, wenn bereits tatsächliche Anhaltspunkte vorliegen, die den Verdacht von im Betrieb begangenen Straftaten begründen. Ein Verdacht liegt noch nicht bei einer bloßen Vermutung bzw. Hypothese, dass Straftaten begangen werden könnten, vor.

Wenn ein Verdacht gegeben ist, dann steht der Einsatz von Videokameras weiter unter dem Vorbehalt der Verhältnismäßigkeit: Bei einer Abwägung der Interessen (Eigentums- und Vermögensschutz des Arbeitgebers vs. Allgemeines Persönlichkeitsrecht des Arbeitnehmers) darf das Interesse des Arbeitnehmers nicht überwiegen. Ein Überwiegen wäre denkbar bei Videoüberwachung in Fällen sehr geringen Schadens bspw. Diebstahl von Büroklammern, einzelnen Kugelschreibern.

Ist eine Videoüberwachung erforderlich, dann sind die Erwägungsgründe zwingend im Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren und eine Datenschutz-Folgenabschätzung durchzuführen.

6. Unterfallen auch Betriebsräte den Vorschriften der DSGVO?

Entgegen der bisherigen Grundsätze des Bundesarbeitsgerichts muss sich künftig auch die Datenverarbeitung durch Betriebsräte an den Maßstäben des Datenschutzrechts messen lassen. Die Regelungen des Betriebsverfassungsgesetzes werden durch die DSGVO nicht verändert.

Für Betriebsräte und andere Arbeitnehmervertretungen bestehen folgende Verpflichtungen:

- Personenbezogene Daten von Arbeitnehmern dürfen Betriebsräte auch zur Erfüllung von Vorgaben des Betriebsverfassungsgesetzes nur noch auf Grundlage einer umfassenden Interessenabwägung verarbeiten
- Gleiches gilt für Rechte oder Pflichten aus Kollektivvereinbarungen.

7. Sind Tarif-, Betriebs- und Dienstvereinbarungen zum Datenschutz zulässig?

Vereinbarungen zur Regelung der Verarbeitung personenbezogener Daten von Beschäftigten sind weiter möglich. Dies umfasst Daten für die Zwecke der Einstellung, Daten für die Organisation der Arbeit und Daten, die die Gesundheit und Sicherheit am Arbeitsplatz betreffen.

Dabei müssen jedoch die Vorgaben der DSGVO eingehalten werden:

- Entgegen der früheren Praxis sind von nun an für Arbeitnehmer nachteilig abweichende Regelungen zum Datenschutz nicht mehr möglich. Die DSGVO legt den Mindeststandard fest.
- Transparenz der Verarbeitung: Arbeitnehmer sind zu informieren, zu welchen Zwecken ihre Daten verarbeitet werden.
- Es gelten die gleichen Anforderungen bei der Datenverarbeitung: Pflicht zum Führen des Verzeichnisses der Verarbeitungstätigkeiten und Durchführung einer Datenschutz-Folgenabschätzung
- Geltung aller in Art. 5 DSGVO festgelegten Datenschutzprinzipien

Diese Anforderungen gelten auch für alle bereits bestehenden Betriebsvereinbarungen. Entsprechend sind eine zeitnahe Anpassung der Vereinbarungen

zum Datenschutzrecht und die zukünftige Einhaltung der Mindeststandards erforderlich.

8. Checkliste zum Arbeitnehmerschutz:

- Welche personenbezogenen Daten besonderer Kategorien von Arbeitnehmern und Bewerbern werden verarbeitet?
- Ist ein besonderer Schutz für besondere Kategorien personenbezogener Daten gewährleistet?
- Auf welcher rechtlichen Grundlage werden Daten von Arbeitnehmern verarbeitet?
- Liegt eine schriftliche, rechtskonforme Einwilligung der Arbeitnehmer vor?
- Sind Betriebsvereinbarungen zum Datenschutz aktualisiert?
- Wie werden Unterlagen mit Daten zu Arbeitnehmern und Bewerbern aufbewahrt?
- Wer hat aktuell Zugang zu Arbeitnehmer- und Bewerberdaten? Ist eine restriktivere Zugangsregelung möglich?
- Wie ist sichergestellt, dass online eingereichte Bewerbungsunterlagen mindestens den gleichen Schutz wie Bewerbungsunterlagen in Papier erhalten? Besteht ein entsprechender Zutrittsschutz und Zugangsschutz?
- Ist die Unterseite, auf der Bewerbungen online eingereicht werden können, verschlüsselt?
- Werden Bewerber bei Online-Bewerbungen über Art und Umfang der Verarbeitung ihrer Daten informiert? Sind die Datenschutzbedingungen entsprechend aktualisiert?
- Sind die Mitarbeiter zu Auskunftsrecht, Widerspruchsrecht und Recht auf Löschen der Arbeitnehmer und Bewerber geschult?

- Ist die Löschung der Bewerberdaten und Daten ausgeschiedener Arbeitnehmer geregelt?
- Sind die Löschfristen im Verzeichnis der Verarbeitungstätigkeiten dokumentiert?
- Wurde die Vereinbarung zur Auftragsverarbeitung durch eine evtl. E-Recruiting-Plattform überprüft?
- Ist der Betriebsrat über die datenschutzrechtlichen Neuerungen informiert?

KAPITEL 13:

Praktische Hinweise zur Umsetzung von Datenschutz

Datenschutz lässt sich manchmal bereits mit wenigen Handgriffen erreichen. Im Folgenden werden praktische Maßnahmen für die einzelnen Hotelbereiche genannt, die den Datenschutz kostengünstig und effizient verbessern. Datenschutz lässt sich letztlich nur vollumfänglich gewährleisten, wenn der Verantwortliche eine Datenschutzinfrastruktur etabliert, die das Hotel in seiner Gesamtheit umfasst.

1. Wie werden Zutrittskontrollen in der Hotellerie umgesetzt?

Daten sind nicht nur durch einen Hackerangriff gefährdet. Oftmals kommt es zu datenschutzrechtlichen Zwischenfällen, indem z.B. sensible Daten von Unberechtigten auf einen USB-Stick gespeichert oder in Papierform ausgedruckt werden. Umfassender Datenschutz bedeutet gerade auch, dass physische Barrieren geschaffen werden, um Daten zu schützen.

Zutritts- und Zugangskontrollen sind ein essentieller Schritt, den Zugang zu personenbezogenen Daten zu regeln und im Falle einer Datenpanne zu rekonstruieren, wer möglicherweise auf die Daten zugegriffen hat.

Folgende Schritte sind dabei zu beachten:

- Dokumentieren Sie, welcher Mitarbeiter welche Rechte eingeräumt bekommen hat: Nicht jeder Mitarbeiter des Hotels benötigt den Zugang zur Datenbank. Wenn die Anzahl der Mitarbeiter, die Zugriff auf Daten haben, reduziert wird, wirkt sich dies auch auf das Risiko eines Datenverlusts aus.
- Sichern Sie datensensible Räume mit einen separaten Schloss, besser noch einem personalisierten Chip: So stellen Sie sicher, dass nur die Personen, die wegen ihrer Arbeitsaufgaben Zugang zum Raum der IT-Abteilung inklusive Serverraum, Dokumentenarchiv, Personalabteilung und Buchhaltung benötigen, auch in diese Räume gelangen.

- Externe Dienstleister wie bspw. Handwerker haben sich an der Rezeption anzumelden und sollten ein sichtbares Kennzeichen ihrer Autorisation tragen, bspw. Hausausweis. So stellen Sie sicher, dass unberechtigte Personen mit dem Anschein eines Handwerkers sich nicht im Hotel aufhalten.

2. Welche Maßnahmen verbessern den Datenschutz an der Rezeption?

An der Rezeption werden einige datenschutzrelevante Vorgänge abgewickelt, die besondere Sicherungsvorkehrungen erforderlich machen.

- Bei der Standortwahl des Bildschirms ist darauf zu achten, dass nur die Mitarbeiter der Rezeption die angezeigten Daten sehen können, nicht hingegen der Gast oder externe Dienstleister.
- Hält sich das Rezeptionspersonal nicht am Empfang auf, sollte bereits nach einem kurzen Zeitraum der Bildschirm automatisch vor unberechtigten Blicken geschützt werden. Dies gelingt durch einen sich nach einem kurzen Zeitfenster einschaltenden Bildschirmschoner. Der Bildschirmschoner setzt die Schwelle höher, dass Unberechtigte spontan ein Blick auf den Schirm werfen können, sollten diese den Bildschirm zu sich drehen. Ein individualisierter Bildschoner kann den Mitarbeiter zeitgleich daran erinnern, sich abzumelden, wenn der Arbeitsplatz länger verlassen wird.
- Ausgefüllte Meldescheine, eingegangene Post oder sonstige Dokumente mit personenbezogenen Informationen sind für Publikumsverkehr nicht offen sichtbar an der Rezeption aufzubewahren, sondern in einer im Optimalfall verschließbaren Schublade.

3. Welche Maßnahmen verbessern den Datenschutz in der Personalabteilung und Buchhaltung?

In der Personalabteilung und Buchhaltung werden die sensibelsten Daten im Hotel verarbeitet. Entsprechend sind die Räumlichkeiten und digitalen Speicherorte zu sichern.

- Die Aktenschränke der Personalabteilung und Buchhaltung müssen abschließbar sein und sind grundsätzlich abgeschlossen zu halten. Der Schlüssel darf nur den berechtigten Personen zugänglich sein.
- Die Türen beider Abteilung sind im besten Fall chipgesichert. Die Büros der Abteilung sind abzuschließen, sobald sich der berechtigte Mitarbeiter außerhalb der Räume befindet.
- Für alle Mitarbeiter freizugängliche Personalfächer dürfen nicht für personenbezogene Daten verwendet werden. Dies gilt insbesondere für Gehaltsabrechnungen.
- Beide Abteilungen sollten von anderen Abteilungen räumlich getrennte Drucker benutzen, damit Unberechtigte keinen Zugang zu den Ausdrucken haben. Im Optimalfall sieht ein zukünftig anzuschaffender Drucker die Möglichkeit vor, dass jeder Druckauftrag nur vom berechtigten Benutzer mittels Chipkarte am Drucker freigegeben werden kann. So wird verhindert, dass möglicherweise Ausdrucke sensibler Daten im Drucker für die gesamte Belegschaft einsehbar sind.

Hinweis:

Dieser Leitfaden dient der unverbindlichen Information. Es handelt es sich um eine zusammenfassende Darstellung der fachlichen und rechtlichen Grundlagen, die jedoch keinen Anspruch auf Vollständigkeit erhebt. Obwohl der Leitfaden mit größtmöglicher Sorgfalt erstellt wurde, kann eine Haftung für die inhaltliche Richtigkeit nicht übernommen werden.

ANLAGE 1 - ÜBERSICHT ALLER CHECKLISTEN

Checkliste zu personenbezogenen Daten

	Gibt es in Ihrem Hotel ein Bewusstsein für die Wichtigkeit von Datenschutz und Datenschutzrisiken?
	Bestehen bereits datenschutzrechtliche Konzepte, bspw. interne Datenschutzleitlinien, Dokumentation von Datenschutzzielen, Verantwortlichkeiten und Datenschutzrisiken, auf die Sie ggf. aufbauen können?
	Sind den einzelnen Abteilungen bekannt, welche technisch-organisatorischen Maßnahmen (TOM) zur Gewährleistung des Datenschutzes bisher vorhanden sind?
	Wer ist in der Abteilung zuständig für die zukünftige Umsetzung von TOM?
	Sind Mitarbeiter geschult, im Arbeitsalltag personenbezogene Daten zu erkennen?
	Hat jede Abteilung eine Übersicht über die Verarbeitungstätigkeiten hinsichtlich personenbezogener Daten?

Checkliste zur Datenverarbeitung

	Analysieren Sie, welche Arten von personenbezogenen Daten in Ihrem Hotel verarbeitet werden. Sind personenbezogene Daten besonderer Kategorien darunter?
	Werden personenbezogene Daten von Kindern verarbeitet?
	Auf welchen Grundlagen werden Daten in Ihrem Hotel verarbeitet?
	Bestehen Datensätze, die aufgrund einer nicht konformen Einwilligung verarbeitet wurden? Gab es in der Vergangenheit Verstöße gegen das Kopplungsverbot?
	Bietet Ihr Hotel einen Online-Newsletter an? Wie wurden die E-Mail-Adressen erhoben?
	Aktualisieren Sie das Anmeldeformular für den Newsletter: Ist ein Hinweis auf das Widerrufsrecht enthalten?
	Wird das Double-Opt-In Verfahren für die Newsletter-Registrierung benutzt?
	Ist die Unterseite der Webseite, die das Anmeldeformular enthält, verschlüsselt?
	Enthalten von Ihnen verwendete AGB Einwilligungen in die Datenverarbeitung? Wenn ja, ist die Einwilligung leicht wahrnehmbar?
	Enthalten die Datenschutzbestimmungen einen ausdrücklichen Hinweis auf das Widerrufsrecht?
	Kommen Sie Ihren Aufklärungs- und Informationsrechten betreffend der Verarbeitung personenbezogener Daten auf der Webseite nach? Aktualisieren Sie die Datenschutzbestimmungen.

Checkliste zur Auftragsverarbeitung

	Sind Externe mit der Verarbeitung personenbezogener Daten als Auftragsverarbeiter betraut?
	Auf welcher Grundlage werden die Auftragsverarbeiter für Sie tätig?
	Sind Verträge mit Auftragsverarbeitern hinsichtlich datenschutzrechtlicher Vorgaben aktualisiert worden und enthalten diese Mindestangaben gemäß Art. 28 Abs.3 DSGVO?
	Gab der Auftragsverarbeiter bislang die Gewähr für einen vertraulichen Umgang mit den übermittelten personenbezogenen Daten?
	Sprechen Sie Ihre Auftragsverarbeiter auf das neue Datenschutzrecht an und lassen Sie sich schriftlich zusichern, dass sich Ihre Auftragsverarbeiter schulen lassen.
	Dokumentieren Sie von nun an Ihre Weisungen an den Auftragsverarbeiter.
	Schließen Sie mit allen Ihren sonstigen Vertragspartnern Zusatzvereinbarungen zum datenschutzkonformen Umgang mit personenbezogenen Daten.

Checkliste zum Datenschutzbeauftragten

	Verfügt Ihr Hotel über einen Datenschutzbeauftragten? Wenn nein, warum nicht? Dokumentieren Sie Ihre Erwägungsgründe.
	Werden in Ihrem Hotel sensible, also personenbezogene Daten besonderer Kategorien verarbeitet? Oder sind mindestens zehn Mitarbeiter ständig mit der Verarbeitung personenbezogener Daten vertraut? Sie benötigen in diesen Fällen einen Datenschutzbeauftragten.
	Wenn Sie keinen Datenschutzbeauftragten benötigen, wer ist dann in Ihrem Betrieb für die Überwachung der Einhaltung des Datenschutzes verantwortlich?
	Wenn Sie in Kürze einen Datenschutzbeauftragten benennen werden: Berücksichtigen Sie die Erwägungen für uns gegen einen internen Datenschutzbeauftragten.
	Ist ein interner Datenschutzbeauftragter als solcher zertifiziert? Wenn nein, wie ist der Datenschutzbeauftragte anderweitig qualifiziert?
	Ist der Datenschutzbeauftragte der Aufsichtsbehörde gemeldet worden?
	Sind die Mitarbeiter geschult, wann der Datenschutzbeauftragte einzubeziehen ist?
	Findet eine jährliche Schulung der Mitarbeiter durch den Datenschutzbeauftragten statt?
	In welchen Abständen berichtet der Datenschutzbeauftragte der Geschäftsleitung über seine Tätigkeit?
	Wird die Zusammenarbeit mit dem Datenschutzbeauftragten dokumentiert?

Checkliste Verzeichnis der Verarbeitungstätigkeit und Datenschutz-Folgenabschätzung

	Besteht bereits ein Verarbeitungsverzeichnis? Wenn ja, prüfen Sie, ob es um die Anforderungen des Art. 30 DSGVO gegebenenfalls erweitert werden kann.
	Besteht für Ihr Hotel die Pflicht, ein Verzeichnis zu führen? Wenn nicht, wie wird der dennoch bestehenden Dokumentationspflicht nachgekommen?
	Wer ist im Betrieb dafür zuständig, das Verzeichnis zu führen und zu aktualisieren?
	Enthält das Verzeichnis alle Pflichtangeben?
	Werden fakultative Angaben im Verzeichnis aufgenommen? Falls nicht, wie erfolgt die Dokumentation alternativ?
	Wurde eine Risikoabschätzung durchgeführt? Ist das Ergebnis dokumentiert?
	Besteht aufgrund des Ergebnisses der Risikoabschätzung die Pflicht zur Datenschutz-Folgenabschätzung?
	Wer ist zuständig für die Durchführung der Datenschutz-Folgenabschätzung?
	Gibt es bislang nicht angewendete und zumutbare TOM, die Risiken für verarbeitete Daten weiter reduzieren?
	Gibt es die Möglichkeit technische Grundeinstellungen von Geräten und Software datenschutzärmer zu konfigurieren („privacy by default“)?

Checkliste Sicherheit von Hotel-Webseiten und Hotel-WLAN

	Steht den Mitarbeitern ein Ansprechpartner für IT-Sicherheit im Hotel oder extern zur Verfügung?
	Sind die Gerätesoftware der Laptops, Tablets, Smartphones etc. der Mitarbeiter aktualisiert?
	Wird auf jedem der Geräte regelmäßig ein Malware-Scanner eingesetzt?
	Sind die WLAN-Netze für Mitarbeiter und Hotelgäste getrennt?
	Werden auf der Hotelwebseite automatische Nutzerprofile angelegt? Liegt eine Einwilligung der Betroffenen vor?
	Sind alle Unterseiten der Hotelwebseite, die Eingabeformulare für personenbezogene Daten enthalten, verschlüsselt?
	Sind die Mitarbeiter über die Bedeutung von Warnungen der Browser bei SSL-Problemen (unverschlüsselte Internetseiten) geschult?
	Ist das WLAN mit einem Passwort gesichert? Wird ein einheitliches Passwort regelmäßig geändert?
	Wird das Passwort durch personenbezogene Daten generiert? Wenn ja, warum ist dies erforderlich? Dokumentation im Verzeichnis der Verarbeitungstätigkeiten erforderlich.
	Sind die Datenschutzbestimmungen (inklusive der Informationspflichten) der Webseite aktualisiert?
	Sind die Datenschutzbestimmungen und Nutzungsbedingungen für WLAN-Zugänge aktualisiert?

Checkliste zur Datenübermittlung an Dritte

	Werden Daten an Dritte außerhalb der EU weitergeleitet? Erfolgte eine Beratung durch einen Spezialisten?
	Wenn ja, hat die empfangende Stelle einen Datenschutzvertreter? Sind Kontaktdaten dieser Person im Verzeichnis der Verarbeitungstätigkeiten genannt?
	Wenn Daten an Dritte innerhalb oder außerhalb der EU weitergeleitet werden, auf welcher Rechtsgrundlage ist die Weiterleitung erlaubt?
	Ist die Rechtsgrundlage im Verzeichnis der Verarbeitungstätigkeiten genannt?
	Werden Daten an zentrale Abteilungen innerhalb eines Konzerns weitergegeben? Sind Ansprechpersonen in den empfangenden Abteilungen im Verzeichnis der Verarbeitungstätigkeiten genannt?

Checkliste zu Auskunfts- und Informationsrechten

	Sind die Datenschutzbedingungen auf der Hotelwebseite aktualisiert? Sind die Datenschutzbedingungen von jeder Unterseite der Webseite aufrufbar?
	Wird das Informationsrecht der Betroffenen auf Vorabinformation, welche personenbezogene Daten zu welchem Zweck verarbeitet werden, auf der Webseite und in Vertragsdokumenten erfüllt?
	Werden Betroffene leicht verständlich auf ihr Recht zu Auskunft, Widerspruch und Löschen in Verträgen und auf der Webseite hingewiesen?
	Ist der Datenschutzbeauftragte als Ansprechperson in den Datenschutzbestimmungen genannt?
	Wer ist im Hotelbetrieb verantwortlich für die Beantwortung etwaiger Anfragen und Bearbeitung von Widersprüchen gegen die Verarbeitung von Daten?
	Ist auf der Webseite eine Ansprechperson für Betroffene genannt, die Auskunft über bereits verarbeitete personenbezogene Daten (nachträglicher Informationsanspruch) geben kann?
	Ist der verantwortliche Mitarbeiter geschult, welche Daten unter welchen Umständen übermittelt werden dürfen?
	Bestehen standardisierte Vorlagen zur schnellen und umfassenden Beantwortung von Anfragen Betroffener?
	Ist den regelmäßig personenbezogene Daten verarbeitenden Mitarbeitern eine Ansprechperson bei der Aufsichtsbehörde bekannt?
	Ist sichergestellt, dass der Aufsichtsbehörde im Falle einer Anfrage, unverzüglich das Verzeichnis der Verarbeitungstätigkeiten oder eine andere Form der Dokumentation übermittelt werden könnte?

Checkliste zum Löschen von Daten

	Sind die ggf. unterschiedlichen Aufbewahrungs- und Löschfristen (abhängig vom jeweiligen Verarbeitungszweck) für alle Datenkategorien dokumentiert und auf regelmäßige Wiedervorlage gesetzt?
	Besteht eine interne Richtlinie (Löschkonzept), wann Daten nach Wegfall des Zwecks der Datenerhebung gelöscht werden?
	Sind die Zuständigkeiten für den Löschvorgang geregelt?
	Wie werden nach Widerspruch des Betroffenen gegen die Verwendung der Daten Sperrvermerke in der Datenbank umgesetzt?
	Wenn Betroffene die Löschung ihrer personenbezogenen Daten verlangt und die personenbezogenen Daten zuvor an Dritte weitergegeben wurden, ist dann ein Verfahren vorgesehen, wie der weitergebende Verantwortliche auch diese Stellen informieren, dass die Daten gelöscht werden sollen?

Checkliste Umgang mit Datenschutzverletzungen

	Wer ist im Hotel zuständig, Datenschutzverletzungen an die Aufsichtsbehörden zu melden?
	Ist gewährleistet, dass eine Meldung innerhalb von 72 Stunden nach Kenntnis von der Datenpanne erfolgt?
	Wurde im Hotel ermittelt, an welchen Stellen der Datenverarbeitung ein beachtliches Risiko für Datenschutzverletzungen besteht?
	Gibt es geeignete Methoden, Datenpannen im Hotel zeitnah aufzuspüren?
	Sind Mitarbeiter geschult, wie sie sich bei Datenschutzverletzungen zu verhalten haben?

Checkliste zum Arbeitnehmerschutz

	Welche personenbezogenen Daten besonderer Kategorien von Arbeitnehmern und Bewerbern werden verarbeitet?
	Ist ein besonderer Schutz für besondere Kategorien personenbezogener Daten gewährleistet?
	Auf welcher rechtlichen Grundlage werden Daten von Arbeitnehmern verarbeitet? Liegt eine schriftliche, rechtskonforme Einwilligung der Arbeitnehmer vor?
	Sind Betriebsvereinbarungen zum Datenschutz aktualisiert?
	Wie werden Unterlagen mit Daten zu Arbeitnehmern und Bewerbern aufbewahrt?
	Wer hat aktuell Zugang zu Arbeitnehmer- und Bewerberdaten? Ist eine restriktivere Zugangsregelung möglich?
	Wie ist sichergestellt, dass online eingereichte Bewerbungsunterlagen mindestens den gleichen Schutz wie Bewerbungsunterlagen in Papier erhalten? Besteht ein entsprechender Zugangsschutz?
	Ist die Unterseite, auf der Bewerbungen online eingereicht werden können, verschlüsselt?
	Werden Bewerber bei Online-Bewerbungen über Art und Umfang der Verarbeitung ihrer Daten informiert? Sind die Datenschutzbedingungen entsprechend aktualisiert?
	Sind die Mitarbeiter zu Auskunftsrecht, Widerspruchsrecht und Recht auf Löschen der Arbeitnehmer und Bewerber geschult?
	Ist die Löschung der Bewerberdaten und Daten ausgeschiedener Arbeitnehmer geregelt?
	Sind die Löschfristen im Verzeichnis der Verarbeitungstätigkeiten dokumentiert?
	Wurde die Vereinbarung zur Auftragsverarbeitung durch eine evtl. E-Recruiting-Plattform überprüft?
	Ist der Betriebsrat über die datenschutzrechtlichen Neuerungen informiert?

ANLAGE 2

Muster für die interne Bestellung zum/zur betrieblichen Datenschutzbeauftragten

Bestellung zum/zur Datenschutzbeauftragten

Hiermit bestellt die [Name des Hotels, Rechtsform bspw. GmbH, Adresse], vertreten durch den Geschäftsführer [Name]

im gegenseitigen Einvernehmen und mit sofortiger Wirkung / zum [Datum]

Herrn / Frau [Name, Anschrift, aktuelle Position]

zum/zur betrieblichen Datenschutzbeauftragten gem. § 38 BDSG / Art. 37 ff. EU-Datenschutz-Grundverordnung.

Der Datenschutzbeauftragte ist in dieser Funktion der Geschäftsleitung unmittelbar unterstellt und erfüllt seine Aufgaben als betriebliche/r Datenschutzbeauftragte/r weisungsfrei. Der Datenschutzbeauftragte erstattet der Geschäftsleitung [einmal jährlich / zweimal jährlich] Bericht über seine Tätigkeit.

Die Aufgaben und Pflichten des Datenschutzbeauftragte/n ergeben sich aus der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz, die in der Anlage weiter konkretisiert wurden.

_____

Ort, Datum Unterschrift des Mitarbeiters

_____

Ort, Datum Unterschrift des Geschäftsführers

Anlage: Pflichten und Aufgaben des internen Datenschutzbeauftragten

ANLAGE 3

Vorlage der Bayerischen Landesamts für Datenschutzaufsicht - Verzeichnis der Verarbeitungstätigkeiten mit Ausfüllhilfe

Verzeichnis von Verarbeitungstätigkeiten Verantwortlicher gemäß Art. 30 Abs.1 DSGVO	Vorblatt
Angaben zum Verantwortlichen Name und Kontaktdaten der Hotelbetriebsgesellschaft / Betriebsinhaber: Hauptniederlassung Name Straße PLZ, Ort Telefon E-Mail-Adresse Internetadresse	
Angaben zum ggf. gemeinsam mit diesem Verantwortlichen Name Straße PLZ, Ort Telefon E-Mail-Adresse	
Angaben zum Vertreter des Verantwortlichen (= EU-Vertreter) Name und Kontaktdaten Name Strasse PLZ, Ort Telefon E-Mail-Adresse	
Angaben zur Person des Datenschutzbeauftragten (extern mit Anschrift) Name, Vorname Straße PLZ, Ort Telefon E-Mail-Adresse	

[Bezeichnung der konkreten Verarbeitungstätigkeit]	Anlage
Datum der Anlegung:	Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse	
Bezeichnung der Verarbeitungs-tätigkeit	
Zwecke der Verarbeitung	
Beschreibung der Kategorien betroffener Personen	☐ Beschäftigte ☐ Gäste ☐ Interessenten ☐ Lieferanten ☐ Sonstige
Beschreibung der Datenkategorien	☐ ☐ ☐ Besondere arten personenbezogener Daten (gemäß Art. 9 DSGVO) ☐

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch werden	☐ Intern ☐ Abteilung / Funktion
	☐ Extern ☐ Empfängerkategorie
Datenübermittlung	☐ Datenübermittlung findet nicht statt und ist auch nicht geplant ☐ Datenübermittlung findet wie folgt statt:
Nennung der konkreten Datenempfänger	Empfängerkategorie
Sofern es sich um eine Datenübermittlung gemäß Art. 49 Abs. 2 DSGVO handelt	Dokumentation geeigneter Kategorien
Fristen für die Löschung der verschiedenen Datenkategorien	

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO. Siehe TOM-Beschreibung.

Datum Unterschrift des zuständigen Mitarbeiters und des Verantwortlichen

Erläuterungen zur Verwendung des Muster Verzeichnis der Verarbeitungstätigkeiten

Vorblatt (Seite 1)

Hinweis: Seite 1 muss nur einmalig ausgefüllt werden.

Im Feld **„Angaben zum Verantwortlichen“** geben Sie die Kontaktdaten Ihres Hotels (Betriebsgesellschaft) an.

Das Feld **„Angaben zum ggf. gemeinsam mit diesem Verantwortlichen“** muss in der Regel nicht ausgefüllt werden, da die Hotelbetriebsgesellschaft die alleinige Verantwortung für die im Hotel erhobenen Daten hat.

Das Feld **„Angaben zum Vertreter des Verantwortlichen“** muss in der Regel nicht ausgefüllt werden. Nur Unternehmen, die nicht in der EU niedergelassen sind, müssen laut DSGVO einen „Vertreter“ benennen.

Das Feld **„Angaben zur Person des Datenschutzbeauftragten“** muss nur ausgefüllt werden, sofern ein externer Datenschutzbeauftragter benannt wurde. Bei einem internen Datenschutzbeauftragten kann die Anschrift weggelassen werden.

Konkrete Verarbeitungstätigkeit (Seite 2 und 3)

Hinweis: Seiten 2 und 3 ist für jede einzelne Verarbeitungstätigkeit separat auszufüllen.

Beispiele für konkrete Verarbeitungstätigkeiten:

- Gästedaten, die über das Buchungsformular auf der Hotelwebseite erfasst werden
- E-Mail-Adressen von Gästen und Interessenten, die über das Newsletter-Anmeldungsformular erhoben werden
- Personaldaten, die in der Personalabteilung verarbeitet werden
- Daten von Vertragspartnern

„Datum der Anlegung“: Tragen Sie hier das Datum der erstmaligen Anlegung des Dokumentationsvorgangs ein.

„Datum der letzten Änderung“: Sofern sich der Datenverarbeitungsprozess geändert hat (z.B. neuer Ansprechpartner aufgrund von Personalwechsel, Zweck der Datenverarbeitung), muss das Verzeichnis angepasst und das Datum der letzten Änderung eintragen werden. Hierbei sollten Daten nicht überschrieben werden, sondern nur ergänzt werden, so dass zu einem späteren Zeitpunkt erkennbar ist, wie die Verarbeitungstätigkeit zu einem früheren Zeitpunkt durchgeführt wurde.

„Verantwortliche Fachabteilung“: z.B. „Buchhaltung“, „Personalwesen“, „Marketing“, „Geschäftsführung“

„Ansprechpartner“: Name des entsprechenden Mitarbeiters

„Telefon“: Dienstliche Telefonnummer des entsprechenden Mitarbeiters

„E-Mail-Adresse“: Dienstliche E-Mail-Adresse des entsprechenden Mitarbeiters

„Bezeichnung der Verarbeitungstätigkeit“: In diesem Feld wird die konkrete Bezeichnung der entsprechenden Verarbeitungstätigkeit, bei der personenbezogene Daten eine Rolle spielen, eingetragen.

Bespiele für typische Verarbeitungstätigkeiten, bei denen personenbezogene Daten eine Rolle spielen:

- Erfassen und Speichern von Personaldaten der Mitarbeiter
- Speichern von Gästedaten, die über die Unternehmenswebseite erfasst werden

„Zwecke der Verarbeitung“: Hier wird eingetragen, zu welchem Zweck personenbezogene Daten verarbeitet werden.

Beispiele für typische Verarbeitungszwecke:

- Lohnabrechnung
- Zimmerreservierung über die Webseite
- Aufbewahrung von Dokumenten gemäß Handelsgesetzbuch/Abgabenordnung um gesetzliche Aufbewahrungsfristen einzuhalten

„Beschreibung der Kategorien betroffener Personen“: Kreuzen Sie hier die betroffene Personengruppe(n) an, deren personenbezogene Daten bei der entsprechenden Verarbeitungstätigkeit verarbeitet werden.

„Beschreibung der Datenkategorien“: Hier können Sie die personenbezogenen Daten, die verarbeitet werden, kategorisieren. Es bietet sich beispielsweise an folgende Kategorien hinter den Kästchen zu notieren:

- Daten, die der 6 bzw.10 jährigen Aufbewahrungsfrist gemäß Handelsgesetzbuch und Abgabenordnung unterliegen
- Daten die keiner gesetzlich geregelten Aufbewahrungsfrist unterliegen

Sollten **„Besondere Arten personenbezogener Daten“** verarbeitet werden, dann sind diese konkret zu benennen.

„Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden“: Unterschieden Sie hier zwischen internen und externen Empfängern.

„Datenübermittlung“: Kreuzen Sie hier an, ob eine Datenübermittlung stattfindet. Sollten die Daten in das EU-Ausland übermittelt werden, dann sind Angaben zu Land, Kontaktdaten des Datenempfängers, Kontaktdaten des EU-Vertreters erforderlich.

„Nennung der konkreten Datenempfänger“: Tragen Sie hier gegebenenfalls die konkreten Datenempfänger, bspw. zentrale Buchhaltung, ein.

„Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.“: Dieses Feld muss in der Regel nicht ausgefüllt werden und betrifft einen Ausnahmekatalog für Datenübermittlungen in das Eu-Ausland.

„Fristen für die Löschung der verschiedenen Datenkategorien“: Tragen Sie hier die jeweilige Löschfristen ein. Ergeben sich die Fristen aus dem Gesetz (bspw. 6 oder 10 Jahre nach Handelsrecht bzw. Steuerrecht), können Sie sich an diesen Fristen orientieren. Handelt es sich bspw. um Reservierungsdaten von Gästen im Restaurant oder Spa, muss im Rahmen eines Löschkonzepts die Speicherdauer festgelegt werden. Orientieren Sie sich hierfür am Zweck der Verarbeitung.

„Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 DSGVO Bemerkungen*: siehe TOM-Beschreibung“:* Verweisen Sie hier auf die TOM-Beschreibung, in der Sie Schutzmaßnahmen für alle standardmäßig anfallenden Datenverarbeitungen festgelegt haben.