DataSolution
thurmann

Leitfaden

Datenschutz in der Hotellerie

Medieninhaber

Hotel- und Gaststättenverband Berlin e.V. (DEHOGA Berlin)
Keithstraße 6
10787 Berlin

Tel.: +49 (0) 30.318048.0
Fax: +49 (0) 30.318048.28
M: info@dehoga-berlin.de
W: www.dehoga-berlin.de

Präsident: Willy Weiland
Hauptgeschäftsführer: Thomas Lengfelder

Autor

DataSolution Thurmann GbR
Datenschutz & Compliance
A. Thurmann u. B. Schubert
Isarstr. 13
D-14974 Ludwigsfelde

Ansprechpartner

Andreas Thurmann
T: +49 (0) 3378.202513
F: +49 (0) 3378.202514
M: mail@hoteldatenschutz.de
W: www.hoteldatenschutz.de

Titelbild

#50802651 – Fotolia
#67174943 – Fotolia

Copyright

Inhaltsverzeichnis

Inhaltsverzeichnis

Inhaltsverzeichnis

Einleitung

Sehr geehrte Hoteliers,

die Verarbeitung von Gastdaten in der Hotellerie zeichnet sich insbesondere durch drei Dinge aus: Das Hotel erhält die Daten auf den unterschiedlichsten Wegen, viele Daten werden während eines Hotelaufenthaltes automatisch erfasst und es handelt sich bei den gespeicherten Daten meist um sehr persönliche und sensible Informationen des Gastes.

Bereits bei der Reservierung erhalten Sie als Hotelier umfangreiche Daten über den Gast. Die Daten, zu meist Namen, Anschrift, Kontaktdaten, Kreditkartennummern und Wünsche, werden in die Hotelsoftware übernommen. Alle zum Vorgang erhaltene oder ausgedruckte Unterlagen werden oft zusätzlich in Reservierungsordnern abgelegt. Darüber hinaus erfährt das Hotel vom Check-In bis zum Check-Out sehr viel Persönliches über seine Gäste, wie z.B. über ihre Essgewohnheiten, Vorlieben und Freizeitinteressen. Unter Umständen können sogar Rückschlüsse auf die Gesundheit des Gastes gezogen werden, z.B. bei Befreiung von Kurbeiträgen wegen einer Behinderung, wenn ein Allergikerzimmer gebucht oder um bestimmte Kissen wegen Rückenschmerzen gebeten wird.

Für den Bereich Sales & Marketing ist interessant, wie potenzielle Gäste gewonnen oder ehemalige Gäste an das Hotel bzw. an eine Hotelgruppe gebunden werden können. Sowohl Firmenkunden als auch der einzelne Gast stehen hier im Fokus der Aktivitäten. Unter Berücksichtigung von datenschutz- und wettbewerbsrechtlichen Aspekten ist bei jeder Aktion zu entscheiden, welche Daten von Interessenten und Gästen zu Werbezwecken genutzt werden dürfen.

Stichtag: 25. Mai 2018

Aktuell regelt in Deutschland das Bundesdatenschutzgesetz (BDSG) den Umgang mit personenbezogenen Daten. Das ändert sich zum 25. Mai 2018, denn ab diesem Zeitpunkt tritt die Europäische Datenschutzgrundverordnung (DSGVO) in Kraft und ist für jedes Unternehmen in Deutschland und somit auch für die Hotellerie und das Gastgewerbe bindend.

Im Gegensatz zur bislang gültigen Datenschutzrichtlinie ist die DSGVO ab Mai 2018 geltendes Recht in allen EU-Mitgliedstaaten. Denn anders als bei einer EU-Richtlinie sind die Mitgliedstaaten verpflichtet, die Verordnung direkt anzuwenden. Aufgrund von Öffnungsklauseln können zusätzlich durch die einzelnen EU-Länder länderspezifische Detailregelungen erlassen werden, die allerdings das Datenschutzniveau der DSGVO nicht unterlaufen dürfen. In Deutschland gilt es dann, neben der DSGVO auch die Vorgaben aus dem BDSGneu, welches adaptiert wurde, zu beachten und umzusetzen.

Der Leitfaden soll Sie dabei unterstützen, die Ihnen bevorstehenden Aufgaben zum Datenschutz, aber auch zur Datensicherheit, zu meistern. Zur besseren Lesbarkeit haben wir Begriffe, die sich zugleich auf Frauen und Männer beziehen, in der männlichen Form angeführt. Dies soll jedoch keinesfalls eine Geschlechterdiskriminierung oder eine Verletzung des Gleichheitsgrundsatzes zum Ausdruck bringen.

1 Das Datenschutzrecht

Zielfragen

- Wann ist das Datenschutzrecht anzuwenden?
- Welche Grundsätze sind zu beachten?
- Wann und in welchem Umfang dürfen personenbezogene Daten verarbeitet werden?
- Wie organisiert man den Datenschutz im Unternehmen?
- Welche Nachweispflichten ergeben sich direkt für den Hotelier?
- Wer weiß was über die gespeicherten personenbezogenen Daten?
- Welche Rechte haben Personen gegenüber datenverarbeitende Stellen?
- Wer kontrolliert die Einhaltung von Datenschutzvorgaben?
- Welche Strafen gibt es bei Datenschutzverstößen?

Ab 25. Mai 2018 gilt für das Datenschutzrecht die EU-Datenschutz-Grundverordnung (in weiterer Folge **DSGVO** genannt) zusammen mit den Erwägungsgründen und dem neuen Bundesdatenschutzgesetz (in weiterer Folge **BDSGneu** genannt). Jedoch sind auch für die elektronische Kommunikation das **Telekommunikationsgesetz** (in weiterer Folge TKG), das **Telemediengesetz** (in weiterer Folge TMG) für das Anbahnen und Abwickeln von Geschäften im Internet, das **Gesetz gegen den unlauteren Wettbewerb** (in weiterer Folge UWG) sowie das **Bundesmeldegesetz** (in weiterer Folge BMG) von Bedeutung.

Dieses Kapitel betrachtet die juristischen, organisatorischen und technischen Anforderungen, die sich aus den gesetzlichen Bestimmungen ergeben. In den darauffolgenden Kapiteln werden wir Ihnen möglichst viele, auf die Hotellerie zugeschnittene Handlungshinweise und Tipps an Hand von Beispielen zu geben. Allerdings geben wir zu bedenken, dass wir nicht alle Themenbereiche so tiefgründig behandeln können, wie Sie es sich eventuell erhoffen, da schon auf Grund der unterschiedlichen Größen von Hotels und die eingesetzte Technik die Prozesse und Anforderungen stark unterscheiden.

1.1 Anwendungsbereich der DSGVO

Die DSGVO gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen. Personenbezogene Daten sind alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person (betroffene Person/ Betroffener) beziehen. Bestimmbar ist eine Person z.B. über Telefonnummer, Gesicht auf einem Foto aber auch IP-Adresse.

Unter Verarbeitung versteht man jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die

Verwendung, die Weitergabe durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleichen oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung personenbezogener Daten mit oder ohne Hilfe automatisierter Verfahren.

Räumlich gilt die DSGVO in der Europäischen Union, unabhängig davon, ob die Verarbeitung innerhalb oder außerhalb der EU stattfindet.

1.2 Grundsätze der Datenverarbeitung

Bei der Verarbeitung personenbezogener Daten ist von den folgenden in Art. 5 DSGVO festgelegten Grundsätzen auszugehen. Diese geben für die nachfolgenden Ausführungsbestimmungen den Rahmen vor. Im Einzelnen enthält Art. 5 DSGVO folgende Grundsätze:

- **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**

  Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für den Gast und Mitarbeiter nachvollziehbaren Weise verarbeitet werden. Der Betroffene ist unaufgefordert über den Umfang und die Zwecke der Verarbeitung zu informieren, um eine faire und transparente Verarbeitung zu gewährleisten. Zudem sind die betroffenen Personen über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu informieren und darüber aufzuklären, wie sie ihre diesbezüglichen Rechte geltend machen können. (z.B. Datenschutzerklärung auf der eigenen Webseite)

- **Zweckbindung**

  Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen dann nicht für andere Zwecke verwendet werden (z.B.an die Mailadresse, welche Sie bei der Reservierung erhalten haben, darf nicht ohne weiteres ein Newsletter versendet werden. Ausnahmeregelungen siehe unter Pkt. 5.3.2).

- **Datenminimierung**

  Die Erhebung von personenbezogene Daten muss auf das für den Zweck der Verarbeitung notwendige Maß beschränkt sein (z.B. ist es nicht legitim, in einem Bewerbungsbogen nach der Sozialversicherungsnummer des Bewerbers zu fragen).

- **Richtigkeit**

  Personenbezogene Daten müssen sachlich richtig und auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden. (z.B. Gästeadressen, Mitarbeiteradressen)

- **Speicherbegrenzung**

  Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. (z.B. Löschung von Gastdaten).

- **Integrität und Vertraulichkeit**

  Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet. Durch geeignete technische und organisatorische Maßnahmen soll auch sichergestellt werden, dass Unbefugte keinen Zugriff auf die Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können (z.B. Benutzerrechte im Hotelreservierungssystem, Zugang zu PCs).

1.3 Rechtmäßigkeit der Datenverarbeitung

Art. 6 DSGVO hält fest, dass jede Verarbeitung personenbezogener Daten in jeder Phase auf Grund des damit verbundenen Eingriffs in das Persönlichkeitsrecht einer Erlaubnis bedarf. Jegliche Verarbeitung personenbezogener Daten **ist grundsätzlich verboten**, soweit sie nicht aufgrund einer der nachfolgenden Ausnahmen zulässig ist. Das Prüfschema für die Zulässigkeit einer Datenverarbeitung ist daher wie folgt:

1. Werden die Daten zur Erfüllung einer **gesetzlichen Bestimmung** benötigt? (z.B. Meldeschein)

2. Wenn die Antwort NEIN ist, dann prüfen Sie, ob die Verarbeitung zur **Erfüllung eines Vertrags** (z.B. Beherbergungsvertrag) oder zur Durchführung **vorvertraglicher Maßnahmen** (z.B. Reservierung) erforderlich ist.

Ist die Verarbeitung personenbezogener Daten durch keinen Erlaubnistatbestand legitimiert, so sind die unzulässigen Daten zu löschen (Art. 17 DSGVO). Es bestehen gegebenenfalls Unterlassungs- und Schadensersatzansprüche (Art. 82 DSGVO). Ferner liegt eine mit Bußgeld zu ahndende Ordnungswidrigkeit (Art. 83 DSGVO) oder auch eine Straftat vor.

3. Wenn weder eine gesetzliche Vorgabe noch ein Vertragsverhältnis vorliegt, dann benötigen Sie eine **Einwilligung** (Art. 7 DSGVO) zur Verarbeitung der personenbezogenen Daten, insbesondere für einen anderen oder mehrere Zwecke (z.B. Anmeldung zum Newsletterservice über die Webseite).

4. Sie können zusätzlich personenbezogene Daten verarbeiten, wenn das **überwiegende berechtigte Interesse** des Verantwortlichen oder eines Dritten überwiegt, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person den Schutz personenbezogener Daten erfordern. So ist z.B. eine Videoüberwachung in Umkleiden oder Saunabereichen verboten, da hier die Privatsphäre der Personen dem Schutzbedürfnis des Betreibers überwiegt.

Der Hotelier hat darzulegen, wieso die jeweilige Erhebung, Verwendung oder Verarbeitung der jeweiligen Daten erforderlich sind, worin ihre Bedeutung für die Interessenwahrung besteht und welche Interessen dies konkret sind.

An eine formgerechte Einwilligung gemäß Pkt. 3 sind weitere Bedingungen gebunden, die vom Hotelier sicherzustellen sind. Nachfolgende Grafik veranschaulicht die Anforderungen.

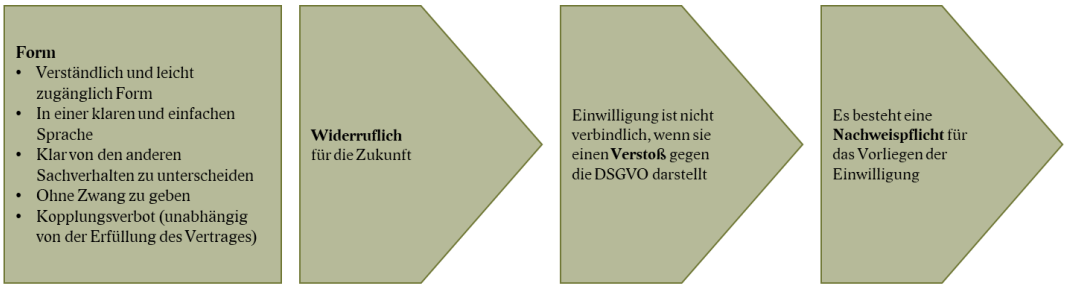

Abbildung 1 | Bedingungen der Einwilligung (Art. 7 DSGVO)

Quelle | in Anlehnung an DATAKONTEX GmbH

Sollen personenbezogene Daten in Länder außerhalb der EU (Drittländer) übermittelt werden, bedarf dieser Vorgang einer besonderen Erlaubnis (Art. 44 ff. DSGVO).

1.4 Datenschutzorganisation und IT-Sicherheit

Die Organisation des Datenschutzes liegt in der Verantwortung des Hoteliers, insbesondere der Hotelleitung und der Geschäftsführung. Die DSGVO fordert ein **Datenschutzmanagementsystem (DSMS)**, das in der eigenen Verantwortung des Unternehmens wirksam sein muss. Die für die Einführung eines DSMS relevanten Normen finden sich in verschiedenen Stellen der DSGVO wie Artt. 5 Abs. 2, 24, 30, 32, 35 und 37.

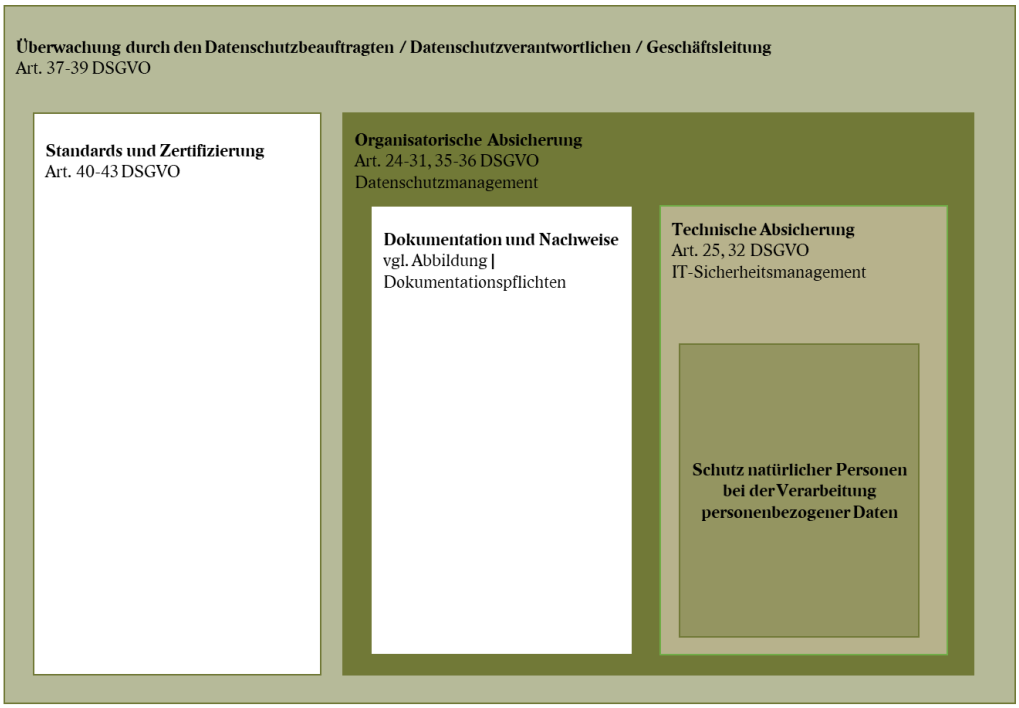

Abbildung 2 | Schutzmodell der DSGVO

Quelle | in Anlehnung an DATAKONTEX GmbH

Es muss im Hinblick auf die sogenannte Rechenschaftspflicht jederzeit möglich sein, die Rechtskonformität der Verarbeitung sowohl in rechtlicher wie auch in technischer und organisatorischer Sicht nachweisen zu können. Hieraus ergeben sich die unterschiedlichsten **Dokumentations- und Nachweisanforderungen**:

- **Regelungen hinsichtlich der**
  - Zuweisung von Zuständigkeiten
    (Wer ist im Unternehmen verantwortlich und zuständig?)
  - Einsatz datenschutzfreundlicher Technologien
    (Anforderung an Software, Speicherort, ...)
  - Durchführung von Kontrollen
    (Ist-Analyse, Audit, Maßnahmenplan)
- **Datenschutzrechtliche Dokumentationspflichten (Datenschutzhandbuch), wie:**
  - Datenschutzrichtlinien (interne Regelungen mit Weisungscharakter für Mitarbeiter im Hotel, wie Datenschutz und Datensicherheit im Unternehmen integriert und aufgebaut ist. Mehr dazu unter Pkt. 8.2.)
  - Führen des Verzeichnisses von Verarbeitungstätigkeiten inkl. Zweckbestimmung, Grundlage der Verarbeitung und Durchführung einer Risikobewertung
  - Verpflichtung Mitarbeiter auf das Datengeheimnis
  - Verpflichtung von Dienstleistern im Rahmen der Datenverarbeitung im Auftrag
  - Sensibilisierung und Schulung von Mitarbeitern
  - Prozesse zur Wahrung der Betroffenenrechte und zum Datenpannenmanagement
  - durchzuführende Datenschutz-Folgenabschätzungen
  - Beschreibung von technischen und organisatorischen Maßnahmen
  - nachweisliche Überprüfung von Datenschutzmaßnahmen

Die DSGVO setzt gemäß Art. 32 das Vorhandensein eines IT-Sicherheits-managements voraus. Zuzüglich verweist sie immer wieder auf Aspekte des Risikomanagements. Hier empfiehlt es sich, die Managementsysteme untereinander zu verknüpfen.

Obige Dokumentations- und Nachweisanforderungen dienen dazu, ein Schutzniveau zu gewährleisten, dass dem Risiko für die Rechte und Freiheiten der von Personen gespeicherten Daten angemessen, aber auch verhältnismäßig ist. Welche technischen und organisatorischen Maßnahmen zu treffen sind, bestimmt der Schutzbedarf der zu speichernden Daten. So ist der Schutzbedarf bei der Speicherung von Bank- und Kreditkartendaten (PCI DSS Normen) wesentlich höher anzusetzen, als beim Speichern von Interessentendaten. Der Schutzbedarf bestimmt den Umfang der Sicherheitsmaßnahmen, wobei der Grundsatz der Verhältnismäßigkeit im Hinblick auf das Risiko und der Eintrittswahrscheinlichkeit anzuwenden ist. Die Bewertung der Verhältnismäßigkeit setzt somit eine Risikobewertung voraus, insbesondere in den Schutzzielen: Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme. So stellt bspw. der Einsatz

von Cloud-Technologien anders geartete Anforderungen an Datensicherungsmaßnahmen, als bei herkömmlichen Client-Server-Lösungen.
Zur Bestimmung der Sicherheitsmaßnahmen sind nach der DSGVO folgende Schritte erforderlich:

- **Feststellung des Schutzbedarfes**. Hier erfolgt die Festlegung der für das Unternehmen relevanten Sicherheitsziele und -strategien in Form einer für alle verbindlichen IT-Sicherheitspolitik. In dieser werden Benutzerrechte, Umgang mit PC und mobilen Endgeräten etc. geregelt.
- Ermittlung und Bewertung der **Risiken**.
- Festlegung geeigneter **organisatorischer und technischer Sicherheitsmaßnahmen**.
- Planung und Durchführung von Sicherheitsüberprüfungen für **regelmäßige interne Kontrollen (Audit)** von festgelegten Maßnahmen.
- Erbringung entsprechender **Nachweise**.

1.5 Rechenschaftspflichten durch Dokumentation

Ausgangspunkt für die Verarbeitungen personenbezogener Daten sind die in Art 5 DSGVO festgeschriebenen und in Punkt 1.2 genannten Grundsätze. Der Hotelier als Verantwortlicher ist für deren Einhaltung rechenschafts- und nachweispflichtig (Art. 5 Abs. 2 DSGVO).

Abbildung 3 | Dokumentationspflichten

Quelle | in Anlehnung an DATAKONTEX GmbH

Der Nachweis ist anhand einer entsprechenden Dokumentation zu führen und ist regelmäßig für die Umsetzung technischer und organisatorischer Maßnahmen zu wiederholen.

Als im Detail geregelte Dokumentationspflicht zu nennen ist unter anderem das **Verzeichnis von Verarbeitungstätigkeiten** und **Verzeichnis für Auftragsverarbeitung**. Für bestimmte Verarbeitungen ist in Abhängigkeit von dem Risiko, das mit einer Verarbeitung verbunden ist, ist vor ihrer Einführung eine **Datenschutz-Folgenabschätzung** durchzuführen. Bei einem **Datentransfer in einen Drittstaat**, welcher als unsicher gilt, sind die Risikoabschätzung und die ergriffenen Schutzmaßnahmen zu dokumentieren und im Verfahrensverzeichnis aufzuzeigen. Nachträglich aufgetretene und gegebenenfalls der Aufsichtsbehörde und den Betroffenen **mitzuteilende Datenschutzverletzungen** sind, verbunden mit den ergriffenen Abwehrmaßnahmen,

festzuhalten. Zusätzliche umfangreiche Dokumentationspflichten bestehen zwecks **Erfüllung der Transparenz-regelungen** gegenüber den Betroffenen.

Der Hotelier muss jederzeit in der Lage sein, die Rechtmäßigkeit seiner Verarbeitungen nachweisen zu können. Das Fehlen einer Dokumentation kann mit einem Bußgeld belegt werden.

1.6 Transparenzvorgaben

Ein elementarer Grundsatz des Datenschutzrechtes ist die Transparenz. Personen sollen in die Lage versetzt werden, die Datenerhebung, -verarbeitung bzw. -nutzung zu prüfen oder wissen *„Wer was wann und bei welcher Gelegenheit über eine Person weiß."* Dieser Grundsatz kann nur dann gewährleistet werden, wenn Unternehmen und Verantwortliche ausreichend über Datenverarbeitungsvorgänge informieren.

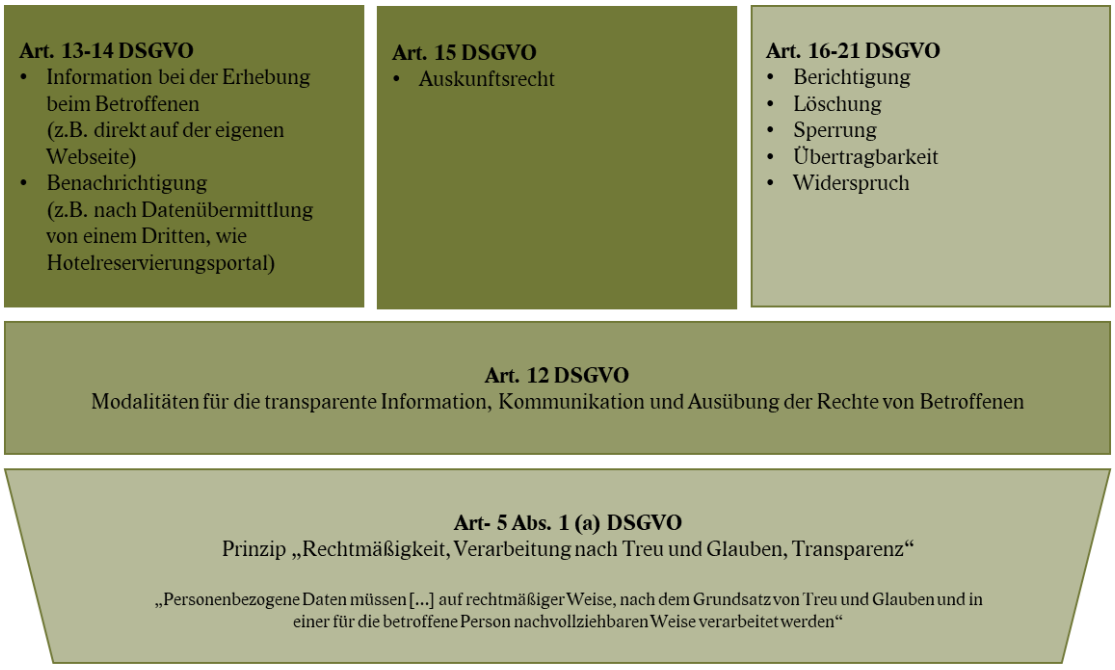

Abbildung 4 | Transparente Verarbeitung

Quelle | in Anlehnung an DATAKONTEX GmbH

Die DSGVO enthält erheblich umfangreichere und detailliertere Regelungen zu Informationspflichten als bisher, welche die Transparenz gegenüber den betroffenen Personen herstellen. Aktive Transparenz begründen Artt. 13, 14 DSGVO bei der Datenerhebung mit umfangreichen Informationen über die Verarbeitung der Daten. Von sich aus tätig werden muss der Hotelier auch bei:

- Datenschutzverletzungen (Art. 34 DSGVO),
- Aufhebung der Einschränkung der Verarbeitung (Art. 18 Abs. 3 DSGVO),
- einmaligen Drittstaatentransfer (Art. 49 Abs. 1 S 4 DSGVO) oder
- der Zurverfügungstellung einer Vereinbarung über gemeinsame Verarbeitung Art. 26 Abs. 2 S 2 DSGVO).

Bedeutsam ist auch die Pflicht zur Information über eine Weiterverarbeitung der gespeicherten Daten zu einem anderen Zweck (Artt. 13 Abs. 3, 14 Abs. 4 DSGVO).

Auf Antrag sind zudem der Auskunftsanspruch nach Art. 15 DSGVO und die Unterrichtung nach Art. 19 S 2 DSGVO über die Information von Datenempfängern über Datenkorrekturen zu erfüllen.

1.6.1 Allgemeine Informationspflichten

Die DSGVO regelt die **Informationspflichten** in den Art. 13 und 14. Es wird unterschieden zwischen Informationspflichten bei der Erhebung personenbezogener Daten bei dem Betroffenen (Art. 13 DSGVO) und den Informationspflichten, wenn die Erhebung nicht direkt bei dem Betroffenen erfolgt (Art. 14 DSGVO).

Bei der Direkterhebung kann nach Art. 13 Abs. 4 DSGVO auf die schriftliche Benachrichtigung verzichtet werden, wenn die Person bereits informiert wurde, z.B. durch die Datenschutzerklärung auf der eigenen Webseite. Dabei ist darauf zu achten, dass der Besucher der Webseite vor dem Versenden seiner Daten den Datenschutzbestimmungen zugestimmt hat.

Durch ein Kontrollkästchen, dessen „Aktivieren" zwingend erforderlich ist, lässt sich eine formgerechte Zustimmung einholen.

Nach Art. 12 DSGVO sind die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form zu erteilen. Dabei können sie schriftlich oder in elektronischer Form an den Betroffenen übermittelt werden. Es ist möglich, auch sog. standardisierte Bildsymbole zu verwenden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln.

Bei der Direkterhebung (z.B. wenn jemand über die Webseite des Hotels bucht) sind nach Art. 13 Abs. 1 DSGVO zum Zeitpunkt der Erhebung folgende Informationen bekannt zu geben:

- Name und Kontaktdaten des Verantwortlichen
- ggf. Kontaktdaten des DSB
- Verarbeitungszwecke und Rechtsgrundlage der Verarbeitung (z.B. für die Zimmerreservierung)
- ggf. Empfänger, Information falls die Absicht besteht die Daten an ein Drittland zu übermitteln
- Speicherdauer
- Betroffenenrechte
- Möglichkeit des Widerrufs
- Beschwerdemöglichkeit bei der Aufsichtsbehörde, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist
- ggf. Hinweis auf Logik und Auswirkungen einer automationsunterstützten Entscheidungsfindung und eine Information bei geplanten weiteren Verwendungszwecken

Wenn die Daten nicht direkt erhoben werden, bspw. bei der Reservierung über ein Hotelreservierungsportal (OTA), muss die Informationen nach Art. 14 Abs. 3 DSGVO grundsätzlich innerhalb einer angemessenen Frist, spätestens jedoch nach einem Monat erteilt werden. Werden die Daten allerdings zur

Bei Verstößen gegen die Informationspflichten drohen Geldbußen. Wie die Umsetzung in die Praxis erfolgen kann, sehen Sie in den weiteren Kapiteln.

Kommunikation mit der Person verwendet oder sollen Informationen an einen Empfänger übermittelt werden, ist die Benachrichtigung zwingend zum Zeitpunkt der Kontaktaufnahme oder ersten Übermittlung vorzunehmen. Zuzüglich zu den Informationen wie im Art 13 DSGVO ist die Information zu geben, von welcher Quelle die Daten stammen (auch im Falle einer öffentlichen Quelle). Wiederum muss nicht nochmals informiert werden, wenn die betroffene Person über die Informationen bereits verfügt.

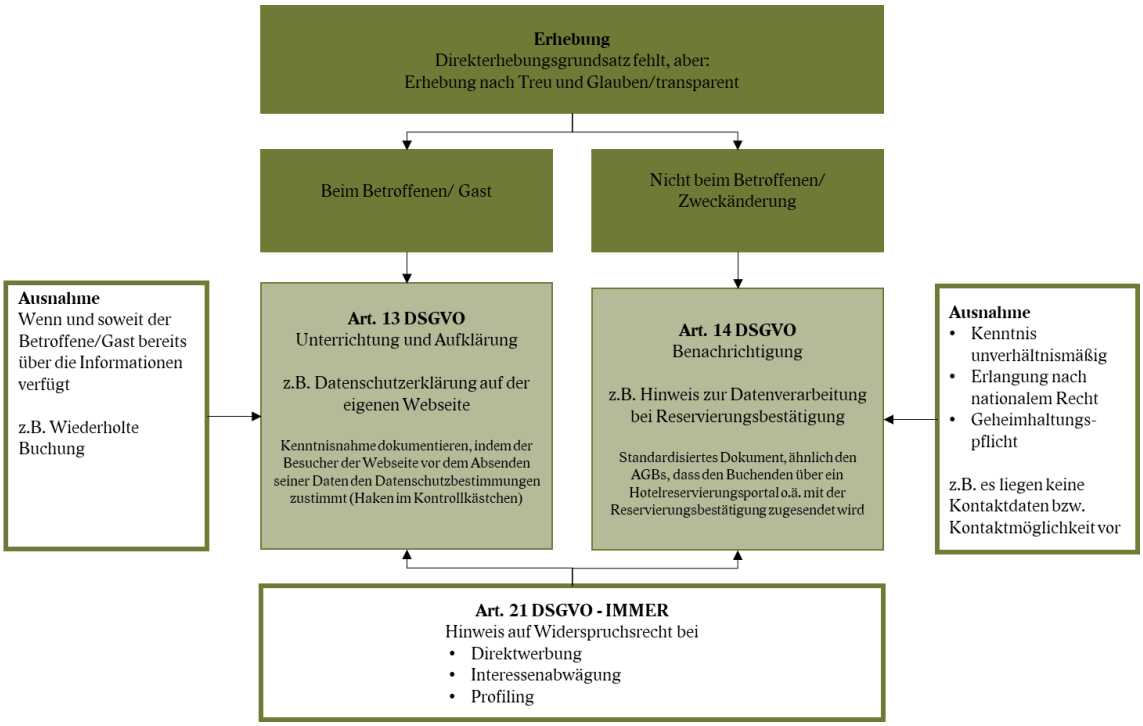

Abbildung 5 | Information bei der Erhebung von personenbezogenen Daten

Quelle | in Anlehnung an DATAKONTEX GmbH

1.6.2 Informationspflichten bei Datenschutzpanne

Verletzungen des Schutzes personenbezogener Daten (z.B. Hackerangriff, Datenverlust oder -diebstahl, unerlaubte Datenübermittlung) müssen unverzüglich, nach Möglichkeit **innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls**, an die zuständige Aufsichtsbehörde gemeldet werden. Eine Ausnahme besteht, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten des Betroffenen führt (vgl. Artt. 33, 34 DSGVO). Ein solches Risiko kann z.B. durch eine geeignete Verschlüsselung von Daten ausgeschlossen werden, die etwa beim Verlust eines Datenträgers die Kenntnisnahme der Daten durch Dritte verhindert. Besteht die Wahrscheinlichkeit, dass die Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die persönlichen Rechte und Freiheiten bewirkt, muss der Hotelier **auch die betroffene Person** ohne unangemessene Verzögerung **benachrichtigen**.

Zu den besonders zu schützenden Daten zählen gemäß Art. 9 Abs. 1 DSGVO Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit sowie die Verarbeitung von genetischen Daten, biometrische Daten zur eindeutigen Identifizierung einer

natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben bzw. der sexuellen Orientierung des Betroffenen.

Auch bei Daten, die

- zu einem physischen, materiellen oder immateriellen Schaden,
- zur Diskriminierung,
- zu einem Identitätsdiebstahl (Diebstahl von Login-Daten),
- zu einem finanziellen Verlust (bspw. Kreditkarten- und Kontoverbindungsdaten),
- zu einer Rufschädigung,
- zu einem Verlust der Vertraulichkeit von Berufsgeheimnissen

führen können (vgl. Erwägungsgrund 75 DSGVO), besteht eine Informationspflicht.

1.7 Rechte der Betroffenen

Jeder Betroffene, hier insbesondere Gäste, Reservierende, Interessenten, Firmenkontakte aber auch Mitarbeiter, kann neben dem **Recht auf Auskunft** sein Recht auf **Berichtigung, Löschung (Vergessenwerden)** oder **Einschränkung der Verarbeitung (Sperrung)** seiner personenbezogenen Daten wahrnehmen, wenn die Daten unrichtig sind oder für den Zweck, für den sie erhoben und gespeichert wurden, nicht mehr erforderlich sind. Neben den oben genannten Rechten haben Betroffene zusätzlich das **Recht auf die Datenübertragbarkeit** und ein **Widerspruchsrecht**.

Der Hotelier muss zusätzlich **allen weiteren Empfängern der Daten** jede Berichtigung, Löschung oder Einschränkung der Verarbeitung **mitteilen** (Art. 19 DSGVO).

Zur Wahrnehmung seiner Rechte kann sich jeder Person an jede beliebige Stelle des Unternehmens wenden und Auskunft über die zu seiner Person gespeicherten Daten verlangen. Unterliegen die Daten noch Aufbewahrungsvorschriften oder ist die Löschung wegen der Art ihrer Speicherung nur mit einem unverhältnismäßig hohen Aufwand möglich, tritt anstelle einer Löschung eine Sperrung. Die gesperrten Daten dürfen ohne Einwilligung des Betroffenen nicht mehr genutzt oder übermittelt werden.

Implementieren Sie im Hotel Standards, in welchen definiert ist, wer für die Bearbeitung der Betroffenenrechte verantwortlich ist, wie der Ablauf der Bearbeitung zu erfolgen hat und erstellen Sie entsprechende Musterbriefe. Um die Praxistauglichkeit zu testen, können Sie „friendly guests“ bitten, diesen Prozess zu testen.

1.7.1 Recht auf Auskunft

Art. 15 DSGVO regelt das Auskunftsrecht der Betroffenen. Jede Person hat das Recht, eine Bestätigung zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist das der Fall, hat sie ein Recht auf Auskunft über diese Daten.

Auf Verlangen des Betroffenen ist der Hotelier verpflichtet, eine Kopie der personenbezogenen Daten (Datenauszug), die Gegenstand der Verarbeitung sind, unentgeltlich zur Verfügung zu stellen. Die Grenzen des Rechts auf Erhalt einer Kopie beginnt aber dort, wo Rechte und Freiheit anderer Personen beeinträchtigt werden.

Das Auskunftsrecht darf Interessen Dritter, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software nicht beeinträchtigen. Allerdings darf dem Betroffenen durch die pauschale Berufung auf Rechte Dritter nicht jegliche Auskunft verweigert werden. Sofern sich der Auskunftsanspruch allerdings auf große Datenmengen bezieht, kann der Hotelier verlangen, dass der Betroffene präzisiert, auf welche Informationen oder welche Verarbeitungsvorgänge sich sein Ersuchen bezieht.

Gemäß Art. 15 DSGVO kann der Betroffene konkret Auskunft verlangen über

- die **personenbezogenen Daten, die den Anfragenden betreffen** sowie die Kategorien, zu denen sie gehören (Adress-, Kontakt-, Abrechnungs-, Marketingdaten, ...),
- die verfügbaren Informationen über die **Herkunft der Daten**,
- die **Zwecke der Verarbeitung** und deren **Rechtsgrundlage**,
- die **Empfänger oder die Kategorien von Empfängern**, gegenüber denen die Daten offengelegt worden sind, insbesondere bei Empfängern in Drittstaaten oder bei internationalen Organisationen,
- die für die Daten **geltende Speicherdauer** oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer sowie
- das **Bestehen eines Rechts auf Berichtigung, Löschung oder Einschränkung** der Verarbeitung der Daten durch den Verantwortlichen.

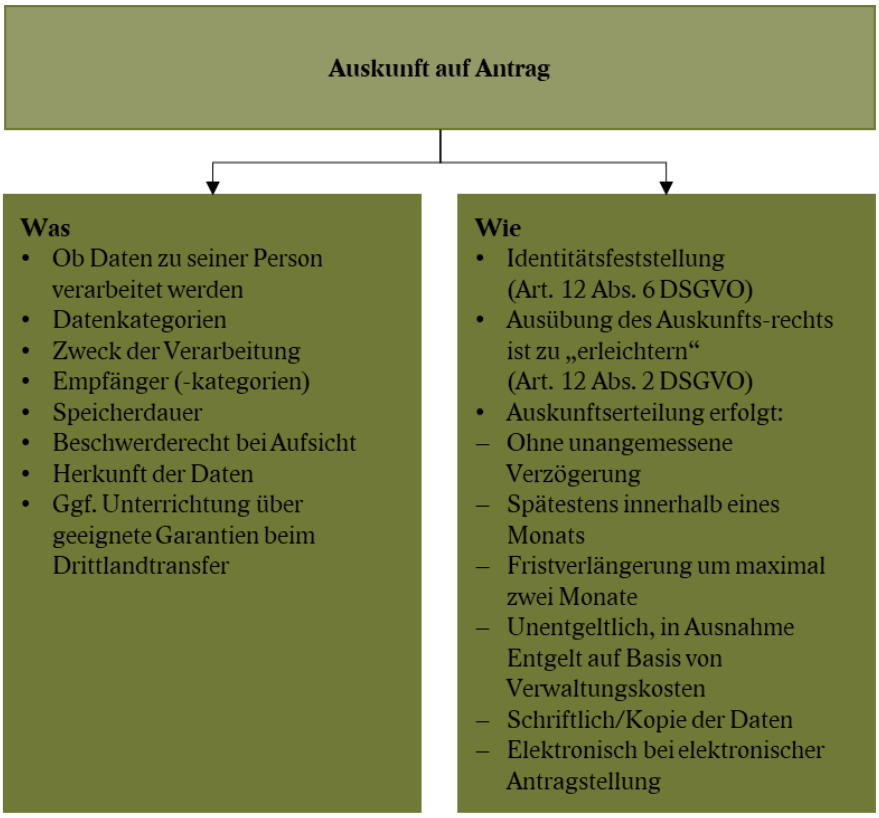

Abbildung 6 | Auskunft (Art. 15 DSGVO)

Quelle | in Anlehnung an DATAKONTEX GmbH

Die Auskunft ist unentgeltlich und verständlich zu verfassen und die verarbeitenden Daten sind korrekt anzuführen. Sind keine Daten vorhanden, so ist eine Negativauskunft zu verfassen, in der informiert wird, dass keine Daten vorliegen. Die Auskunft hat unverzüglich zu erfolgen, spätestens binnen eines Monats nach Eingang. Handelt es sich um komplexere Begehren kann diese Frist auf zwei Monate verlängert werden. Davon ist der Betroffene zu informieren.

Jede Person hat das Recht Auskunft zu verlangen, welche Daten über sie gespeichert wurden, woher diese stammen und was mit den Daten gemacht wird. Dafür hat der Anfragende im Zweifel (z.B. telefonische Anfrage oder über eine Fantasie-Mail-Adresse) seine Identität mit z.B. einer Ausweiskopie zu bestätigen. Des Weiteren hat der Anfragende dabei eine Mitwirkungspflicht, wenn die auskunftserteilende Stelle darum ersucht. Damit soll vermieden werden, dass ein unverhältnismäßiger, finanzieller als auch zeitlicher Aufwand entsteht.

1.7.2 Recht auf Richtigstellung und Löschung

Hotels sind verpflichtet, nur korrekte Daten über den Gast zu speichern. Der Gast oder eine andere Person hat jederzeit das Recht, die Berichtigung sowie im Hinblick auf den Zweck die Vervollständigung sie betreffender/unzutreffender personenbezogener Daten zu verlangen (Art. 16 DSGVO).

Die Betroffenen haben zudem nach Art. 17 DSGVO (mit bestimmten Ausnahmen) das Recht, die unverzügliche Löschung ihrer Daten zu verlangen - zum Beispiel, wenn:

- der **Zweck** der Speicherung **weggefallen** ist,
- der Betroffene seine **Einwilligung widerrufen** hat und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt,
- der Betroffene **Widerspruch** gegen die Verarbeitung eingelegt hat und keine vorrangig berechtigten Gründe für die Verarbeitung vorliegen oder
- die **Speicherung unzulässig** ist.

Die **Löschungsverpflichtung** bei Wegfall des Zwecks der Datenverarbeitung **entfällt,** sofern satzungsmäßige oder vertragliche **Aufbewahrungsvorschriften** der Löschung entgegenstehen. Eine **Ausnahme** besteht, soweit die Verarbeitung zur **Ausübung der freien Meinungsäußerung** erforderlich ist sowie **Rechtsansprüche** geltend gemacht, auszuüben oder zu verteidigen sind.

Als besondere Ausformung des Löschungsanspruches besteht nun auch ein **„Recht auf Vergessenwerden“** (Art. 17 Abs. 2 DSGVO), wenn die verantwortliche Stelle die zu löschenden Daten öffentlich gemacht hat. Hier muss der Verantwortliche vertretbare Schritte unternehmen, um die Stellen, die diese Daten verarbeiten, zu informieren, dass die betroffene Person von ihnen die Löschung aller Links zu diesen Daten oder von Kopien oder Replikationen verlangt.

Auch hier gilt eine einmonatige Frist in der die Bearbeitung und Antwort an den Betroffenen zu erfolgen hat. In komplexeren Fällen ist auch hier die Ausdehnung auf zwei Monate, bei Vorabinformation an den Betroffenen möglich.

1.7.3 Recht auf Einschränkung der Verarbeitung (Sperrung)

Eine Person kann in bestimmten Fällen auch die Einschränkung der Verarbeitung verlangen (Art. 18 DSGVO) – zum Beispiel, wenn das Hotel die Daten nicht mehr länger benötigt, allerdings der Gast zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Die Einschränkung der Verarbeitung entspricht damit begrifflich im Wesentlichen der Sperrung im Sinne von Art. 20 Abs. 3 DSGVO.

Methoden zur Beschränkung der Verarbeitung personenbezogener Daten könnten etwa darin bestehen, dass ausgewählte Informationen vorübergehend auf ein anderes Verarbeitungssystem übertragen werden, dass sie für Nutzer gesperrt werden (Setzen auf inaktiv im PMS) oder dass veröffentlichte Daten vorübergehend von einer Webseite entfernt werden.

Wurde die Verarbeitung auf Antrag des Gastes oder einer anderen Person eingeschränkt, dürfen diese personenbezogenen Daten - von ihrer Speicherung abgesehen - nur

- mit Einwilligung der betroffenen Person oder
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder
- zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder
- aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaates verarbeitet werden.

Hebt der Verantwortliche die Einschränkung auf, hat er den Betroffenen im Vorfeld zu informieren. Die Frist entspricht der Fristsetzung der anderen Betroffenenrechte.

1.7.4 Recht auf Widerspruch

Nach Art. 21 Abs. 1 DSGVO hat ein Gast oder eine andere Person grundsätzlich ein allgemeines Widerspruchsrecht gegen eine an sich rechtmäßige Verarbeitung von personenbezogenen Daten (Art. 6 Abs. 1 lit. e oder f DSGVO). Der Hotelier darf dann die Daten nur noch verarbeiten, wenn er zwingende berechtigte Gründe für die Verarbeitung nachweisen kann, die die Interessen, Rechte und Freiheiten des Betroffenen überwiegen.

Ein voraussetzungsloses und uneingeschränktes Widerspruchsrecht besteht bei der **Datenverarbeitung zum Zweck des Direktmarketings**. Das gilt auch für das Profiling, soweit es mit der Direktwerbung zusammenhängt (Art. 21 Abs. 2 und 3 DSGVO), also jede Art der automatisierten Verarbeitung von personenbezogenen Daten, die darin besteht, dass diese personenbezogene Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten. Insbesondere handelt es sich hier um eine Analyse bezüglich der Arbeitsleistung, wirtschaftliche Lage, Gesundheit, Kaufverhalten, Lebensumstände (Wohnort, Haus oder Mietwohnung, ...), aber auch persönliche Vorlieben und Interessen, Zuverlässigkeit, u.v.m., um Vorhersagen im zukünftigen Verhalten zu treffen. Der Empfänger von Werbung ist ausdrücklich, in verständlicher Form und getrennt von jeglicher anderen Information auf das Widerspruchsrecht hinzuweisen (Art. 21 Abs. 4 DSGVO).

Widerspricht der Empfänger der Nutzung oder Übermittlung seiner Daten z.B. für Zwecke der Werbung, hat das Hotel durch geeignete organisatorische bzw. technische Maßnahmen sicherzustellen, dass seinem Recht entsprochen wird. Neben den datenschutzrechtlichen Sanktionen kann der Betroffene zivilrechtlich gegen die Nichtbeachtung des Widerspruchs vorgehen.

Widerspricht ein Empfänger der Werbung, so muss gewährleistet sein, dass er nicht ein wiederholtes Mal angeschrieben wird (z.B. durch einen Sperrvermerk in der Hotelsoftware).

1.8 Kontrolle und Rechtsschutz

Abgesehen von den ordentlichen Gerichten sind die Aufsichtsbehörden für Datenschutz, Verbraucherverbände, der Datenschutzbeauftragte aber auch Betriebsräte und der Betroffene selbst als Kontrollorgane anzusehen. Die DSGVO geht von einem mehrphasigen Kontrollsystem aus.

1.8.1 Das Kontrollsystem

Der **Betroffene** in seiner Eigenschaft als Bürger, Arbeitnehmer, Kunde (Gast), Internetnutzer usw. kontrolliert seine Daten selbst. Dabei erhält er, bereits bei der Erhebung seiner Daten oder – soweit die Daten nicht bei ihm erhoben wurden – durch Benachrichtigung durch den Verantwortlichen umfangreiche Kenntnis, insbesondere über Art der verarbeiteten Daten, die Zwecke der Verarbeitung und seine Rechte. Sind die Daten zu beanstanden, so hat der Betroffene Anspruch auf Berichtigung, Einschränkung der Verarbeitung oder Löschung. Darüber hinaus kann er jederzeit Auskunft zu seinen Daten fordern und der weiteren Verarbeitung widersprechen. Sein Beschwerde- und Klagerecht kann der Betroffene an berufene Verbände abtreten. (siehe Rechte der Betroffenen)

Verbraucherverbände können im Interesse des Verbraucherschutzes bei Datenschutzverstößen Unternehmen auf Unterlassung und Beseitigung in Anspruch nehmen (Verbandsklagerecht).

Der **Datenschutzbeauftragte** hat die Einhaltung der DSGVO sowie anderer Vorschriften über den Datenschutz im Hotel zu überwachen. Er berät den Hotelier in Datenschutzfragen und ist Ansprechstelle für im Hotel tätige Mitarbeiter und durch das Hotel erfasste Externe (z.B. Gäste, Vertragspartner). Insofern obliegt ihm eine besondere Verschwiegenheitspflicht über die Identität des Betroffenen, der sich an ihn wendet.

Die in Deutschland zuständigen **Aufsichtsbehörden** für Datenschutz und Informationsfreiheit (je Bundesland) überwachen die Ausführung der DSGVO sowie andere Vorschriften über den Datenschutz im privaten Bereich. Sie haben insbesondere Beanstandungen von Betroffenen nachzugehen.

Schließlich sind dem **Betriebsrat** durch das Betriebsverfassungsgesetz im Bereich Personalwesen ähnliche Überwachungsbefugnisse zugewiesen, wie dem Datenschutzbeauftragten (§ 80 BetrVG). Der Betriebsrat ist aber nicht nur Kontrollorgan, sondern er gestaltet die vom Arbeitgeber gewünschte Verarbeitung maßgebend über Betriebsvereinbarungen mit.

1.8.2 Der Datenschutzbeauftragte

Unternehmen haben nach § 38 BDSGneu einen betrieblichen Datenschutzbeauftragten zu bestellen, wenn **mehr als 9 Mitarbeiter** personenbezogene Daten erheben, speichern, nutzen, verarbeiten und/oder löschen.

Aufgabe des Datenschutzbeauftragten ist es, bei der Umsetzung der DSGVO sowie anderer Vorschriften des Datenschutzes im Hotel, ... fachkundig beratend zu unterstützen und ihre Beachtung zu überwachen. Er soll auf die Wahrung der Rechte der Betroffenen bei der Verarbeitung ihrer personenbezogenen Daten achten. Hierzu hat er fachkundig die Erstellung von betriebsinternen Verfahren, Anweisungen und Richtlinien (DSMS), die für die Umsetzung von technischen und organisatorischen Maßnahmen der DSGVO erforderlich sind, zu unterstützen.

Die DSGVO benennt insbesondere folgende Aufgaben:

- Unterrichtung und Beratung hinsichtlich der Datenschutzpflichten des Unternehmens und der Beschäftigten
- Ratgeber für Betroffene zu allen Fragen der Verarbeitung ihrer Daten und der Wahrnehmung ihrer Rechte
- Überwachung hinsichtlich
    - der Einhaltung der DSGVO und anderer Rechtsvorschriften
    - der „Strategien“ [interne Richtlinien], also des DSMS insbesondere in Bezug auf
        - die Zuweisung von Zuständigkeiten
        - die Sensibilisierung und Schulung der Mitarbeiter
        - die Überprüfung (Audits)
- Beratung bei der Datenschutz-Folgenabschätzung
- Zusammenarbeit mit der Aufsichtsbehörde

In den meisten Fällen wird der Datenschutzbeauftragte seine Aufgaben im Rahmen eines Arbeitsverhältnisses wahrnehmen. In kleineren Unternehmen wird er hierfür nur einen Teil seiner Arbeitszeit aufwenden dürfen. Bei der Bestellung zum Datenschutzbeauftragten ist darauf zu achten, dass sich kein Interessenskonflikt aus seiner eigentlichen Tätigkeit im Unternehmen ergibt, weil er sich zugleich kontrollieren muss (z.B. Leiter IT, HR, Controlling). Hier besteht ein gesetzliches Verbot!

Der Datenschutzbeauftragte ist weisungsfrei. Bei der Ausübung seiner Tätigkeit darf er keine Anweisungen bezüglich der Ausübung seiner Aufgaben erhalten. Diese Unabhängigkeit wird dadurch abgesichert, dass er einen Benachteiligungs- und Abberufungsschutz genießt, er kann nicht wegen der Erfüllung seiner Aufgaben abberufen werden. Zudem genießt der Datenschutzbeauftragte einen Kündigungsschutz (1 Jahr nach Abberufung).

Der Datenschutzbeauftragte kann intern oder extern bestellt werden, wobei eine externe Bestellung nicht nur hinsichtlich der Fachkunde und Haftungsfrage, sondern auch in der Transparenz der Kosten Vorteile mit sich bringt.

1.8.3 Die Aufsichtsbehörde

Neben den Beratungsaufgaben haben Aufsichtsbehörden Überwachungsfunktionen und weitreichende Sanktionsbefugnisse. So sind sie auch befugt, Bußgelder zu verhängen.

Die Aufgaben der Aufsichtsbehörden ergeben sich unmittelbar aus Art. 57 DSGVO. Die wesentlichsten und für den Hotelier relevantesten sind:

- Überwachung der Anwendung und Durchsetzung der DSGVO
- Befassung mit Beschwerden
- Befassung mit jeder sonstigen Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten

Zuständig ist grundsätzlich die Aufsichtsbehörde am Sitz des Unternehmens oder des Betroffenen. Nur dann, wenn die Verarbeitung der Daten in einem anderen Mitgliedsstaat der EU erfolgt, als der Verantwortliche seinen Sitz hat, bemisst sich die Zuständigkeit der Aufsichtsbehörde an dem sogenannten One-Stop-Shop-Prinzip. D.h. die federführende Aufsichtsbehörde bei grenzüberschreitender Verarbeitung ist grundsätzlich die Aufsichtsbehörde der sog. Hauptniederlassung des Verantwortlichen. Eine Ausnahme besteht nur für Verarbeitungen, die allein mit der Niederlassung in einem bestimmten Mitgliedstaat zusammenhängt oder nur Betroffene in einem bestimmten Mitgliedstaat erheblich beeinträchtigt, dann ist die Aufsichtsbehörde dieses Mitgliedstaates zuständig.

1.8.4 Instrumente der Selbstregulierung

Neben spezialgesetzlichen Regelungen eröffnet die DSGVO den verantwortlichen Stellen die Möglichkeit, durch eigene Regelungen den Datenschutz zu gestalten.

So ist in Unternehmen, wo es einen Betriebsrat gibt, eine klassische Form der Selbstregulierung die **Betriebsvereinbarung**. Hier werden Anforderungen im Umgang mit personenbezogenen Mitarbeiterdaten betriebsspezifisch konkretisiert. Danach sind Betriebsvereinbarungen zu beschränken auf „spezifische Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigungsdaten. Mitarbeiter sollen durch die Verarbeitung ihrer Daten im Rahmen einer Leistungs- und Verhaltenskontrolle nicht benachteiligt werden. So ist die Auswertung von Protokolldaten bei der Nutzung von E-Mail und Internetdiensten, dem Einsatz von Videokameras bis hin zu elektronischen Türschließsystemen zu regeln. Sollte es keinen Betriebsrat im Unternehmen geben, sind die Regelungen über **Richtlinien** zusammen mit **individuellen Nutzungsvereinbarungen** festzuschreiben.

Eine weitere Form der Selbstregulierung bilden **Unternehmens- bzw. Konzernregelungen** zum Datenschutz, sogenannte Binding Corporate Rules (BCR). Deren Rechtsnatur nach beinhalten sie eine Selbstbindung der konzernangehörigen Unternehmen in Bezug auf die Verarbeitung von personenbezogenen Daten.

Auch das in Art. 42 DSGVO geregelte **Datenschutzaudit** setzt als Prüfungsgegenstand eines Verfahrensaudits das Vorhandensein eines Datenschutzkonzepts voraus, welches im Wege der Selbstregulierung entwickelt werden muss.

Insbesondere Berufs- und Wirtschaftsverbände haben überdies die Möglichkeit, gemäß Art. 40 DSGVO ihre **Verhaltensregeln** zur Förderung des Datenschutzes durch die Aufsichtsbehörden genehmigen zu lassen.

Unternehmensintern können Verhaltensregeln im Rahmen eines **Code of Conducts** (Verhaltenskodex) für Mitarbeiter und Geschäftspartner aufgestellt werden.

1.9 Sanktionen bei Datenschutzverstößen

Die DSGVO gibt Personen unabhängig voneinander das Recht, sich bei einem (angenommenen) Datenschutzverstoß an eine Aufsichtsbehörde zu wenden sowie gegen die Verantwortlichen oder Auftragsverarbeiter vorzugehen.

Jede Person hat die Möglichkeit, bei einem vermuteten Verstoß gegen datenschutzrechtliche Bestimmungen und einer damit verbundenen Verletzung eigener Rechte das Recht, **Beschwerde bei einer Aufsichtsbehörde** einzulegen. Sollte dieses der Fall sein, wird sich die Aufsichtsbehörde mit dem Verantwortlichen schriftlich in Verbindung setzen und um Stellungnahme bitten. Zusammen mit der Stellungnahme wird die Aufsichtsbehörde Unterlagen aus der Dokumentation (siehe Pkt. 1.4), insbesondere zum Verfahrensverzeichnis bzw. zu Verträgen mit Auftragsverarbeitern anfordern und prüfen.

Neben der Beschwerde können Personen **zivilrechtlich** oder im Rahmen des **Verbandsklagerecht** gegen verantwortliche Stellen oder Auftragsverarbeiter **vorgehen**.

Führt ein Verstoß gegen Datenschutz zu einem materiellen oder immateriellen Schaden, so sind der Verantwortliche oder der Auftragsverarbeiter **schadensersatzpflichtig**. Für den Auftragsverarbeiter setzt die Haftung zusätzlich die Verletzung einer speziell auferlegten Pflicht aus der DSGVO oder eine Missachtung von rechtmäßig erteilten Anweisungen des Verantwortlichen voraus. Die Haftung setzt Verschulden voraus, das vermutet wird, wenn der Verantwortliche sich nicht entlasten kann. Mehrere Beteiligte (Verantwortliche und Auftragsverarbeiter) haften als Gesamtschuldner, deren interner Ausgleich richtet sich nach deren jeweiligen Verantwortung.

Die DSGVO sieht bei Verstößen gegen die datenschutzrechtlichen Bestimmungen **Bußgelder von 10 Mio. EURO oder bis zu zwei Prozent** des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres (Art. 83 Abs. 4 DSGVO) vor.

Hierzu zählen insbesondere Verstöße gegen:

- Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft (Art. 8)
- Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist (Art. 11)
- Pflichten für Verantwortliche und Auftragsverarbeiter (Artt. 25 – 31) inkl. datenschutzfreundliche Voreinstellungen, Vertragsverhältnis Auftragsverarbeitung und Verzeichnis von Verarbeitungstätigkeiten
- Sicherheit der Verarbeitung (Art. 32)
- Meldung von Datenschutzverletzungen (Artt. 33, 34)
- Datenschutz-Folgenabschätzung (Artt. 35, 36)
- Benennung Datenschutzbeauftragten (Artt. 37 – 39)
- Zertifizierung (Artt. 42, 43)

Andere Verstöße folgen derselben Systematik. Allerdings verdoppeln sich die Höchststrafen auf **vier Prozent bzw. 20. Mio. EURO**. Hierzu zählen insbesondere Verstöße gegen:

- Grundsätze der Verarbeitung (Art. 5)
- Rechtmäßigkeit der Verarbeitung (Art. 6)
- Bedingungen für die Einwilligung (Art. 7)
- Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9)
- Rechte der Betroffenen (Artt. 12 – 22)
- Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen (Artt. 44 – 49)
- Anweisungen und Auflagen der Aufsichtsbehörden (Art. 58 Abs. 1, 2)

Ein Datenschutzverstoß wird von der Aufsichtsbehörde nur auf Antrag verfolgt. So kann es lange gut gehen, mit personenbezogenen Daten wissentlich bzw. unwissentlich unsachgemäß umzugehen. Erst wenn das Kind in den Brunnen gefallen ist, sieht man sich neben möglichen Imageverlusten auch hohen Geldstrafen und Schadensersatzansprüchen bis hin zu Freiheitsstrafen (2-3 Jahre gemäß § 42 BDSGneu) gegenüber.

Art. 82 Abs. 1 DSGVO sieht vor, dass jede Person einen Anspruch auf Schadenersatz hat, wenn aufgrund eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist. Die Anwendungsfälle sind vielseitig. Beispiele dafür sind die Zugänglichmachung von Daten einer betroffenen Person für Dritte ohne Einwilligung, unzulässige Videoüberwachung, das Bereitstellen von Fotos in sozialen Medien ohne Einwilligung, Identitätsdiebstahl, die unautorisierte Kontaktaufnahme zu Marketingzwecken sowie überhaupt jegliche Form der rechtswidrigen Datenverarbeitung.

Die Sanktionsbestimmungen der DSGVO richten sich grundsätzlich gegen Verantwortliche bzw. Auftraggeber, also gegen die Unternehmen selbst. Beschäftigte müssen mit Sanktionen rechnen, wenn sie vorsätzlich eine Ordnungswidrigkeit oder Straftat im Zusammenhang mit der Verarbeitung oder Weitergabe von personenbezogenen Daten begehen (Erwägungsgrund 148).

Die Geschäftsführung ist verantwortlich und haftet persönlich bei Verstößen gegen die datenschutzrechtlichen Bestimmungen, wenn sie keine Maßnahmen zum Datenschutz getroffen hat.

- Datenschutz dient dem Schutz natürlicher Personen (insbesondere Interessenten, Gäste, Mitarbeiter und Firmenkontakte) bei der Verarbeitung und Übermittlung von Daten, um deren Persönlichkeitsrechte und Privatsphäre zu stärken und das Recht auf informationelle Selbstbestimmung zu wahren.
- Datenschutz gilt für natürliche oder juristische Personen, Behörden sowie andere Einrichtungen (z.B. Vereine, ...).
- Von Relevanz sind personenbezogene (bestimmte oder bestimmbare) und identifizierbare Daten natürlicher Personen, die ganz oder teilweise automatisiert verarbeitet oder in Dateisystemen gespeichert werden.
- Betroffenenrechte beinhaltet insbesondere das Recht auf Auskunft, Recht auf Richtigstellung und Löschung bzw. Sperrung sowie das Recht auf Widerspruch.
- Kontrollorgane sind Datenschutzbeauftragte, die Datenschutzbehörde , Verbraucherverbände und ordentliche Gerichte.
- Aufsichtbehörden können Bußgelder bis zu 20 Mio. EURO oder 4 Prozent des weltweiten Jahresumsatzes (je nachdem, was höher ist) verhängen. Hinzu kommen evtl. Schadensersatzforderungen, Imageschäden oder Freiheitsstrafen.

- ✓ Benötigen wir einen Datenschutzbeauftragten?
- ✓ Unter welchen Voraussetzungen können wir personenbezogene Daten speichern?
- ✓ Wie sichern wir den Betroffenen (Gäste, Mitarbeiter) ihre Rechte zu?
- ✓ Wie speichern und bewahren wir jegliche Daten auf?
- ✓ Werden sicherheitsaspektliche Belange beachtet?
- ✓ Werden die Aufbewahrungsfristen eingehalten?

2 Umgang mit Gast- und Mitarbeiterdaten

Zielfragen

- Wie geht man mit Gast- und Mitarbeiterdaten gesetzeskonform um?
- Was habe ich bei der Auswahl der Hotelsoftware zu beachten?
- Wie gehe ich mit Kreditkartendaten um?
- Was steckt hinter der Meldepflicht?
- Darf ich einen Personalausweis kopieren?
- Was muss ich bei der Videoüberwachung beachten?
- Hafte ich für eine gesetzeswidrige Internetnutzung durch meinen Gast?

2.1 Gastdaten

Als Hotelier dürfen Sie nur jene Daten Ihrer Gäste speichern und verwenden, die Sie für die Erfüllung des Beherbergungsvertrags benötigen. Dabei sind sowohl die Datenschutzgrundsätze Datenminimierung und Zweckbindung zu beachten als auch die Speicherbegrenzung. Es darf eine Speicherung nur so lange erfolgen, als dies zeitlich erforderlich ist und der Zweck nicht entfallen ist.

2.1.1 Anforderungen an die Hotelsoftware

Die zentrale Speicherung und Verwaltung von Gastdaten erfolgt in der Hotelsoftware. Bei der Suche nach einem guten Hotelmanagement System sollten neben den hotelspezifischen Funktionalitäten auch immer datenschutzrechtliche Anforderungen berücksichtigt werden. Sie sind als Hotelier für die ordnungsgemäße Datenverarbeitung verantwortlich und können sich nicht auf den Standpunkt zurückziehen, dass das eingesetzte System leider nicht über erforderliche, datenschutzkonforme Funktionalitäten verfügt. Bereits bei der Auswahl des einzusetzenden Systems sind diese Funktionalitäten zu berücksichtigen. Die Durchführung einer Datenschutz-Folgenabschätzung (siehe dazu Kap. 4.3) dokumentiert unter anderem auch den Entscheidungsprozess. Welche Funktionalitäten und gesetzliche Anforderungen Sie auf jeden Fall prüfen sollten, werden nachfolgend beschrieben:

1. Kleine Hotels haben andere Anforderungen als Häuser mit 50 oder mehr Zimmern. Während kleine Häuser eher ein einfaches, **webbasiertes Hotelverwaltungssystem** einsetzen, arbeiten größere Hotels und Hotelketten mit einem **Property Management System (PMS)**, eine Hotelsoftware für die Zimmerreservierung und Abrechnung von Leistungen und Beeinflussung von Kassensoftware und anderen Peripheriegeräten. Zunächst ist zu klären, wo sich die Daten befinden, ist der **Standort der Datenbank/des Systems** direkt im Hotel oder werden die Daten auf Servern von Dienstleistern gehostet?

   Befinden sich die Daten auf den eigenen Servern im Hotel, muss sichergestellt sein, dass kein Unbefugter sich Zutritt und Zugang zu den Servern verschaffen kann. Es sind strenge Anforderungen an die Einrichtung eines

Serverraums umzusetzen, um die Vertraulichkeit und Integrität (Grundsätze der Datenverarbeitung) zu gewährleisten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt hierzu eindeutige Handlungsempfehlungen. Ein fehlendes Platzangebot für den sicheren Standort von Servern wird nicht akzeptabel sein. In diesem Fall sollten Überlegungen getroffen werden, die Daten dezentral in einem Rechenzentrum eines Dienstleisters zu hosten. Dienstleister kann sowohl der Anbieter des Hotelmanagement Systems als auch ein Spezialanbieter für Hosting (Betreiber von Rechenzentren) sein. Bei der Auswahl des Hosters ist darauf zu achten, dass die Daten innerhalb der EU oder einem sicheren Drittstaat gespeichert werden und eine Datenübermittlung in ein unsicheres Drittland (wie z.B. USA, Russland, China) ausgeschlossen werden können. Ist dennoch eine Datenübermittlung bzw. Datenspeicherung in ein Drittland geplant, so sind die Anforderungen gemäß Artt. 46, 47 DSGVO umzusetzen.

2. Eng verbunden mit der Auswahl des Dienstleisters ist auch die Regelung für eine nachfolgende **Betreuung des Hotelmanagement-Systems**, dem Support. Es reicht bereits aus, dass der Systemanbieter im Rahmen von (Fern-) Wartungsarbeiten die Möglichkeit erhält, personenbezogene Daten zur Kenntnis zu nehmen. In diesem Fall ist mit dem Systemanbieter als Auftragsverarbeiter eine Datenschutzvereinbarung abzuschließen, die Modalitäten zum Fernzugriff sind zu regeln. (Art. 28 DSGVO i.V.m. Art. 4 Nr. 2 DSGVO)

   Für das Hosting von Daten innerhalb der EU ist eine Datenschutzvereinbarung abzuschließen, wenn der Hoster die Möglichkeit erhält, Daten bei Wartungsarbeiten oder bei der Datensicherung einzusehen. Zu berücksichtigen sind Datenbanken aber auch Daten von Fileservern (Dateien).

   Fragen Sie Ihren Systemanbieter bzw. Hoster nach einer Datenschutzvereinbarung. Sollten er Ihnen keine bereitstellen können, sind das schon die ersten Hinweise darauf, dass der Datenschutz keinen hohen Stellenwert hat. Allerdings ist der Auftragsverarbeiter auch nicht verpflichtet, Ihnen eine entsprechende Vereinbarung zur Verfügung zu stellen. Als Auftraggeber sind Sie dafür verantwortlich, eine Vereinbarung nach den Vorgaben der DSGVO abzuschließen und alle erforderlichen technischen und organisatorischen Maßnahmen, insbesondere bei Wartungsarbeiten, der Vertraulichkeit (Verschlüsselung), der Speicherfristen und ggf. der Datensicherung, festzulegen.

   Nur wenn ausgeschlossen werden kann, dass der Dienstleister keine Möglichkeit hat, die Daten einzusehen (z.B. Verschlüsselung), kann auf eine Datenschutzvereinbarung verzichtet werden.

3. Nach den datenschutzrechtlichen Bestimmungen sind **personenbezogene Daten** zu **löschen**, wenn der Zweck der Verarbeitung weggefallen ist. Dem gegenüber stehen oft Aufbewahrungsfristen, die einzuhalten sind. In diesem Fall schreibt der Gesetzgeber vor, dass die Daten zu sperren sind. Schlussfolgernd empfiehlt es sich, den Zugriff auf Gastdaten spätestens ein Monat nach Abreise (es gibt keine Forderungen mehr seitens des Hotels) für die Benutzer des Hotelmanagement Systems zu entziehen, also automatisiert zu sperren. Das lässt sich natürlich schwer in einer Hotelsoftware darstellen, da bei wiederholten Besuchen

   Zu berücksichtigen ist das Recht des Gastes, die Verarbeitung seiner Daten einzuschränken (Art. 18 DSGVO). Widerspricht ein Gast der Datennutzung, muss systemseitig sichergestellt werden, dass seine Daten händisch gesperrt (deaktiviert) werden können. Auch ein teilweiser Widerspruch, z.B. bei der Nutzung seiner E-Mail-Adresse oder Anschrift zu Werbezwecke ist umzusetzen.

eine Gästehistorie aufgebaut werden soll. Aus diesem Grund ist bei der Wahl des Systems darauf zu achten, dass die ständigen Zugriffsrechte für die Reservierung, aber auch Sales & Marketing gewährleistet werden können. Mit einer wiederholten Buchung werden so die Gastdaten wieder aktiviert, bis dahin haben aber das Front Office, Housekeeping etc. keine Möglichkeit, die Gastdaten abzurufen.

Gastdaten sind auch dann regelmäßig zu löschen, wenn Gäste z.B. nicht angereist sind und es keine Verpflichtung gibt, diese aufzubewahren (z.B., weil es keinen steuerrechtlichen Vorgang gab). Sind steuerrechtliche Aufbewahrungsfristen zu berücksichtigen, sind die Gastdaten spätestens nach 10 Jahren zu löschen.

4. Insbesondere **Hotelketten** setzen ein PMS mit dem Ziel ein, auf eine **gemeinsame Datenquelle** zuzugreifen. So sollen unterschiedliche Hotels die Möglichkeit erhalten, auf bereits gespeicherte Gastdaten aus einem anderen Partnerhotel zuzugreifen, um ggf. Sonderwünsche im Vorfeld zu berücksichtigen. Auch hier wird i.d.R. eine Gästehistorie aufgebaut.

   Unabhängig davon, dass die oben genannten Anforderungen zu erfüllen sind, ist darauf zu achten, dass das jeweilige Hotel nur die eigene Gästehistorie einsehen kann. Eine gemeinsame Nutzung der Daten ist nur in einem begrenzten Umfang möglich.

   Eine **gemeinsame Nutzung von personenbezogenen Daten** setzt voraus, dass eine Vereinbarung auf Grundlage von Art. 26 DSGVO zwischen den Verantwortlichen getroffen wird. Es gibt kein Konzernprivileg!

   Der Gast ist mit der ersten Speicherung unter anderem auch darüber in Kenntnis zu setzen, dass mehrere Hotels auf seine Daten zugreifen können. Er ist auf sein Widerspruchsrecht hinzuweisen. In diesem Fall ist zu prüfen, ob er generell der Datennutzung widerspricht oder nur der Datenübermittlung an die Partnerhotels. Das Hotelmanagement-System sollte diese Anforderungen berücksichtigen.

5. Neben einem ordentlichen **Passwortmanagement** (elektronische Vorgaben zu Länge und Komplexität des Passwortes, Passwortwechsel, automatisiertes Abmelden nach x min., Sperren bei x Fehleingaben, ...) sollten **Benutzerrechte** in Abhängigkeit von Positionen (z.B. Front Office, Front Office Manager, Front Office Nightshift, Front Office Azubi, Reservierung, ...), auch individuell definiert und vergeben werden können. Hier sind insbesondere die Zugriffsrechte auf Kreditkartendaten (anonymisiert oder Klartext) aber auch zum Datenexport stark einzuschränken und durch die Hotelleitung individuell zu genehmigen.

   Für jeden Mitarbeiter/Benutzer ist ein individueller Zugang mit entsprechenden Zugriffsrechten einzurichten. Die Vergabe, Freigabe, Änderung und Löschung der Benutzerrechte ist für jeden Benutzer zu dokumentieren und 10 Jahre aufzubewahren.

6. Auf Grund der Vertraulichkeit und zur Integrität der gespeicherten Daten im Hotelmanagement System hat der Systemanbieter sicherzustellen, dass im Hintergrund **jede Aktivität von jedem Benutzer protokolliert** wird und durch den Systemadministrator abgerufen werden kann.

   Die Benutzer sind darüber zu belehren, sich vom Hotelmanagement-System abzumelden, wenn sie den Computerarbeitsplatz verlassen sowie das die Weitergabe ihres Passwortes nicht gestattet ist.

2.1.2 Reservierung

Bereits bei der Reservierung erhält das Hotel umfangreiche Daten über den Gast. Die Daten, die über die unterschiedlichsten Kommunikationskanäle zum Hotel gelangen, sind zu meist Namen, Anschrift, Kontaktdaten, Kreditkartennummern und Wünsche. Alle Informationen werden in die Hotelsoftware übernommen, zum Vorgang erhaltene oder ausgedruckte Unterlagen werden zusätzlich in Reservierungsordnern abgelegt und wenn die Anfrage über E-Mail eingehen, werden diese zusätzlich im Mail-Account gespeichert.

Im Rahmen eines **vorvertraglichen Geschäftsverhältnisses** können die Reservierungsdaten gespeichert werden, wobei zu beachten ist, dass die Daten bei einer kostenfreien Stornierung wieder zu löschen sind. Nachfolgend möchten wir insbesondere die Punkte benennen, auf die Sie als Hotelier immer zu achten haben, um eine sichere Datenverarbeitung zu gewährleisten:

1. Wenn Sie auf Ihrer Webseite ein **Onlinereservierungssystem** eingebunden haben, sollte die Eingabe und Übermittlung der **Reservierungsdaten verschlüsselt** (https://...) erfolgen. Fragen Sie auch hier nur den Umfang an Daten ab, den Sie für die Reservierung benötigen.

   Mit der Erhebung der Reservierungsdaten müssen die Buchenden nach Art. 13 DSGVO **(Informationspflicht bei Erhebung personenbezogener Daten)** darüber informiert werden, welche Daten zu welchem Zweck erhoben werden, wann diese gelöscht und ob die Daten ggf. an Dritte übermittelt werden (auch wenn das Onlinereservierungssystem über einen externen Dienstleister betrieben wird bzw. die Daten innerhalb einer Hotelgruppe genutzt werden sollten). Zusätzlich sind die Buchenden über ihre Rechte (Auskunft, Berichtigung, Löschung, Widerspruch, Datenübertragbarkeit sowie Beschwerderecht bei der Aufsichtsbehörde) zu informieren. Die Informationen werden üblicherweise in der **Datenschutzerklärung auf der Webseite** bereitgestellt. Als Webseitenbetreiber müssen Sie sicherstellen, dass Sie Ihrer Informationspflicht nachgekommen sind. Hier empfiehlt es sich, mit Abschluss der Eingabe der Reservierungsdaten einen Kurztext zum Datenschutz (inkl. Link zur Datenschutzerklärung) mit Kontrollkästchen zu integrieren. Nur mit Bestätigung des Kontrollkästchens sollte nachfolgend die Reservierung erfolgen.

Wenn das Onlinereservierungssystem von einem Dienstleister integriert und betrieben wird, ist eine Datenschutzvereinbarung mit diesem abzuschließen. Reservierungsdaten im Online-Reservierungssystem sollten zeitnah gelöscht werden.

Denken Sie auch daran, den Dienstleister in der Datenschutzerklärung auf der Hotelwebseite aufzuführen, wenn die Reservierungsdaten auf den Servern des Dienstleisters gespeichert werden.

Textbeispiel zur Datenverarbeitung durch das Online-Buchungssystem auf der Webseite

Hinweis zum Datenschutz: Wir sind sehr darum bemüht, all unseren Kunden und Besuchern unserer Webseite einen ausgezeichneten Service zu bieten. Dazu gehört auch der Schutz Ihrer Daten. Wenn Sie von unseren Webseiten eine Online-Buchung vornehmen, so geschieht das durch das Online-Reservierungssystem *xyz*, dessen Anbieter unser Vertragspartner ist. Alle von Ihnen eingegebenen Daten werden grundsätzlich verschlüsselt übertragen. Unser Vertragspartner hat sich zum datenschutzgerechten Umgang mit Ihren übermittelten Daten verpflichtet. Er ergreift alle organisatorischen und technischen Maßnahmen zum Schutz Ihrer Daten. Weitere Informationen zur Erhebung und Verarbeitung personenbezogener Daten können Sie unserer Datenschutzerklärung entnehmen.

☐ Ich bin damit einverstanden, dass meine Daten zum Abschluss dieser Reservierung elektronisch gespeichert werden.

2. Ein Großteil der Reservierungen erfolgt über die zahlreichen **Hotelreservierungsportale (OTAs).** Auch wenn der Betreiber des jeweiligen Systems selber für die Umsetzung der datenschutz- und datensicherheitstechnischen Anforderungen verantwortlich ist, muss die Reservierung sehr vertrauensvoll mit den Zugangsdaten umgehen. Hier empfiehlt es sich, ein Passwortmanagement (Ort der Speicherung inkl. Zugriffsbeschränkungen, Komplexität, Zyklen des Passwortwechsels) festzulegen.

   Andererseits läuft das Hotel Gefahr, bei einem unerlaubten Zugriff auf die Daten durch den Betreiber auf Schadenersatz wegen Vertragsverletzung und Fahrlässigkeit verklagt zu werden.

Da die Betreiber der Hotelreservierungsportale im eigenen Namen agieren, muss hier keine Datenschutzvereinbarung abgeschlossen werden.

3. **Reservierungen über E-Mail und Telefon** werden direkt entgegengenommen und bearbeitet. Sofern E-Mails ausgedruckt und im Reservierungsordner abgelegt werden, sollte die E-Mail aus dem Postfach gelöscht werden.

Denken Sie daran, dass die E-Mails auch aus dem Ordner „Gelöschte Elemente“ entfernt werden.

4. Zu beachten sind die **Informationspflichten nach Art. 14 DSGVO**, wenn der Buchende nicht direkt bei der Erhebung seiner Daten informiert werden konnte. Das ist dann der Fall, wenn die Buchung über ein Hotelreservierungsportal, über ein Reisebüro, per E-Mail, Fax, Telefon etc. erfolgte. Sofern die Buchungsdaten in das Hotelmanagementsystem übernommen werden, ist der Buchende über die Datenspeicherung und -nutzung (wie im ersten Punkt beschrieben) zu informieren. Mit der Buchungsbestätigung sollte die Information schriftlich und nachweislich erfolgen.

   Ist es nicht möglich der Informationspflicht nachzukommen, weil keine Adress- und/oder Kontaktdaten vom Gast vorliegen, so ist der Gast bei Anreise über die Datenverarbeitung in Kenntnis zu setzen. Soweit aber eine Kontaktaufnahme möglich wäre (z.B. über das Portal eines OTAs mit einem systeminternen E-Mail-Account), ist der Gast über die Datenspeicherung im Rahmen einer Pre-Stay-E-Mail zu informieren. Bei Kenntnis der Adressdaten kann der Gast auch per Post angeschrieben und informiert werden.

5. Auch die **Reservierungsordner** unterliegen einer hohen Vertraulichkeit. So empfiehlt es sich insbesondere dann, wenn im Ordner Kreditkartendaten enthalten sind, die Reservierungsunterlagen unter Verschluss zu halten (in der Reservierung, im Front Office aber auch im Archiv).

2.1.3 Check-In

Es empfiehlt sich einen Diskretionsbereich an der Rezeption einzurichten, wenn es häufiger vorkommt, dass viele Gäste zugleich einchecken.

Mit der Anreise des Gastes geht das vorvertragliche Geschäftsverhältnis in ein Vertragsverhältnis über, d.h. spätestens ab diesen Zeitpunkt sind handels- und steuerrechtliche Aufbewahrungsfristen zu berücksichtigen. Mit dem Einchecken werden alle offnen Fomalitäten erledigt. Der Gast füllt seinen **Meldeschein** aus und bezahlt eventuell schon vorab sein Zimmer bzw. er hinterlässt Zahlungsdaten, wie seine Kreditkartennummer. Überlegen Sie sich rechtzeitig, welche Gastdaten Sie über die Erfüllung des Beherbergungsvertrages hinaus verarbeiten möchten und daher eine Einwilligung durch den Betroffenen benötigen. Im zweiten Schritt prüfen Sie, zu welchem Zeitpunkt die Einwilligung eingeholt werden kann (z.B. bei der Reservierung oder bei Check-In) und ob mehrere Verarbeitungszwecke auf einem Einwilligungsblatt eingeholt werden können (z.B. Newsletter, aber auch die Speicherung von sensiblen Daten). Soweit dieses auf dem Meldeschein vorgesehen ist, sind diese separat und unabhängig von den Meldedaten einzuholen. Es besteht eine besondere Kennzeichnungspflicht!

Textbeispiel für den Datenschutzhinweis auf dem Meldeschein

Hotel xyz respektiert Ihre Privatsphäre. Unser Unternehmen speichert und verwendet personenbezogene Daten nur im Rahmen der gesetzlichen Bestimmungen nach der Datenschutz-Grundverordnung (DSGVO) und dem BDSGneu (Bundesdatenschutzgesetz). Gerne können Sie jederzeit bei *Hotel xyz* erfragen, welche persönlichen Daten *Hotel xyz* über Sie gespeichert hat und diese entsprechend korrigieren oder löschen lassen.

Hotel xyz respects your privacy. Our company stores and utilizes personal data in strict accordance with the General Data Protection Regulation (GDPR) and the new German Federal Data Protection Act. You can contact *Hotel xyz* at any time to find out which personal data the company has stored about you and to have such data corrected or deleted accordingly.

Textbeispiel für eine Einwilligungserklärung

☐ Ich bin an Angebote und Neuigkeiten vom *Hotel xyz* interessiert. Ich erkläre mich damit einverstanden, dass mein Name, meine Adresse und meine E-Mail-Adresse zur Übersendung von Informationsmaterial von *Hotel xyz* verwendet werden kann. Ich bin damit einverstanden, Informationen von *Hotel xyz* auch per E-Mail zu erhalten. Ich weiß, dass ich meine Einwilligung jederzeit widerrufen kann.

I am interested in receiving special offers from and news of *Hotel xyz*. I agree that my name, address and email address will be used for sending information material from *Hotel xyz*. I agree to receive information about *Hotel xyz* via email. I can revoke my consent to use of data at any time.

Das Front Office hat darauf zu achten, dass die Unterlagen nach ihrer Bestimmung getrennt und sicher aufbewahrt werden. Insbesondere ist auf eine Trennung nach Meldeschein, Reservierungsunterlagen und Abrechnungsunterlagen (Rechnung inkl. Händlerbeleg) zu achten. Wenn die **Händlerbelege** Angaben zu den Kontodaten des Gastes (z.B. Kreditkartennummer) enthalten, sind diese zwingend verschlossen aufzubewahren. Aus datenschutzrechtlichen Gründen und dem damit verbundenen hohen Risiko eines Missbrauchs empfiehlt sich die Anonymisierung der Kreditkartendaten auch auf dem Händlerbeleg.

Personalausweise von Gästen dürfen nicht kopiert, gescannt oder einbehalten werden. Sofern ein Mitarbeiter vom Front Office einem Gast misstraut (z-B. beim Walk-in), kann dieser sich maximal den Ausweis zeigen lassen, um die Daten mit dem Meldeschein abzugleichen.

2.1.4 Der Meldeschein

Seit dem 01.11.2015 ist das neue bundesweite Meldegesetz in Kraft getreten.

Als große Erleichterung wurde das Ausfüllen des Meldescheines vorab durch die bereits gespeicherten Daten in der Hotelsoftware angesehen. Damit bleiben für den Gast lediglich das Ausfüllen der offenen Pflichtfelder und die händische Unterschrift, die auch weiterhin notwendig ist. Darüber hinaus entfällt die Nutzungspflicht bestimmter Meldescheinformulare, sodass eine IT-basierte Umsetzung erleichtert wird.

Folgende Inhalte sind im zukünftigen Bundesmeldegesetz §§ 29-31 verankert:

1. Nach § 29 Abs. 2 haben alle Personen am Tag der Ankunft einen besonderen Meldeschein handschriftlich zu unterschreiben. Fehlende Pflichtangaben sind zu ergänzen.

2. Mitreisende Angehörige sind nur der Zahl nach anzugeben.

3. Bei Reisegesellschaften mit mehr als 10 Personen hat nur der Reiseleiter den Meldeschein zu unterschreiben, es sind die Anzahl und die Staatsangehörigkeiten der Mitreisenden anzugeben.

4. Folgende Daten sind Pflichtangaben:
   a. Datum der Ankunft und der voraussichtlichen Abreise
   b. Familienname
   c. Vornamen
   d. Geburtsdatum
   e. Staatsangehörigkeiten
   f. Anschrift
   g. Zahl der Mitreisenden und ihre Staatsangehörigkeit (bei Reisegruppen)
   h. Seriennummer des anerkannten, gültigen Passes bei ausländischen Gästen

Sollte auf dem Meldeschein über die oben genannten Pflichtangaben weitere Angaben (z.B. E-Mail-Adresse, Kfz-Kennzeichen für Garage) abgefragt werden, sind diese gesondert als *„freiwillig“* zu kennzeichnen.

5. Beherbergte ausländische Gäste haben ein gültiges Identitätsdokument (anerkannter gültiger Pass oder Passersatz) vorzulegen. Sollten sich Abweichungen ergeben, sind diese auf dem Meldeschein zu notieren.

Legen ausländische Personen kein oder kein gültiges Identitätsdokument vor, ist dies auf dem Meldeschein zu vermerken.

6. Durch Landes- und Kommunalrecht kann bestimmt werden, welche zusätzlichen Daten bzgl. Fremdenverkehrs- und Kurbeiträgen notwendig sind.

7. Die Meldescheine sind vom Tag der Anreise 1 Jahr aufzubewahren und innerhalb von 3 Monaten nach Ablauf der Aufbewahrungsfrist zu vernichten.

8. Die Meldescheine sind so aufzubewahren, dass kein Unbefugter Einsicht nehmen kann.

9. Auf Verlangen sind die Meldescheine den genannten Behörden zur Einsichtnahme vorzulegen:
   - Polizeibehörden des Bundes und der Länder,
   - Staats- und Amtsanwaltschaften,
   - Gerichte, soweit sie Aufgaben der Strafverfolgung, der Strafvollstreckung oder des Strafvollzugs wahrnehmen,
   - Justizvollzugsbehörden,
   - Zollfahndungsdienst,
   - Hauptzollämter oder
   - Finanzbehörden, soweit sie strafverfolgend tätig sind.

Meldescheine dürfen außerdem zur Aufklärung des Schicksals von Vermissten und Unfallopfern, für die Erhebung von Fremdenverkehrs- und Kurbeiträgen, zur Ausstellung kommunaler Gästekarten sowie für die Beherbergungs- und die Fremdenverkehrsstatistik verarbeitet und genutzt werden.

2.1.5 Kreditkartendaten

Es gibt eine besondere Meldepflicht gegenüber der Aufsichtsbehörde für Datenschutz, wenn es zu einem Missbrauch oder Diebstahl von Kreditkartendaten gekommen ist. Soweit die Daten nicht verschlüsselt wurden, reicht ein Verdacht bereits aus.

Kreditkartendaten sind vom Gesetzgeber als besonders vertrauenswürdig eingestuft worden. Von daher empfiehlt es sich, feste Vorgaben im Umgang mit den Kreditkartendaten festzulegen und die Mitarbeiter regelmäßig zum Umgang zu belehren. Insbesondere ist darauf zu achten, dass:

- Kreditkartendaten nach Abreise des Gastes gelöscht werden. (spätestens nach 30 Tagen, im Online-Reservierungssystem auf der eigenen Webseite 7 Tage nach Buchung)
- Kreditkartendaten verschlüsselt gespeichert werden. (Fragen Sie Ihren Zahlungsdienstleister auch nach Tokenization, dabei werden die Kreditkartendaten durch Zahlenkombinationen sog. Token ersetzt)
- die Benutzerrechte im Zugriff auf die Kreditkartendaten in der Hotelsoftware stark eingeschränkt sind. (Anonymisierung)
  - dass ausgedruckte Kreditkartendaten immer unter Verschluss aufbewahrt werden. (Rechnungen, Archiv, Reservierungsunterlagen, ...)

2.1.6 Aufenthalt

Wie bereits in der Einleitung erwähnt, erfährt das Hotel vom Check-In bis zum Check-Out sehr viel Persönliches über seine Gäste, unter Umständen sogar zu gesundheitlichen Aspekten. Dies ist beim Umgang mit diesen Daten zu berücksichtigen, um die Persönlichkeitsrechte der Gäste zu schützen.

Gastronomie & Service

All diejenigen personenbezogenen Daten, die für die Leistungserbringung durch das Hotel erforderlich sind, dürfen auf Basis einer gesetzlichen Erlaubnis, nämlich auf der Basis des Beherbergungsvertrages, erhoben, verarbeitet und genutzt werden. So ist es zulässig, wenn ein Hotel zwecks **späterer Rechnungslegung** Informationen über konsumierte Getränke und Speisen (Minibar oder Restaurant) zu einem Gast erhebt und speichert. Gleiches gilt für die Inanspruchnahme weiterer kostenpflichtiger Dienste (Internet, Telefon, Pay-TV) oder Angebote (Wellness-Leistungen, Events, Ausflüge). Sensible Daten, wie z.B. Lebensmittelunverträglichkeiten dürfen nur dann gespeichert werden, wenn vom Gast eine Einwilligung vorliegt. (siehe dazu „Aufnahme von Gastwünschen und Informationen in die Hotelsoftware“)

Videoüberwachung

In vielen Hotels ist die Installation und Inbetriebnahme von Videoüberwachungen bereits durchgeführt oder noch geplant. Als Verantwortlicher ist der Hotelier verpflichtet, eine Videoüberwachung gesetzeskonform zu betreiben bzw. auch zu implementieren.

Elektronische Türschließsysteme

Das elektronische Türschließsystem dient in erster Linie als „Schlüsselersatz“ zum Betreten von Hotelzimmern und anderen nichtöffentlichen Bereichen im Hotel. Die Programmierung und Protokollierung des Türschließsystems und der Türschließkarten dient ausschließlich dem **Zutrittsmanagement** von Räumen. Eine zusätzliche Nutzung der Daten für andere Zwecke als der Fehleranalyse, Aufklärung von Sachverhalten und in Ausnahmefällen der Strafverfolgung ist nur eingeschränkt erlaubt.

Protokolldaten dürfen nicht zur Leistungs- und Verhaltenskontrolle von Mitarbeitern oder Dritten genutzt werden. Im Rahmen der Aufklärung von Straftaten hat der Hotelier die Persönlichkeitsrechte seiner Mitarbeiter oder anderer Dritter zu berücksichtigen. So sind ausgelesene Protokolldaten, die Rückschlüsse auf eine oder mehrere Personen zum Betreten eines Raumes ermöglichen, nur auf der Grundlage einer richterlichen Anordnung an die Strafverfolgungsbehörden herauszugeben. Eine Weitergabe der Protokolldaten in anonymisierter Form ist bereits vorab zur Klärung des Sachverhaltes möglich.

Aufnahme von Gastwünschen und Informationen in die Hotelsoftware

Um Gästewünsche und Erwartungen erfüllen zu können werden deren Bedürfnisse als auch Vorlieben notiert und in der Hotelsoftware vermerkt. Die Anmerkungen sind von unterschiedlicher Natur. Sie können einerseits belanglos sein, z.B. dass der Gast gerne zusätzliche Polster hätte oder eine bestimme Zeitung am Frühstückstisch bis hin zu sensiblen persönlichen Daten wie z.B. Allergien. Um diese Daten datenschutzkonform verarbeiten zu dürfen, ist eine ausdrückliche Zustimmung vom Gast einzuholen.

Beachten Sie weiters, dass in der Hotelsoftware nur die Mitarbeiter die Einsicht auf die Gastwünsche und Anmerkungen haben, die für die Erfüllung dieser verantwortlich sind. Weiters empfehlen wir, dass in der Datenschutzerklärung auf der Webseite als auch bei der Informationspflicht angeführt wird, dass das Hotel die Wünsche und Bedürfnisse speichert, um diese erfüllen zu können.

Dies kann bereits zu einem im Rahmen der Reservierung über Ihr Buchungsportal geschehen, per Mail bei der Übermittlung der Reservierungsbestätigung oder direkt vor Ort beim Check-In.

Internetnutzung

Hotels, die ihren Gästen die Möglichkeit bieten, per LAN bzw. WLAN im Internet zu surfen, haben die Anforderungen des Telekommunikationsgesetzes (TKG) und Telemediengesetzes (TMG) zu beachten. Insbesondere sind die Pflicht zur Wahrung des **Fernmeldegeheimnisses** (§ 88 TKG) sowie die in §§ 91 ff. TKG enthaltenden Datenschutzregelungen umzusetzen.

Als Anbieter eines öffentlichen WLAN-Netzes gilt das Hotel als Diensteanbieter und unterliegt somit dem Telemediengesetz. Zur Bereitstellung der Mediendienste gelten folgende Vorschriften im Zusammenhang mit dem Datenschutz:

- § 12 TMG **|** personenbezogene Daten dürfen seitens des Diensteanbieters nur zum Zweck der **Bereitstellung der Telemedien** erhoben werden. Eine Verwendung für andere Zwecke bedarf der Einwilligung des Betroffenen, also des Gastes (siehe dazu Art. 5 DSGVO). Die Einwilligung muss jederzeit für die Zukunft widerrufbar sein.
- § 13 TMG **| Der Anbieter hat den Nutzer** zu Beginn des Nutzungsvorganges, also mit Anmeldung zum WLAN-Netz über Art, Umfang und Zweck der Verarbeitung der Daten sowie über die Übermittlung in ein Drittland (außerhalb der EU) **zu informieren** (siehe dazu Art. 13 DSGVO). Der Inhalt der Unterrichtung muss jederzeit abrufbar sein.
- § 13 Abs. 4 TMG **|** Der Diensteanbieter hat die **personenbezogenen Daten** unmittelbar nach Beendigung des Dienstes bzw. **nach Ablauf des Zugriffs zu löschen** bzw. zu sperren.
- § 15 TMG **|** Nutzungsdaten dürfen seitens des Diensteanbieters nur erhoben und verwendet werden, wenn es zur Inanspruchnahme der Telemedien erforderlich ist.

  Zu den Nutzungsdaten zählen:

  - Merkmale zur Identifikation der Nutzer
  - Angaben zu Beginn und Ende sowie Umfang der Nutzung
  - Vom Nutzer in Anspruch genommene Telemedien

  Eine Verwendung der Nutzungsdaten für Werbungszwecke oder zur bedarfsgerechten Gestaltung der Telemedien ist nur pseudonymisiert erlaubt und wenn der Nutzer dem nicht widerspricht. Die Nutzungsdaten dürfen nicht mit Daten zusammengeführt werden, die den Nutzer identifizieren.
- Mit der Gesetzesänderung aus Juni 2017 entfällt die **Störerhaftung** für Diensteanbieter. Damit möchte der Gesetzgeber das Angebot von öffentlichem WLAN-Netzen vereinfachen. Somit ist es nicht mehr erforderlich, persönliche Daten von Nutzern zu erheben und zu speichern oder die Eingabe eines Passwortes zu verlangen. Auf freiwilliger Basis kann dies weiterhin angewendet werden, unterliegt aber auch hier der Zweckbindung.

2.1.7 Haftung Internetzugang

Es besteht grundsätzlich keine Mithaftung, wenn ein Hotelgast eine Urheberrechtsverletzung begeht (Störerhaftung). Dem Hotelier trifft auch keine Überwachungspflicht und er haftet auch im Weiteren nicht für Webseiten, die der Gast besucht hat. Es gibt jedoch eine Pflicht zur Herausgabe von Daten gegenüber Strafverfolgungsbehörden, aber keine Pflicht für eine Speicherung von Daten. Werden Daten daher nicht gespeichert oder sind bereits gelöscht, so ist eine Auskunftserteilung nicht möglich.

Zur Wahrung der Sicherheit des WLAN-Netzes empfiehlt es sich, das Gäste-WLAN verschlüsselt und im Wohnbereich mit individuellen Zugangsdaten anzubieten.

2.1.8 Check-Out

Am Ende des Hotelaufenthalts steht der Check-Out. Da hierbei in der Regel keine neuen personenbezogenen Daten des Gastes mehr anfallen, ergeben sich insofern grundsätzlich keine Besonderheiten. Unproblematisch ist ein Umgang mit personenbezogenen Daten, soweit diese zu Abrechnungszwecken erforderlich sind. Um den Gast hinsichtlich seiner Zufriedenheit zu befragen, kann das Front Office die Möglichkeit nutzen, eine datenschutzgerechte Einwilligungserklärung für eine Online-Befragung einzuholen.

Für die Zeit nach der Abreise hat der Hotelier insbesondere eine ordnungsgemäße Aufbewahrung von Meldescheinen und Reservierungsunterlagen in dafür geeigneten Archivräumen sicherzustellen. Gerade in den Reservierungsunterlagen sind oft sensible Daten wie Kreditkartennummern abgelegt. Ein vertraulicher Umgang muss gewährleistet werden, Aufbewahrungsfristen sind zu berücksichtigen. Alle Unterlagen sind nach Ablauf der Aufbewahrungsfristen datenschutzgerecht zu vernichten. Hierzu können Dienstleister in Anspruch genommen werden.

- Die Hotelsoftware ist der zentrale Speicherort für Gastdaten. Mit der DSGVO werden zahlreiche datenschutzrelevante Forderungen (datenschutzfreundliche Software) an die eingesetzte Software gestellt, die umzusetzen sind.
- Kreditkartendaten gelten als streng vertraulich, entsprechend ist mit ihnen umzugehen.
- Die Meldepflicht ist gesetzlich geregelt und für den Hotelier daher verpflichtend durchzuführen.
- Es gibt keine gesetzliche Erlaubnis, Personaldokumente zu kopieren. Die Front Office Mitarbeiter können sich die Dokumente zeigen lassen. Allerdings ist ein inländischer Gast nicht verpflichtet, sein Personaldokument mitzuführen.
- Es erfolgt keine Haftung für die Internetnutzung durch den Gast, jedoch bei den Mitarbeitern.

- ✓ Überprüfung der Hotelsoftware. Werden alle datenschutzrechtliche Belange umgesetzt?
- ✓ Wie sicher sind die Kreditkartendaten? Ich welchem Umfang muss ich haften, wenn etwas passiert?
- ✓ Überprüfung des Umgangs der Meldepflicht im Hotel. Gibt es einen Standard?
- ✓ Wie informiere ich den Gast formgerecht über die Speicherung und Verarbeitung seiner Daten?

2.2 Mitarbeiterdaten

Zielfragen

- Unter welchen Bedingungen darf ich Beschäftigtendaten verarbeiten?
- Wer zählt zu den Beschäftigten?
- Was ist im Bewerbungsverfahren zu beachten?
- Wie führe ich die Personalakte?
- Darf ich meine Mitarbeiter überwachen?
- Dürfen die Mitarbeiter Internet und E-Mail auch privat nutzen?

Unter dem Stichwort Beschäftigten- oder Arbeitnehmerdatenschutz werden Regelungen zusammengefasst, die sich speziell mit der Erhebung, Verarbeitung und Nutzung von Arbeitnehmerdaten bzw. Daten im Zusammenhang mit einem Beschäftigungsverhältnis befassen. In der deutschen Gesetzgebung finden sich diese Vorschriften in sehr unterschiedlichen, bereichsspezifischen Gesetzen. Die Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses ist vorrangig in § 26 BDSGneu geregelt. In der DSGVO sind keinerlei spezifische, rechtsgestaltende Regelungen zum Beschäftigtendatenschutz enthalten, sie enthält lediglich in Art. 88 eine Öffnungsklausel zu nationalen Regelungen in den Mitgliedsstaaten. Diese können des Weiteren durch Kollektivvereinbarungen (Tarifverträge und Betriebs- oder Dienstvereinbarungen) ausgestaltet werden.

Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies

- für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist, oder
- nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung erforderlich ist, oder
- für dessen Beendigung erforderlich ist.

Unberührt und weiterhin gültig bleiben alle übrigen einschlägigen und bereichsspezifischen Datenschutzvorschriften, die eine Datenerhebung, -verarbeitung oder -nutzung erlauben oder anordnen. Dies gilt auch für die Regelungen zur Datenerhebung, -verarbeitung oder -nutzung auf der Grundlage einer **freiwilligen Einwilligung**. Es gelten deshalb unverändert alle von der Rechtsprechung auf der Grundlage des verfassungsrechtlich geschützten allgemeinen Persönlichkeitsrechts entwickelten Grundsätze zum Datenschutz im Beschäftigungsverhältnis. Danach besitzt jeder Arbeitnehmer am Arbeitsplatz einen **Anspruch auf den Schutz seines Persönlichkeitsrechts**.

Beschäftigte im Sinne des BDSGneu sind

- Arbeitnehmerinnen und Arbeitnehmer, einschließlich Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher,
- Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist,
- Auszubildende,
- Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
- in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
- nach dem Jugendfreiwilligendienstgesetz Beschäftigte (Praktikanten),
- Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist,
- Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
- Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

Durchführung des Beschäftigungsverhältnisses

Zur Einstellung und nach der Einstellung darf der Hotelier vom Beschäftigten alle Daten über Umstände und Sachverhalte erheben und speichern, die erforderlich sind, um seine Pflichten im Zusammenhang mit dem Beschäftigungsverhältnis erfüllen zu können.

Zulässig sind unter diesen Gesichtspunkten **alle Daten, die im Zusammenhang mit der Personalverwaltung**, zur Durchführung der Lohn- und Gehaltsabrechnung, zur Mitarbeiterführung, Personalplanung, zur betrieblichen Fortbildung und Personalentwicklung etc. **erforderlich sind**.

Der Hotelier darf aber auch Mitarbeiterdaten erheben, speichern und nutzen, um seine Rechte im Zusammenhang mit dem Beschäftigungsverhältnis wahrnehmen zu können. Dazu gehören **Kontrollen zu Leistung und Verhalten des Beschäftigten** ebenso wie Informationen als Grundlage zur Wahrnehmung seines Weisungsrechts. Auch Maßnahmen und Kontrollen zur Verhinderung von Straftaten oder sonstigen Rechtsverstößen im Beschäftigungsverhältnis sind datenschutzrechtlich zu beurteilen.

Beendigung des Beschäftigungsverhältnisses

Der Begriff der Beendigung umfasst die vollständige Abwicklung eines Beschäftigungsverhältnisses. Der Hotelier darf alle zur Beendigung erforderlichen bzw. damit im Zusammenhang stehenden Mitarbeiterdaten erheben und speichern. Dazu gehören auch alle Daten zur Sozialauswahl im Rahmen betriebsbedingter Kündigungen und sonstige Daten, die eine Kündigung begründen, wie Abmahnungen oder Beweismittel zur Begründung einer Kündigung und im Falle eines Rechtsstreites auch alle im Zusammenhang mit der Durchführung des Rechtsstreits anfallenden Daten und Unterlagen.

Zu regeln ist auch die Frage der Aufbewahrungsdauer der **Personalakte** nach dem Ausscheiden eines Mitarbeiters. Es gibt hier keine definierte Aufbewahrungsfrist, sodass die Frist nach den individuellen Verhältnissen des jeweiligen Unternehmens festgelegt werden kann. Zweckmäßig ist es aber, die Personalakte bei Ausscheiden eines Mitarbeiters auszudünnen und nicht mehr erforderliche Unterlagen zu vernichten.

Grundsatz der Erforderlichkeit

Mitarbeiterdaten dürfen erhoben, gespeichert, verarbeitet und genutzt werden, wenn dies erforderlich ist. Der Begriff der Erforderlichkeit ist ein unbestimmter Rechtsbegriff und bedarf deshalb der näheren Betrachtung und Interpretation. Grundsätzlich dürfen nicht mehr Daten erhoben, gespeichert und verarbeitet werden, als zur Erfüllung der jeweiligen Aufgabe benötigt werden. Dieses Gebot ist nicht neu und ergibt sich auch schon aus dem **Grundsatz der Datenvermeidung und Datensparsamkeit**. Es dürfen auch keine Daten auf Vorrat erhoben werden, z.B. unter dem Gesichtspunkt, dass die Daten zu einem späteren Zeitpunkt für eine andere oder zusätzliche Nutzung vielleicht ganz nützlich wären. Welche Daten grundsätzlich und im Einzelfall konkret erforderlich sind, entscheidet der Hotelier nach eigenem Ermessen.

Zurückhaltung ist geboten, je sensibler die Daten sind und je mehr in das Persönlichkeitsrecht des Mitarbeiters eingegriffen wird (z.B. Behinderung, Gewerkschaftszugehörigkeit, Gesundheitsdaten).

Informationspflichten bei der Datenerhebung

Mit der Datenerhebung und -speicherung ist der Mitarbeiter gemäß Art. 13 DSGVO über die Identität der verantwortlichen Stelle (i.d.R. das Hotel als Arbeitgeber), die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung, die Löschfristen und bei Datenübermittlungen auch über die Kategorien von Empfängern zu unterrichten. Zusätzlich ist der Mitarbeiter über seine Rechte bzgl. der Datenverarbeitung und Einschränkungsmöglichkeiten aufzuklären und auf sein Beschwerderecht hinzuweisen. Seiner Informationspflicht sollte der Hotelier gleich bei der Einstellung des Mitarbeiters nachkommen.

Innerhalb eines Konzerns kann sich diese Anforderung nach einer Unterrichtung über die Identität des Arbeitgebers ergeben, wenn die Personalhoheit bzw. Personalzuständigkeit an die Konzernmutter oder an eine andere bestimmte Gesellschaft im Konzernverbund übertragen und dies bei der Einstellung für den Bewerber nicht erkennbar ist.

Über Kategorien von Empfängern muss der Betroffene unterrichtet werden. Hierunter fällt nun auch die Unterrichtungspflicht über Empfänger, an die im Arbeitsleben eine Datenübermittlung üblich ist, z.B. bei Übermittlungen an die Krankenkasse oder an das Bankinstitut zur Auszahlung des Gehalts oder bei Offenbarungen an den Betriebsrat. Eine Unterrichtungspflicht besteht des Weiteren, wenn zur Verarbeitung von Personaldaten im Wege der Datenverarbeitung im Auftrag Dienstleistungsunternehmen (z.B. an die externe Lohnbuchhaltung) eingeschaltet werden oder wenn bestimmte personenbezogene Daten für konzernübergreifende Verarbeitungsverfahren an die Muttergesellschaft übertragen werden (insbesondere, wenn diese ihren Sitz im Ausland hat), soweit hierzu nicht ohnehin eine Einwilligung des Betroffenen erforderlich ist.

Beschäftigtendaten in nichtautomatisierten Verfahren und Dateien (Akten)

Das Datenschutzgesetz ist auch anzuwenden, wenn im Rahmen eines Beschäftigungsverhältnisses personenbezogene Daten aus einer nicht automatisierten Datei erhoben, verarbeitet oder genutzt werden. Damit ist klargestellt, dass die **Personalakten**, unabhängig von der technisch-organisatorischen Form und dem Aufbau der

Personalakten immer den Vorschriften des Datenschutzgesetzes unterliegen. Werden im Rahmen eines **Bewerbungsverfahrens** vom Bewerber Informationen erfragt und manuell festgehalten oder bei der Einstellung ein Personalfragebogen ausgefüllt, fallen diese Unterlagen ebenfalls unter den Schutzbereich des Datenschutzgesetzes.

2.2.1 Bewerbung

Basierend auf dem Grundsatz der Datenvermeidung und Datensparsamkeit dürfen im Bewerbungsverfahren nur diejenigen Fragen gestellt und Daten erhoben werden, die im Bewerbungsverfahren und zur Entscheidung über die Bewerbung erforderlich sind. Der Abschluss des Arbeitsvertrags ist ein anderer Zweck.

Soweit Daten erfragt werden sollen, die Anhaltspunkte für eine Diskriminierung der Betroffenen ergeben können, greifen vorrangig die Vorschriften des Allgemeinen Gleichbehandlungsgesetzes (AGG). Fragen, die Indizien für eine **potenzielle Diskriminierung** liefern können (Fragen nach Staatsangehörigkeit, Gesundheit, Behinderung, Religion und Weltanschauung, Rasse oder ethnische Herkunft, Geschlecht, Alter und sexuelle Identität) sind deshalb grundsätzlich **unzulässig**.

Zusätzliche Daten, die erst für den Abschluss des Arbeitsvertrags erforderlich sind, dürfen erst zum Vertragsabschluss erhoben werden. Diese Differenzierung mag bezogen auf denjenigen Bewerber, der die Anstellung erhält, nicht von großer Bedeutung erscheinen. Sie schützt aber alle anderen Mitbewerber vor einer unnötigen Offenlegung persönlicher Informationen und Umstände, die für das Bewerbungsverfahren unwichtig sind.

Die Zulässigkeit der **Web-Recherche** wird unterschiedlich beurteilt. Einerseits wird argumentiert, dass diese Daten allgemein zugänglich zur Verfügung stehen, in aller Regel sogar von den Betroffenen selbst eingestellt worden sind und deshalb vom Arbeitgeber unter Beachtung des Erforderlichkeitsprinzips auch abgefragt werden dürfen. Gestützt wird diese Auffassung auf der Ausnahmevorschrift vom Direkterhebungsgebot, die eine Erhebung von personenbezogenen Daten aus allgemein zugänglichen Quellen erlaubt. Dies ist aber nur dann der Fall, wenn das schutzwürdige Interesse des Betroffenen am Ausschluss der Erhebung nicht offensichtlich überwiegt. Andererseits wird die Rechtsauffassung vertreten, dass die Vorschrift (die eine Erhebung von personenbezogenen Daten im Bewerbungsverfahren nur im Rahmen der Zulässigkeit erlaubt) für die Erhebung von Personaldaten für ein Beschäftigungsverhältnis nicht mehr greifen kann. Da dann diese Ausnahmeregelung vom Direkterhebungsgebot nicht mehr angewendet werden kann, verbleibt es beim Direkterhebungsgebot. Daraus folgt, dass allgemeine Web-Recherchen zur Beschaffung von Zusatzinformationen über den Bewerber unzulässig sind. Darüber hinaus soll sich ein Bewerber, wenn er sich in ein Anbahnungsverhältnis begibt, darauf verlassen können, dass diese quasi-vertragliche Beziehung auch den Rahmen der zulässigen Datenerhebung umreißt. Ein Rückgriff durch den Arbeitgeber auf andere Quellen würde sich vom gemeinsamen Willen der Beteiligten entfernen. Das Vertrauen darauf, dass dies nicht geschieht, ist schützenswert.

Nicht berücksichtigte Bewerbungen sind deshalb zurückzugeben oder datenschutzgerecht zu vernichten. Soweit Bewerbungen elektronisch gespeichert sind, ergibt sich eine Löschungsverpflichtung auch aus dem Datenschutzgesetz.

Es ist vertretbar, wenn ein Unternehmen die Bewerberunterlagen bis zu sechs Monate ab Abschluss des Bewerbungsverfahrens noch vorhält. Die Frist beginnt bei einer Bewerbung mit dem Zugang der Ablehnung.

Gemäß dem AGG kann der Bewerber innerhalb einer Frist von zwei Monaten nach Kenntnis einer Benachteiligung einen Anspruch auf Schadensersatz erheben und binnen weiterer drei Monate einklagen. Werden vom abgelehnten Bewerber Indizien vorgelegt, die eine Benachteiligung nach den Vorschriften des AGG vermuten lassen, liegt die Beweislast dafür, dass kein Verstoß vorgelegen hat, beim Arbeitgeber. Um im Falle einer Klage den Entlastungsbeweis führen zu können, empfiehlt es sich deshalb, zumindest die entscheidungserheblichen Auszüge aus der Bewerbung, die Kriterien für das Auswahlverfahren und die Entscheidungsgründe über die Bewerbung für einen angemessenen Zeitraum aufzubewahren bzw. zu speichern. Die Frist für die Geltendmachung einer Benachteiligung beginnt mit der Kenntnis der Benachteiligung. Dies muss nicht immer der Zeitpunkt der Zustellung der Ablehnung sein, sondern es kann auch ein späterer Zeitpunkt sein. Unter Berücksichtigung von Postlaufzeiten und sonstigen eventuell möglichen Liegezeiten ist sicher kein Verstoß gegen das AGG und den Datenschutz zu erkennen, wenn die Zweimonatsfrist als Mindestaufbewahrungsfrist gehandhabt und um einen angemessenen Zeitraum verlängert wird.

Anders wäre es, wenn der Bewerber erklärt hat, mit einer längeren Speicherung einverstanden zu sein, bis das Unternehmen für ihn eine geeignete Stelle gefunden hat oder das Unternehmen eine solche Absicht dem Bewerber mitteilt und dieser damit einverstanden ist.

Textbeispiel

„Ihr Einverständnis vorausgesetzt würden wir gern Ihre Bewerbungsunterlagen noch länger behalten. Sollten wir nicht auf Sie zukommen, werden wir Ihre Unterlagen spätestens nach einem Jahr datenschutzgerecht vernichten. Teilen Sie uns bitte mit, wenn Sie der längeren Aufbewahrung widersprechen.“

Eine Weiterleitung von Bewerbungen (z.B. innerhalb von konzernangehörigen Unternehmen) an eine Schwestergesellschaft oder an die Muttergesellschaft ist nur mit Einwilligung des Bewerbers zulässig. Ebenso ist eine Aufbewahrung der Bewerbung für eine später zu besetzende Stelle nur mit Einwilligung des Betroffenen zulässig. Sollte eine derartige Weiterleitung oder Aufbewahrung in Frage kommen, kann die Einholung der Einwilligung mit dem Ablehnungsschreiben verbunden werden, dass dem Bewerber angeboten, wird, innerhalb einer zu setzenden Frist hierzu seine Einwilligung einzureichen. Ansonsten wird je nach Speicherungsform seine Bewerbung nach Ablauf der nach dem AGG angemessenen Frist gelöscht, vernichtet oder zurückgegeben.

2.2.2 Personalakte

In der Privatwirtschaft gibt es keine Formvorschriften über die Führung von Personalakten. Form und Gestaltung der Personalakten obliegen deshalb der Gestaltungsfreiheit des Hoteliers.

Die Führung der Personalakten wird von folgenden Grundprinzipien bestimmt:

1. Vertraulichkeit der Personalunterlagen
2. Richtigkeit und Vollständigkeit
3. Zulässigkeit und Zweckbindung der Informationen
4. Transparenzgrundsatz

Vertraulichkeit der Personalunterlagen

Ebenso sind die **Personalakten sicher** zu **verwahren** und vor dem Zugriff unbefugter Personen zu schützen. Der **Kreis der zugriffsbefugten Personen** ist auch innerhalb der Personalabteilung auf den notwendigen Umfang zu **begrenzen**.

Gesundheitsdaten des Arbeitnehmers dürfen, soweit sie überhaupt als Inhalt der Personalakte erlaubt sind, nur besonders verschlossen geführt werden. Der Zugriff darf nur besonders befugten Personen erlaubt sein. Keinesfalls dürfen ärztliche Zeugnisse oder sonstige Unterlagen mit Informationen über die gesundheitlichen Verhältnisse des Mitarbeiters ungeschützt in der Personalakte abgelegt werden. Wenn sensible Gesundheitsdaten in die Personalakte aufgenommen werden dürfen, hat der Arbeitnehmer Anspruch darauf, dass dies unter Berücksichtigung seiner Interessen geschieht und der Hotelier diese Daten in besonderer Weise schützt und aufbewahrt.

Sofern sich Gesundheitsdaten des Mitarbeiters in der Personalakte befinden, sind diese getrennt zu führen, zum Beispiel in einem verschlossenen Umschlag oder einer gesonderten Akte.

Richtigkeit und Vollständigkeit der Personalakten

Die Personalakte hat ein möglichst objektives und richtiges Bild von der Person, deren Tätigkeit und Leistungen zu vermitteln. Die Angaben müssen begründet und sachlich richtig sein und es dürfen Unterlagen nicht willkürlich hinzugefügt oder entfernt werden. Da für Unternehmen der Privatwirtschaft keine gesetzliche Verpflichtung zur Führung einer Personalakte besteht, existieren auch keinerlei Vorschriften darüber, welche Unterlagen in einer Personalakte enthalten sein müssen. Abgesehen von den gesetzlichen **Nachweispflichten** liegt es deshalb im Ermessen des Hoteliers, welche Unterlagen er neben diesen Nachweisdokumenten in die Personalakte aufnimmt. Grundsatz ist, dass alle Beschäftigten gleich behandelt werden müssen.

Unrichtige Daten sind zu berichtigen bzw. zu entfernen. Bestreitet der Beschäftigte die Richtigkeit der Daten, besteht ein **Recht auf Gegendarstellung**. Die Gegendarstellung ist in die Personalakte aufzunehmen und mit den bestrittenen Unterlagen zu verbinden.

Das **Gebot der Vollständigkeit** verlangt auch, dass die Sachverhalte vollständig, zutreffend und nicht lückenhaft aktenkundig gemacht werden. Sachverhalte müssen deshalb chronologisch und umfassend dargestellt sein. Unzulässig wäre es einzelne Unterlagen nicht aufzunehmen, den Sachverhalt damit lückenhaft darzustellen oder einzelne Unterlagen zu einem späteren Zeitpunkt ohne Wissen des Betroffenen wieder zu entfernen.

Inhalt und Aufbewahrungsfristen

Umfang und Inhalt der Personalakte ergeben sich zunächst aus den arbeits-, sozial-, steuer- und handelsrechtlichen Anforderungen unter dem Gesichtspunkt der Nachweispflichten des Hoteliers. Darüber hinaus wird der Inhalt durch den Anspruch des Arbeitnehmers auf Wahrung seines Persönlichkeitsrechts begrenzt. In die Personalakte bzw. in die Sammlung der Personalaktendaten dürfen deshalb nur solche Daten und Unterlagen aufgenommen werden, die in zulässiger Weise, d.h. unter Beachtung der Vorschriften zu Datenschutz und Arbeitsrecht, gewonnen worden sind.

Anhaltspunkte hierzu liefern auch die zum Fragerecht des Arbeitgebers entwickelten Grundsätze und die sich aus dem AGG ergebenden Anforderungen. Ebenso sind **Mitwirkungspflichten und Beteiligungsrechte der**

Mitarbeitervertretungen zu beachten, wenn für die Erhebung von Bewerber- oder Mitarbeiterdaten Bewerber- bzw. Personalfragebögen eingesetzt werden. Unter dem Gesichtspunkt der Zulässigkeit ist auch die Frage der **Aufbewahrung der Personalakten** und der **Entfernung von Vorgängen** aus der Personalakte zu beurteilen.

Für die steuer- oder sozialversicherungsrechtlich relevanten Unterlagen gelten die hierzu bestimmten **Aufbewahrungsfristen**. Für die sonstigen Unterlagen sind keine Aufbewahrungsfristen geregelt. Die **Dauer der Aufbewahrung** regelt sich deshalb bei elektronisch gespeicherten Daten nach den Vorschriften des Datenschutzgesetzes.

Bezüglich der manuell geführten Unterlagen greift das Recht der Betroffenen auf informationelle Selbstbestimmung. Dies hat zur Konsequenz, dass Unterlagen zu entfernen sind, wenn die Zweckbestimmung, welche die Aufnahme in die Personalakte rechtfertigte, weggefallen ist. Dieser **Entfernungsanspruch** gilt insbesondere für Vorgänge mit für den Betroffenen belastenden Inhalten, z.B. für Abmahnungen. Hier richtet sich die Aufbewahrungsfrist nach der Schwere des Vorgangs und der künftigen Bedeutung der Abmahnung. Sie ist nach der Rechtsprechung des Bundesarbeitsgerichts zu entfernen, wenn sie für den Arbeitnehmer belastend, aber für die Zukunft belanglos ist.

Für die **Zeit nach dem Ausscheiden eines Beschäftigten** existiert ebenfalls keine Aufbewahrungsvorschrift. In Verbindung mit dem Ausscheiden können nicht mehr erforderliche Unterlagen entfernt werden. Für Unterlagen, die steuer- oder sozialversicherungsrechtlich von Bedeutung sind, müssen natürlich die jeweiligen Aufbewahrungsfristen beachtet werden. Vorgänge, aus denen die Betroffenen auch nach Beendigung des Beschäftigungsverhältnisses noch Rechte herleiten könnten, sollten ebenfalls bis zum Ablauf von etwaigen Verjährungsfristen (z.B. 3 Jahre für Arbeitszeugnis gemäß § 195 BGB) aufbewahrt werden. Da Unterlagen, insbesondere über Inhalt und Verlauf des Beschäftigungsverhältnisses, auch lange nach Beendigung des Beschäftigungsverhältnisses noch nachgefragt werden können, sind diese im Interesse der Betroffenen noch für einen angemessenen Zeitraum aufzubewahren. Ein Zeitraum von **10 Jahren** gilt i.d.R. als ausreichend, kann aber z.B. auch abhängig vom Alter der Betroffenen länger gestaltet werden.

Transparenzgrundsatz

Beschäftigte besitzen ein **Recht auf Einsichtnahme** in die vollständige Personalakte. Dieses Einsichtsrecht ist ein Kernbestandteil der Schutzrechte im Beschäftigungsverhältnis. Damit der Beschäftigte sein Einsichtsrecht auch umfassend geltend machen und der Arbeitgeber dieses Recht auch gewähren kann, muss für beide Seiten Umfang und Inhalt der Personalaktendaten definiert sein. Dies kann insbesondere dann unübersichtlich sein, wenn die Personalaktendaten auf mehrere Teilakten und Datenbestände an verschiedenen Orten (z.B. Personalabteilung, Niederlassung und Firmenzentrale oder Vorgesetzte) verteilt geführt werden.

Bei komplexen Personaldatenstrukturen mit Haupt-, Sonder- und Nebenakten ist in die Hauptpersonalakte ein Hinweis auf die Sonder- und Nebenakten aufzunehmen, um dem Beschäftigten die Möglichkeit zur Realisierung seines Einsichtsrechts zu geben. Als Selbstverständlichkeit ergibt sich auch das Verbot der Führung von Geheimakten, die dem Arbeitnehmer nicht bekannt sind und ihm nicht zugänglich gemacht werden.

2.2.3 Elektronisches Personalaktenarchiv

Neben den allgemeinen Anforderungen an ein elektronisches Archiv bestehen aus der Sicht des Datenschutzes an ein elektronisches Personalaktenarchiv folgende besonderen Anforderungen:

Zugriffsschutz

Da die Personalakten einem besonderen Vertraulichkeitsschutz unterliegen, sind die Zugriffsberechtigungen differenziert zu regeln. Folgende Zugriffsberechtigungen müssen regelbar sein:

- uneingeschränkter Zugriff auf alle Unterlagen, z.B. für die Betroffenen
- eingeschränkter Zugriff auf ausgewählte Unterlagen, z.B. für die Fachvorgesetzten
- u.U. Differenzierung der Zugriffsberechtigungen auf Teile der Personalakte, z.B. für Personalsachbearbeiter mit bestimmten Teilzuständigkeiten (Lohnabrechnung, disziplinar- oder arbeitsrechtliche Angelegenheiten etc., soweit im HR-Bereich eine derartige Arbeitsteilung besteht)
- Unterlagen über Krankheiten oder sonstige besonders sensible Unterlagen, die einem besonderen Schutz unterliegen, müssen zusätzlich geschützt werden können

Erforderlich ist unter diesen Gesichtspunkten die Möglichkeit einer differenzierten Rechtegestaltung für bestimmte Personengruppen auf bestimmte Dokumentengruppen und die Möglichkeit, darüber hinaus zusätzlich einzelne Dokumente besonders zu schützen.

Verknüpfung von Dokumenten

Das Personalaktenrecht ermöglicht dem Mitarbeiter zu einem bestimmten Vorgang eine eigene Stellungnahme hinzuzufügen, z.B. zu einer disziplinarischen Maßnahme. Bei in Papierform geführten Personalakten muss diese Stellungnahme in einer solchen Form mit dem auslösenden Dokument verbunden werden, dass beide Dokumente nur gleichzeitig zur Kenntnis genommen werden können. Dies erfordert, dass bei einer elektronischen Personalakte beispielsweise eine Abmahnung mit einer nachträglichen Stellungnahme des Mitarbeiters so verknüpft werden muss, dass die Abmahnung nicht für sich alleine aufgerufen werden kann.

Löschung oder Sperrung von Dokumenten

Da die Dokumente einer Personalakte unterschiedlich lang aufbewahrt werden müssen, müssen die Dokumente differenziert löschbar sein. Die Löschungsbefugnis muss aber an bestimmte Voraussetzungen bzw. Berechtigungen gebunden sein, d.h. es muss regelbar sein, wer nur lesen und wer auch Dokumente löschen können soll. Die Löschungsbefugnis sollte möglichst eingeschränkt werden.

Im Personalbereich ist nicht auszuschließen, dass Unterlagen anfallen, deren Richtigkeit vom Betroffenen bestritten wird und zumindest für einen bestimmten Zeitraum die Richtigkeit oder Unrichtigkeit nicht zuverlässig festgestellt werden kann. In einem solchen Fall verlangt das Datenschutzrecht, dass diese Daten gesperrt werden können, d.h. die Daten sind zwar gespeichert, dürfen aber nicht genutzt werden. Derartige Dokumente müssen mit einem Sperrvermerk versehen bzw. entsprechend gekennzeichnet werden können.

Protokollierung von Zugriffen

Aufgrund der besonderen Vertraulichkeit von Personalunterlagen sollten die Zugriffe auf die Unterlagen vom System protokolliert werden. Das Datenschutzgesetz verlangt hierzu, dass nachträglich festgestellt werden kann,

von wem welche Daten in das System eingeben, verändert oder entfernt worden sind. Die Dokumentation des Systems sollte deshalb ein Konzept enthalten, das die Protokollierungen nachprüfbar beschreibt.

Weitergabekontrolle

Ebenfalls aufgrund der besonderen Vertraulichkeit der Personaldaten sollte die Möglichkeit, von den gespeicherten Dokumenten Kopien herzustellen, eingeschränkt werden können. Ideal wäre eine solche Einschränkung sowohl bezüglich bestimmter Dokumente als auch hinsichtlich bestimmter Benutzer des Systems. Die Herstellung von Kopien sollte protokolliert werden können.

Bei der Übertragung der Daten an den Datenserver sollten die Daten verschlüsselt werden. Ebenso sollten die Daten verschlüsselt gespeichert werden.

Zugriffsmöglichkeiten durch Administratoren

Zu beachten ist auch, welche Rechte die Administratoren des IT-Systems haben, in dem die elektronischen Personalakten verwaltet werden. Es ist insbesondere nicht zulässig, dass die Administratoren die einzelnen Personalakten kraft ihrer umfassenden Berechtigung einsehen oder gar verändern können. Schutz bieten hier z.B. eine Verschlüsselung der Daten oder das Vieraugenprinzip bei der Gestaltung der Rechte der Administratoren.

Information der Betroffenen

Die Mitarbeiter müssen über die Einrichtung einer elektronischen Personalakte unterrichtet werden. Ferner muss für die Mitarbeiter eine Zugangsmöglichkeit zur elektronischen Personalakte eingerichtet werden, um dem Einsichtsrecht der Mitarbeiter nachkommen zu können.

Mitbestimmungspflicht

Je nach Ausgestaltung der elektronischen Personalakte und der Nutzungsmöglichkeiten der Daten kann die Einrichtung einer elektronischen Personalakte mitbestimmungspflichtig sein. Deshalb muss der Betriebsrat vor Implementierung rechtzeitig beteiligt werden. Ist kein Betriebsrat vorhanden, so ist der Mitarbeiter darüber zu informieren, ggf. sind Einzelvereinbarungen abzuschließen.

Datenschutz-Folgenabschätzung

Je nach Ausgestaltung des Verfahrens kann das Persönlichkeitsrecht der Betroffenen in unterschiedlicher Weise berührt sein. Daher ist der Datenschutzbeauftragte rechtzeitig zu beteiligen, um eventuell eine Datenschutz-Folgenabschätzung durchzuführen.

2.2.4 Arbeitsvertrag inkl. Verpflichtungen und Vereinbarungen

Mit Abschluss des Arbeitsvertrages ist der Mitarbeiter auf das **Datengeheimnis** zu verpflichten. Dies geschieht auf Grundlage von **Art. 32 Abs. 4 DSGVO.**

> *„Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.“*

Die Verpflichtung unterliegt der Freiwilligkeit und darf aus diesem Grund nicht im Arbeitsvertrag, sondern als Anlage zum Arbeitsvertrag erfolgen. Aus der Verpflichtung zum Datengeheimnis ergibt sich die **Pflicht zu Schulungen**.

Neben der Verpflichtung zum Datengeheimnis empfiehlt es sich mit dem Mitarbeiter weitere Vereinbarungen zur Nutzung der IT- und Kommunikationsdienste zu treffen.

2.2.5 Lohnabrechnung

Beauftragt der Hotelier ein externes Lohnsteuerbüro, so unterliegt die Beauftragung der Datenverarbeitung im Auftrag. Entsprechend ist das Lohnsteuerbüro zu prüfen und es ist eine Datenschutzvereinbarung abzuschließen. In der Datenschutzvereinbarung sind technische und organisatorische Maßnahmen festzulegen, die den Schutz der Mitarbeiterdaten betreffen. Insbesondere sind Maßnahmen für eine sichere Datenübermittlung, z.B. per E-Mail (Verschlüsselung) zu treffen.

2.2.6 Zustimmungspflichtige Maßnahmen

Durch den Arbeitsvertrag ergibt sich das Recht des Arbeitgebers auf Kontrolle der Einhaltung der arbeitsrechtlichen Pflichten des Arbeitnehmers. Das Recht der Kontrolle ist nicht uneingeschränkt. Gemäß §§ 90, 91 BetrVG unterliegen Verfahren, die zu einer Leistungs- und Verhaltenskontrolle von Mitarbeitern geeignet sind sowie deren Persönlichkeitsrechte einschränken können, dem Mitbestimmungsrecht, also der Zustimmung durch den Betriebsrat. Die Regelungen werden in Betriebsvereinbarungen festgelegt, der Betriebsrat gibt seine Zustimmung im Namen aller Mitarbeiter.

Ist in einem Hotel kein Betriebsrat vorhanden, so ist vor der Implementierung von Kontrollmaßnahmen (Videoüberwachung, Zutrittskontrollsystem) die Zustimmung der betroffenen Arbeitnehmer einzuholen. Die Zustimmung sollte schriftlich und befristet für einen bestimmten Zeitraum eingeholt werden. Es sind Einverständniserklärungen und Nutzungsvereinbarungen mit den Mitarbeitern abzuschließen.

2.2.7 E-Mail und Internetnutzung am Arbeitsplatz

Wenn keine Nutzungsregelung in einer Betriebsvereinbarung, einem Arbeitsvertrag oder durch Anweisung des Arbeitgebers vorhanden ist, so ist von einer erlaubten, auf das für den Arbeitgeber zumutbaren Ausmaß reduzierten Nutzung auszugehen. Darunter ist zu verstehen, dass die Arbeit nicht beeinträchtigt werden darf, die technischen Ressourcen dürfen nicht belastet werden, es darf kein zusätzliches Sicherheitsrisiko geschaffen werden und es dürfen keine widerrechtlichen Handlungen (z.B. Kinderporno) unterstützt werden.

Ist eine Privatnutzung untersagt, so kann der Arbeitgeber stichprobenartige und begründete Kontrollen durchführen. Wichtig dabei ist, dass die Kontrollen so gestaltet werden, dass weder in die Persönlichkeitsrechte eingegriffen, noch die Menschenwürde berührt wird.

Wenn die Privatnutzung erlaubt ist, kann die Menschenwürde eher berührt werden und in die Menschenwürde eingegriffen werden, wenn z.B. Kontrollen zur Überprüfung der Einhaltung der Nutzungsbestimmungen durchgeführt werden und im Zuge dessen auch Daten aus der Privatsphäre des Mitarbeiters ausgewertet werden.

Es ergibt sich daher die Empfehlung, zu einer klaren Regelung, damit sowohl Arbeitnehmer als auch Arbeitgeber über ihre Rechten und Pflichten informiert sind. Dafür wird empfohlen, dass eine klare Trennung von dienstlicher und privater E-Mail-Kommunikation geregelt wird. Für die Internetnutzung empfiehlt es sich, eine private Nutzung unter den Voraussetzungen zu dulden, solange die Arbeitsleistung nicht beeinträchtigt wird. Hier kann von ca. 15 min. am Tag ausgegangen werden, wobei die Zeit möglichst in den Pausen zu nutzen ist.

- Alle Informationen, die einem einzelnen Arbeitnehmer zugeordnet werden können, sind personenbezogene Daten.
- Bezüglich des Inhalts von Personalakten sind alle Mitarbeiter nach einheitlichen Grundsätzen zu behandeln. Die in der Personalakte gesammelten Daten müssen objektiv, richtig und vollständig sein.
- Inhalte, die den Betroffenen belasten, müssen aus der Personalakte entfernt werden, sobald der Grund für die Aufnahme entfallen ist und diese für die Zukunft nicht mehr erforderlich sind (z.B. Abmahnungen).
- Es ist unzulässig, neben den als offizielle Personalakte definierten Unterlagen weitere Personalakten zu führen, die dem betroffenen Mitarbeiter nicht zugänglich sind.
- Bei komplexen Personalaktenstrukturen, die für den Betroffenen nicht erkennbar sind (z.B. bei mehreren Teil- oder Nebenakten, Verteilung auf verschiedene Standorte oder Vorgesetzte), sollte ein Personalaktenverzeichnis angelegt und dem Beschäftigten bei der Einsichtnahme zugänglich gemacht werden. Damit können sich die Beschäftigten bei einer Einsichtnahme einen Überblick über die gesamte Personalakte bilden.
- Im Bewerbungsverfahren dürfen nur Fragen gestellt werden, die nach objektiven Maßstäben zur konkreten Entscheidung über die Bewerbung erforderlich sind. Fragen, die erst zum Vertragsabschluss relevant werden, sind unzulässig (z.B. Fragen zur Religionszugehörigkeit).
- Kommt es nicht zur Einstellung, können die erhobenen Bewerbungsdaten bis zu sechs Monate nach Ablehnung der Bewerbung vorgehalten werden.
- Bei Anwendungen, die eine Leistungs- und Verhaltenskontrolle des Mitarbeiters ermöglichen, sind Informationspflichten und Mitbestimmungsrechte zu beachten.
- Die Nutzung von Kommunikationsmedien durch Mitarbeiter im Hotel ist zu regeln, anderenfalls ist alles erlaubt. Das kann zum Nachteil des Hoteliers in seinen Kontrollrechten führen.

- ✓ Ist der Beschäftigtendatenschutz ein fester Bestandteil unserer Datenschutzorganisation?
- ✓ Haben wir Regelungen im Umgang mit Personaldaten, insbesondere der Datenspeicherung und -nutzung sowie im Umgang mit der Personalakte?
- ✓ Haben wir mit unserem externen Lohnverrechner eine Datenschutzvereinbarung abgeschlossen? Die Tätigkeiten unterliegen nicht der Verschwiegenheitspflicht eines Steuerberatungsbüros.
- ✓ Schränken wir unsere Mitarbeiter bei der Ausübung ihrer Tätigkeit in ihren Persönlichkeitsrechten ein?
- ✓ Regelungen zur privaten Nutzung von E-Mail und Internet. Welche Regeln müssen unsere Mitarbeiter beachten?

3 Auskunftspflichten

Zielfragen

- Unter welchen Bedingungen darf ich Auskünfte über Personen weitergeben?
- Was darf eine Strafverfolgungsbehörde?

In der täglichen Praxis kann es zu Anfragen von Betroffenen (i.d.R. Gäste, ehemalige Gäste oder Interessenten), aber auch öffentlichen Einrichtungen und Unternehmen der Privatwirtschaft oder Privatpersonen über gespeicherte, personenbezogene Daten kommen. Beim Auskunftsersuchen müssen die datenschutzrechtlichen Belange aller Personen (Mitbestimmungs- und Persönlichkeitsrechte) berücksichtigt werden.

3.1 Gast

Wird eine Auskunftsanfrage an eine Abteilung im Hotel (insbesondere Direktion, Empfang, Reservierung oder Sales & Marketing) gestellt, so ist diese innerhalb von einem Monat bzw. innerhalb von zwei Monaten bei komplexen Angaben zu erteilen. Dabei ist auf dem Umfang entsprechend Art. 15 DSGVO (siehe hierzu auch Pkt. 1.6.1 - Recht auf Auskunft) Bezug zu nehmen. Die Auskunft ist schriftlich (in Briefform oder in Ausnahmefällen per Mail, nicht per Fax) und unentgeltlich zu erteilen. Sie ist direkt an den Betroffenen zu richten.

Bei Zweifel am Auskunftsbegehren oder bei einer telefonischen Auskunftsanfrage kann ein Identitätsnachweis (Kopie eines Personaldokumentes) erbeten werden. Der Betroffene hat seine Identität in geeigneter Form nachzuweisen.

Für die direkte Beantwortung von Kurzauskünften am Telefon muss der Mitarbeiter in Ausnahmefällen mindestens zwei eindeutige Identifikationsmerkmale beim Betroffenen abfragen, um sicherzustellen, dass mit der richtigen Person gesprochen wird. Im Zweifelsfall ist die Auskunft am Telefon zu verweigern und schriftlich zuzustellen.

3.2 Behörden

Soweit es sich nicht um eine vom Gesetzgeber vorgegebene Datenübermittlung handelt (**gesetzliche Grundlage** zur Datenübermittlung oder Datenoffenbarung), hat das Auskunftsersuchen schriftlich durch die Behörde zu erfolgen. In der Anfrage müssen die anfragenden Behörden (z.B. Polizei, Meldestelle, ...) den Grund der Anfrage, den Datenumfang und die Rechtsgrundlage für die Auskunft benennen. Erfolgt das Auskunftsersuchen telefonisch, so sollte um eine schriftliche Anfrage gebeten werden.

Sollten eine Behörde um Auskunft bitten, lassen Sie sich die Auskunftsanfrage immer in Schriftform mit Verweis auf die gesetzlichen Grundlagen geben. Auf dieser Grundlage können Sie prüfen, ob eine Datenoffenbarung oder Datenübermittlung gesetzlich abgesichert ist. Das Verfahren gilt auch für Anfragen der Polizei. Kann hier im Rahmen einer Strafverfolgung keine Rechtsgrundlage benannt werden, ist eine richterliche Anordnung, in Ausnahmefällen eine Anordnung der Staatsanwaltschaft, einzufordern.

Für die Weitergabe von Informationen über den Betroffenen ohne Rechtsgrundlage bedarf es dem **Einverständnis des Betroffenen** oder der **gerichtlichen Anordnung** und ist anlassbezogen direkt beim Betroffenen schriftlich einzuholen.

§ 24 BDSGneu regelt die Verarbeitung zu anderen Zwecken durch Unternehmen. Auf dieser Grundlage ist zu prüfen, ob eine Auskunft auch ohne Nennung der Rechtsgrundlage, gerichtlichen Anordnung oder Einwilligung erfolgen kann, wenn sie zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist.

Der Meldebehörde und den Organen des öffentlichen Sicherheitsdienstes ist auf Verlangen jederzeit Zugriff auf die Meldescheine zu geben.

3.3 Unternehmen und nichtöffentliche Einrichtungen

Für Unternehmen aus dem nichtöffentlichen Bereich (wie Verbände, Versicherungen, Anwälte, ...) gibt es grundsätzlich keine Rechtsgrundlage zur Weitergabe von personenbezogenen Daten. Für die Weitergabe von Informationen über den Betroffenen bedarf es dem Einverständnis des Betroffenen. Diese ist anlassbezogen *(Einverständniserklärung oder Schweigepflichtentbindungserklärung)* direkt beim Betroffenen schriftlich einzuholen.

§ 24 BDSGneu regelt auch hier einen Ausnahmetatbestand. Auf dieser Grundlage ist zu prüfen, ob eine Auskunft auch ohne Einwilligung erfolgen kann, wenn sie zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist, sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Datenweitergabe überwiegen.

3.4 Sonstige Dritte

Für alle anderen Personen (Dritte), die Auskünfte über Informationen eines Betroffenen (insbesondere Gast oder Mitarbeiter) erhalten wollen, gibt es grundsätzlich keine Rechtsgrundlage zur Weitergabe von personenbezogenen Daten (Datenoffenbarung). Die Privatsphäre ist zu wahren!

Beispiele hierfür können sein:

- Ein Gast erkundigt sich über die Kontaktdaten oder Zimmernummer eines anderen Gastes.
- Familienangehörige oder andere Dritte möchten Informationen zum Aufenthalt über einen Gast erhalten.
- Die Buchhaltung eines Unternehmens oder ein anderer Dritter erfragt eine Rechnungskopie.

Erhält die Rezeption eine Anfrage zum Aufenthalt eines Gastes, so ist diese Anfrage immer mit der notwendigen Sensibilität zu behandeln. Direkte Aussagen gegenüber dem Anfragenden dürfen nicht gemacht werden, auch nicht, wenn darum gebeten wird, sich mit dem Gast telefonisch verbinden zu lassen! Es ist mit dem Gast telefonisch Rücksprache zu führen, bevor ein Gespräch weitervermittelt wird. Ist der Gast nicht erreichbar oder möchte dieser nicht verbunden werden, ist unter Berufung auf das Datenschutzgesetz die Auskunft zu verwehren, unabhängig ob der Gast im Hause wohnt oder nicht.

- Bei der Auskunftspflicht zu Gastdaten ist zwischen den in der Hotelsoftware gespeicherten Daten, wie Adress- und Kontaktdaten, Gästehistorie oder Rechnungen zu unterscheiden. Meldedaten sind der Meldebehörde und den Organen des öffentlichen Sicherheitsdienstes über den Meldeschein jederzeit zugänglich zu machen. Die Herausgabe von Gästelisten, in der Hotelsoftware gespeicherte Daten bis hin zur Videoüberwachung im Rahmen der Aufklärung von Straftaten bedürfen i.d.R. einer richterlichen Anordnung.
- Auskunftsanfragen aus dem nichtöffentlichen Bereich (Unternehmen, Vereine, Verbände, ...) können nicht auf gesetzlicher Grundlage erfolgen. Dementsprechend ist immer deren berechtigtes Interesse mit dem Schutzbedürfnis des Betroffenen abzuwägen. Rechtskonforme Voraussetzungen sind zu schaffen.
- Auskunftsanfragen sind immer mit der entsprechenden Diskretion zu behandeln, insbesondere bei telefonischen Auskunftsanfragen.

- ✓ Überprüfung des Umgangs der Auskunftspflicht im Hotel. Werden alle rechtlichen Belange erfasst? Gibt es dafür einen Standard?
- ✓ Wer beantwortet im Hotel die Anfragen betreffend Datenauskunft? Sind Vorlagen dafür vorhanden?
- ✓ Wie gehen wir bei Auskunftsanfragen um?

4 Verzeichnis von Verarbeitungstätigkeiten

Zielfragen

- Ist das Verzeichnis von Verarbeitungstätigkeiten neu?
- Muss ich das Verzeichnis von Verarbeitungstätigkeiten führen?
- Was beinhaltet das Verzeichnis von Verarbeitungstätigkeiten?
- Gehört die Datenschutz-Folgenabschätzung zum Verzeichnis von Verarbeitungstätigkeiten?

Aus dem Verfahrensverzeichnis bzw. der Verarbeitungsübersicht gemäß der §§ 4e und 4g BDSG wird künftig das Verzeichnis von Verarbeitungstätigkeiten (VVT) gemäß Art. 30 DSGVO. Nach Erwägungsgrund 82 der DSGVO soll der Verantwortliche, also der Hotelier *„zum Nachweis der Einhaltung dieser Verordnung“* das Verzeichnis von Verarbeitungstätigkeiten führen. Weiterhin kann die zuständige Aufsichtsbehörde die Vorlage verlangen, um die betreffenden Stellen hoheitlich zu kontrollieren.

In der Regel müssen alle Verantwortlichen (Unternehmen/Behörden etc.) ein VVT führen. Gem. Art. 30 Abs. 5 DSGVO ist diese Pflicht zwar beschränkt auf Unternehmen

- mit einer Größe ab 250 Mitarbeitern oder
- mit einem besonderen Risiko bei der Verarbeitung oder
- mit Verarbeitung von sensiblen Daten (Artt. 9 und 10 DSGVO) oder
- einer nicht nur gelegentlichen Verarbeitung.

Allerdings geht diese Ausnahmeregelung ins Leere. Spätestens bei Zugrundelegung einer regelmäßigen Verarbeitung, der Verarbeitung von Beschäftigtendaten, Videoüberwachung bzw. Kreditkartendaten (Verfahren, die einer Datenschutzfolgeabschätzung unterliegen) ist der Hotelier unabhängig von seiner Mitarbeiterstärke betroffen.

Während das alte Verfahrensverzeichnis allerdings in weiten Teilen noch auf Antrag jedermann zugänglich zu machen war, besteht diese Pflicht nur noch gegenüber den Aufsichtsbehörden. Es wird also nicht mehr zwischen internen und öffentlichen Verzeichnissen unterschieden.

Im Gegensatz zum Verfahrensverzeichnis nach BDSG ist das VVT nicht an den Datenschutzbeauftragten zu übergeben, sondern unmittelbar vom Verantwortlichen zu führen. Es mag allerdings naheliegen, das Verzeichnis zentral führen zu wollen. Die Angaben zum Verzeichnis sind durch das Hotel bzw. – im Wege der Delegation – durch die Abteilungen beizubringen.

Im Sinne einer *„best practice“* erscheint es sinnvoll, dass das Verzeichnis als Dreh- und Angelpunkt des gesamten Datenschutzmanagements vom Datenschutzbeauftragten geführt wird. Mit Blick auf die weitergehenden Dokumentationspflichten der DSGVO avanciert das VVT zum zentralen Bestandteil der Dokumentation.

Das VVT kann auch als Grundlage für Risikobewertungen durch den Datenschutzbeauftragten für dessen risikoorientierten Überwachungsauftrag genutzt werden (Art. 39 Abs. 2 DSGVO). Ohne eine solche strukturierte Dokumentation sind die Beratungs- und Kontrollpflichten des Datenschutzbeauftragten kaum umsetzbar.

4.1 Inhalte

Das VVT ist – wie früher das Verfahrensverzeichnis nach dem BDSG – nicht als Auflistung einzelner Verarbeitungen, sondern als **prozessorientierte Übersicht der Verarbeitungen** zu verstehen. Entscheidend ist, dass über das VVT der einzelne Verarbeitungsprozess zu identifizieren ist. Die Inhalte des VVT umfassen:

- den Namen und die Kontaktdaten
- des Verantwortlichen
    - ggf. des gemeinsam mit ihm Verantwortlichen
    - ggf. des Vertreters in der EU
    - ggf. des Datenschutzbeauftragten beim Verantwortlichen
- die Zwecke der Verarbeitung
- die Kategorien betroffener Personen
- die Kategorien personenbezogener Daten
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation
    - einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation
    - bei den in Art. 49 Abs. 1 UAbs. 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien
- die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DSGVO

Denkbar sind interne Erweiterungen des VVT durch Risikoabschätzungen bzw. eine zusätzliche Strukturierung, die festhält, welche Verarbeitungen ggf. eine Datenschutz-Folgenabschätzung erfordern und welche nicht. Daneben können die durchgeführten Prüfungen aufgenommen werden.

4.2 Muster

Hotels die bereits jetzt ein gutes Datenschutzmanagement haben und Verfahrensverzeichnisse nach dem BDSG führen, wird die Umstellung leichtfallen. Es sollte geprüft werden, inwieweit die bisher geführten Verfahrensverzeichnisse die inhaltlichen Anforderungen des Art. 30 DSGVO erfüllen und ggf. entsprechend ergänzt werden.

Im Falle von fehlender Datenschutzdokumentation muss zunächst ermittelt werden, in welchen Fällen personenbezogene Daten von z.B. Gast- und Interessentendaten, Lieferanten oder Beschäftigten erhoben und verarbeitet werden. Hierzu bietet es sich als ersten Anhaltspunkt an, alle innerhalb der Systemlandschaft des Hotels eingesetzten Anwendungen und Tools aufzulisten, in denen personenbezogene Daten gespeichert werden. Die Auflistung hilft gleichsam bei der Ermittlung der Datenflüsse im Unternehmen und kann auch als Grundlage für das VVT dienen. Dieses wird in der Praxis zwecks Übersichtlichkeit meist aus mehreren Verzeichnissen für verschiedene Verarbeitungsvorgänge (z.B. Hotelmanagementsystem (PMS), Online-Reservierungssystem, Zeiterfassungssystem, CRM System, Personalverwaltungssystem, Videoüberwachung, ...) bestehen.

Jedes Verfahren muss separat aufgeführt werden. Hierzu können im Muster zum Verzeichnis von Verarbeitungstätigkeiten die Anlagen in fortlaufender Nummerierung genutzt werden.

Im Anhang finden Sie ein Muster zum Verzeichnis von Verarbeitungstätigkeiten mit entsprechenden Erläuterungen.

4.3 Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung wird in Art. 35 DSGVO geregelt und ist nichts anderes, als die bisher im deutschen Datenschutzrecht schon bekannte Vorabkontrolle (§ 4d Abs. 5 BDSG). Eine Datenschutz-Folgenabschätzung ist immer dann durchzuführen, wenn besonders sensible Daten verarbeitet werden oder die Datenverarbeitung dazu bestimmt ist, die Persönlichkeit des Betroffenen, einschließlich seiner Fähigkeiten, Leistungen oder seines Verhaltens zu bewerten.

Nach Art. 35 Abs. 1 DSGVO ist eine Datenschutz-Folgenabschätzung grundsätzlich immer dann durchzuführen, wenn:

> *„(...) eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge (hat)“.*

Darüber hinaus werden in Art. 35 Abs. 3 DSGVO Regelbeispiele genannt, bei denen eine Durchführungspflicht besteht:

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlicher Weise erheblich beeinträchtigen
- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10
- systematische weiträumige Überwachung öffentlich zugänglicher Bereiche

Dies lässt im Vergleich zum BDSG einen größeren Anwendungsbereich für die Datenschutz-Folgenabschätzung erwarten, als dies noch für die Vorabkontrolle der Fall war. Durch den relativ offenen Tatbestand des Art. 35 Abs. 1 DSGVO wird aber auch Klärungsbedarf geschaffen, wann dieser denn nun genau erfüllt ist. Hier kommen auf die Aufsichtsbehörden Pflichten zu, Verfahren zu definieren, bei denen eine Datenschutz-Folgenabschätzung zwingend durchzuführen ist. Diese müssen nämlich gemäß Art. 35 Abs. 4 DSGVO im Rahmen ihres jeweiligen Zuständigkeitsbereichs eine Liste der Verarbeitungsvorgänge erstellen und veröffentlichen, für die eine Datenschutz-Folgenabschätzung nach Abs. 1 durchzuführen ist.

Der Datenschutzbeauftragte prüft die dem Verfahren innewohnenden besonderen Risiken für die Rechte und Freiheiten des Betroffenen und gibt am Ende dieser Prüfung eine Stellungnahme zur Rechtmäßigkeit der Datenverarbeitung ab. Genau wie die Vorabkontrolle dient die Datenschutz-Folgenabschätzung also der Bewertung von Risiken und deren mögliche Folgen für die persönlichen Rechte und Freiheiten der Betroffenen.

Die DSGVO bestimmt in Art. 35 Abs. 7 Mindestanforderungen bezüglich des Inhalts einer Datenschutz-Folgenabschätzung. Diese muss demnach enthalten:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem für die Verarbeitung Verantwortlichen verfolgten berechtigten Interessen.
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck.
- eine Bewertung der Risiken der Rechte und Freiheiten der betroffenen Personen.
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen werden soll.

- Das Verzeichnis für Verarbeitungstätigkeiten ersetzt das öffentliche und interne Verfahrensverzeichnis.
- Das VVT verfolgt einen prozessorientierten Ansatz. Es beschreibt das Verfahren der Datenverarbeitung, bei welchem auch mehrere Software-Anwendungen beteiligt sein können.
- Das VVT ist zentraler Bestandteil der Rechenschaftspflicht durch Dokumentation.
- Auf Grund der Ausnahmeregelungen ist letzendlich doch jedes Hotel dazu verpflichtet, das VVT vorzuhalten.
- Datenschutz-Folgenabschätzung und das VVT sind getrennt zu betrachten, d.h. es sind zwei unterschiedliche Dokumente, wobei auf Grund der Risikobewertung ein Bezug im VVT hergestellt werden kann.

- ✓ Haben wir bereits ein Verfahrensverzeichnis?
- ✓ Wenn JA; was kann daraus für die Erstellung des VVT herangezogen werden?
- ✓ Wenn NEIN, wie sind unsere Prozesse und wie sieht das VVT aus?
- ✓ Wer führt das VVT?
- ✓ Führt jede Abteilung eigenverantwortlich das VVT oder delegieren wir die Tätigkeiten zentral an den Datenschutzbeauftragten? Wie bzw. wer unterstützt den Datenschutzbeauftragten bei der Erstellung?

5 Sales & Marketing

Zielfragen

- Was muss ich auf meiner Webseite berücksichtigen?
- Welche Urheberrechte habe ich beim Internetauftritt zu berücksichtigen?
- An wen darf ich Newsletter verschicken und welche Informationspflichten habe ich zu beachten?
- Darf ich ehemalige Gäste kontaktieren?
- Welche Vorteile bringen Kundenbindungsprogramme?

5.1 Der Internetauftritt

Nutzer von Firmenwebseiten und firmeneigener Social Media Dienste sind rechtzeitig und in geeigneter Form auf die Speicherung, Nutzung und Übermittlung von personenbezogenen Daten an Dritte hinzuweisen. Ein **Impressum** gemäß § 5 Telemediengesetz (TMG) sowie eine **Datenschutzerklärung** nach § 13 TMG sind so einzubinden, dass sie **von jeder Seite aus abrufbar** sind.

5.1.1 Informationspflichten

Wenn das Hotel eine oder mehrere Webseiten anbietet, tritt es als Dienstanbieter gemäß Telemediengesetz auf. Entsprechend kommen auf das Hotel zunächst **„Allgemeine Informationspflichten“ (Impressum)** zu.

Gemäß § 5 TMG gehören zu den allgemeinen Angaben:

- den **Namen und die Anschrift**, unter der sie niedergelassen sind, bei juristischen Personen zusätzlich die
- **Rechtsform**, den Vertretungsberechtigten und, sofern Angaben über das Kapital der Gesellschaft gemacht werden, das Stamm- oder Grundkapital sowie, wenn nicht alle in Geld zu leistenden Einlagen eingezahlt sind, der Gesamtbetrag der ausstehenden Einlagen
- Angaben, die eine **schnelle elektronische Kontaktaufnahme** und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post
- das Handelsregister, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister, in das sie eingetragen sind, und die entsprechende **Registernummer**
- in Fällen, in denen sie eine **Umsatzsteueridentifikationsnummer** nach § 27a des Umsatzsteuergesetzes oder eine Wirtschafts-Identifikationsnummer nach § 139c der Abgabenordnung besitzen, die Angabe dieser Nummer
- bei Aktiengesellschaften, Kommanditgesellschaften auf Aktien und Gesellschaften mit beschränkter Haftung, die sich in **Abwicklung oder Liquidation** befinden, die Angabe hierüber.

Weitere Informationspflichten kommen auf den Webseitenbetreiber zu, wenn personenbezogene Daten direkt oder indirekt erhoben werden. Das fängt bei den Kontaktfeldern und Online-Reservierungen an und endet bei Protokolldaten (IP-Adresse, verwendeter Browser, etc.) und der Nutzung von Trackingtools (z.B. Google Analytics, Cookies, ...). Die Nutzung und ggf. Weitergabe der erhobenen Daten an Dritte ist genau und in verständlicher Form zu beschreiben. Seiner **zusätzlichen Informationspflicht** kommt der Webseitenbetreiber in einer **Datenschutzerklärung** (auch Privacy Policy) nach. Genau wie das Impressum auch, muss die Datenschutzerklärung von jeder Seite aus erkennbar und leicht erreichbar sein. Aus diesem Grund ist abzuraten, die Datenschutzerklärung im Impressum oder bei den AGBs zu integrieren, sondern diese sollte als eigene Seite in der Webseite erscheinen. Eine **Checkliste** zur Vollständigkeit einer Datenschutzerklärung finden Sie im Anhang.

Der Hotelier hat somit die Nutzer seiner Webseite *„**zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten** außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31) in **allgemein verständlicher Form zu unterrichten**, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. ...“*

Art. 7, 13 DSGVO fordern vor der direkten Erhebung von personenbezogenen Daten beim Nutzer eine formgerechte Einwilligung sowie die Benachrichtigung über den Umfang, die Nutzung, ... (siehe Pkt. 1.5.1) der erhobenen Daten. Als Webseitenbetreiber müssen Sie nachweislich sicherstellen, dass der Nutzer die Inhalte der Datenschutzerklärung gelesen bzw. bestätigt hat. Entsprechend empfiehlt sich das aktive Setzen eines Hakens in einem Kontrollkästchen und der Hinweis auf die allgemeinen Datenschutzbestimmungen inkl. Link auf die Datenschutzerklärung, bevor eine Datenübermittlung (Kontaktfelder, ...) oder verbindliche Reservierung durch den Nutzer erfolgen kann.

5.1.2 Urheberrechtsschutz

Beachten Sie, dass eine unerlaubte Veröffentlichung und Nutzung von Fotos und Grafiken auf der Webseite oder auch in Ihren Flyern Ansprüche auf Unterlassung, Beseitigung, Zahlung eines (verschuldensunabhängigen) angemessenen Lizenzentgeltes und Schadenersatzanspruches auslöst (§§ 2 UrhG). Ebenfalls die Verwendung von Musik, wie z.B. als Hintergrundmusik auf der Webseite, unterliegt dem Urheberrechtsschutz und ist entsprechend zu melden.

Sollten Sie Fotos oder Filme mit Personen anfertigen lassen oder diese auch selbst anfertigen, um diese auf der Webseite oder in sozialen Netzwerken, aber auch in anderen Printmedien zu veröffentlichen bzw. zu posten, beachten sie das Recht des Gastes oder auch Mitarbeiters am eigenen Bild gem. §§ 22, 23 KunstUrhG. Für diese Fälle benötigen Sie immer eine individuelle Einwilligungserklärung vom Abgebildeten. Wenn mehrere Personen auf einem Bild abgebildet werden, ist von jeder einzelnen Person das Einverständnis einzuholen. Ein Gruppenrecht gibt es nicht, Ausnahmen bestehen nur bei Personen aus dem öffentlichen Leben.

Auf größeren Veranstaltungen hat es sich bewährt, die Teilnehmer im Vorfeld (z.B. auf der Einladungskarte) über evtl. Film- und Fotoaufnahmen zu informieren, um ihnen die Möglichkeit zu geben zu entscheiden, ob sie sich derer entziehen möchten. Ein Aufsteller mit einer entsprechenden Information im Eingangsbereich der Veranstaltung sollte die Informationspflichten abrunden, um einer individuellen Einwilligung zu entgehen.

5.1.3 Verwendung von Cookies auf der Webseite

Wenn auf Ihrer Webseite **Cookies** verwendet werden, ist dies dem **Nutzer mitzuteilen**. Dies erfolgt i.d.R. durch eine Information in der Datenschutzerklärung. Verwendete **Cookies** sind genau zu beschreiben. Wenn die Cookies personenbezogene bzw. personenbeziehbare Daten speichern aber auch bei Cookies von Drittanbietern (Tracking & Targeting"-Cookies) zur Werbung anhand von Persönlichkeitsprofilen der Nutzer, ist eine Einwilligung erforderlich.

Derzeit erfolgt die Zustimmung des Nutzers stillschweigend. Dennoch wird empfohlen, dass bei Cookies, welche personenbezogene Daten verarbeiten, die aktive Zustimmung des Benutzers eingeholt wird.

Auf der Webseite der EU-Kommission http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm werden deren Vorstellungen /Anforderungen an den Umgang mit Cookies beschrieben. Ebenfalls finden Sie hier ein Script, welches auf der Hotelwebseite eingebunden werden kann.

Es empfiehlt sich einen Hinweis auf die Möglichkeit der Änderung der Nutzereinstellung im Browser in die Datenschutzerklärung mit aufzunehmen.

5.2 Social Media (Web 2.0)

Soziale Medien verändern die Prinzipien der Kommunikation. Aus dem klassischen „in-eine-Richtung-Kommunizieren" entwickelt sich eine Vielfalt an Kommunikationswegen mit vielen Sendern von Botschaften.

Hotels bieten sich daraus die Chancen, Nutzer schneller und besser zu erreichen, um diese z.B. über Angebote zu informieren und eine Bindung zu ihnen aufzubauen. Da die Trennung von beruflichem und privatem Auftreten bei der Nutzung sozialer Medien nur schwer möglich ist, ist es notwendig, sich über gemeinsame Regeln für die Nutzung der sozialen Medien zu verständigen (z.B. Darstellungen von persönlichen Meinungen, Veröffentlichung von Bildern, ...). Nur so ist ein erfolgreicher und gesetzeskonformer Einsatz von Kommunikation in den sozialen Medien möglich und die einzelnen Nutzer können Orientierung für ihr Handeln erhalten.

Offizielle Web 2.0-Angebote des Hotels (z.B. auch abteilungsbezogene Twitter-Accounts, Blogs, Facebook-Fanseiten etc.) sollten immer mit der Hotelleitung bzw. wenn vorhanden mit dem Bereich Sales & Marketing sowie dem PR Department abgestimmt werden. Die Einrichtung offizieller Accounts erfolgt im Namen des Hotels. Soweit ein Firmen-Account eingerichtet wird (z.B. Facebook-Fanseite), empfiehlt es sich, bei der Benutzerverwaltung darauf zu achten, verschiedene Rechte (Administrator, Redakteur, Moderator) zu vergeben. Denken Sie daran: Der Mitarbeiter, der die Facebook-Fanseite eventuell angemeldet und eingerichtet hat, wird nicht ewig im Hotel tätig sein.

Die Nutzer von firmeneigenen Social Media Diensten sind rechtzeitig und in geeigneter Form auf die Speicherung, Nutzung und Übermittlung von personenbezogenen Daten an Dritten hinzuweisen. Ein Impressum gemäß § 5 TMG ist einzubinden.

Mit der Veröffentlichung von Fotos, Bildern und Videos sind auch hier Urheberrechte und das Recht am eigenen Bild zu beachten. Ohne Zustimmung des Rechteinhabers bzw. der jeweiligen Personen dürfen die Bilder nicht veröffentlicht werden. Für die Veröffentlichung von Fotos mit Personen ist eine Fotoeinverständniserklärung einzuholen.

5.3 Werbemaßnahmen

Es gibt zahlreiche Möglichkeiten, an Adressen heranzukommen. Auf jeden Fall sollte immer geprüft werden, ob die **Herkunft der Daten rechtmäßig** ist oder ob diese eigentlich zu einem anderen Zweck erhoben wurden. Greift man auf seinen eigenen Datenbestand zurück, so ist zu prüfen, ob die Daten verwendet werden können. Grundsätzlich muss davon ausgegangen werden, dass die Daten zur Vertragserfüllung erhoben wurden.

Auf Anfrage von Interessenten (potenzielle Gästen) wird oft Informationsmaterial über das Hotel sowie über Dienst- und Serviceleistungen an diese auf dem Postweg oder elektronisch zugesendet. Bei den Anfragenden ist zwischen Geschäfts- und Privatkunden zu unterscheiden. Informationsanfragen wie die Zusendung von Prospekten sowie Informationen zu Gutscheinen und Arrangements sind vorrangig **Privatkunden** zuzuordnen. Die Kontakt- bzw. Adressdaten sind nur zum Zweck der Beantwortung der Anfrage zu erfassen bzw. zu speichern. Im Anschluss an den Vorgang sind die personenbezogenen Daten zu löschen. Ausnahmsweise können die Daten befristet gespeichert bleiben, wenn Vorgänge auf Wiedervorlage gelegt werden. Die Betroffenen sind davon in geeigneter Form in Kenntnis zu setzen. Angebotsanfragen sind meist **Geschäftskunden** zuzuordnen. Die Kontakt- bzw. Adressdaten der Unternehmen und derer Ansprechpartner sind nur zum Zweck der Beantwortung der Anfrage zu erfassen bzw. zu speichern. Eine Nachbereitung der Anfragen bzw. zusätzliche Akquisetätigkeiten bei Geschäftskontakten ist gemäß den gesetzlichen Rahmenbedingungen zulässig. Adress- und Kontaktdaten von Geschäftskunden sollten spätestens 3 Jahre nach dem letzten Kontakt gelöscht werden. Es ist die Verjährungsfrist gemäß § 195 BGB anzuwenden.

Wenn für die Durchführung der Werbung keine gesetzliche oder vertragliche Ermächtigung oder Verpflichtung vorhanden ist, wird fast immer die Zustimmung des Gastes einzuholen sein, wenn dieser beworben werden soll. Beachten Sie dafür, wie die **Einwilligungserklärung** formuliert ist. Vorgaben hierzu macht die DSGVO in den Artt. 7, 8. Es müssen hierbei die Werbemaßnahmen beschrieben sein, damit für den Gast Transparenz gegeben ist. Die Einwilligung muss freiwillig (unabhängig von einem Vertragsverhältnis) gegeben werden, leicht verständlich sowie nachweisbar sein und sich auf die jeweilige Datennutzung beziehen. Zur Nachweisbarkeit kann sowohl die Schriftform als auch die elektronische Protokollierung (z.B. Double-Opt-in) gewählt werden. Achten Sie auch auf den Hinweis zum Widerrufsrecht.

5.3.1 E-Mail-Werbung (Newsletter)

Die Nutzung der E-Mail-Adresse für einen **Newsletterservice** bedarf der schriftlichen Einverständniserklärung des Gastes, und dem Hinweis auf sein Recht auf Widerruf. Das Gesetz gegen den unlauteren Wettbewerb (UWG) besagt in § 7 Abs. 2 Nr. 3, dass die Zusendung von elektronischer Post, einschließlich SMS und Fax, ohne vorherige Einwilligung unzumutbar und somit unzulässig ist.

Soweit E-Mail-Adressen von Gästen direkt erhoben werden, dürfen diese zunächst nur zur Kommunikation genutzt werden. Die Nutzung für einen Newsletterservice bedarf der schriftlichen Einverständniserklärung des Gastes, und dem Hinweis auf sein Recht auf Widerruf.

Der Gast muss mit dem aktiven Setzen eines Hakens oder Kreuzes und/oder seiner Unterschrift einwilligen. Die elektronische Einwilligung muss vom angegebenen Empfänger stammen. Als einzige anerkannte Verfahrensweise gilt das „Double-Opt-in“ Verfahren. Der Versender des Newsletters sendet dem neuen Empfänger eine Authentifizierungs-E-Mail mit einem Aktivierungslink zu. Der Empfänger bestätigt den Erhalt durch Anklicken des Links. Der Zeitpunkt der Aktivierung ist zu Nachweiszwecken zu speichern. Der Versender und Empfänger schützen sich so vor dem Missbrauch von E-Mail-Adressen durch Dritte.

Die Bekanntgabe der E-Mail-Adresse in öffentlichen Verzeichnissen oder auf Briefköpfen, Visitenkarten und dergleichen ist keine Einwilligung zur Zusendung von Werbung. Aus Verzeichnissen oder Homepages abgeschriebene E-Mail-Adressen dürfen nicht werblich angeschrieben werden.

Eine Weitergabe von E-Mail-Adressen innerhalb eines Unternehmens-verbundes ist unzulässig, soweit keine explizite Einwilligung vorliegt.

Der Empfänger muss jederzeit die Möglichkeit haben, den Newsletter wieder abzubestellen. Diese Möglichkeit ist vorzugsweise auf jedem Newsletter zu integrieren, wo der Betroffene über seine Widerrufsrechte aufgeklärt wird. Die Bestellung und Abbestellung des Newsletters inkl. der Einwilligungserklärung ist zu dokumentieren.

5.3.2 Ausnahmeregelung für E-Mail-Werbung

E-Mail-Werbung ohne Einwilligung des Adressaten ist eine unzumutbare Belästigung. Dies gilt für den Privatbereich wie auch bei Geschäftskunden. Ausnahmen bestehen unter bestimmten Voraussetzungen für bestehende Geschäftsbeziehungen (§ 7 Abs. 3 Nr. 1 bis Nr. 4 UWG). So kann der Hotelier einen Newsletter auch ohne Einwilligung versenden, wenn er *„im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat.“*

Es müssen alle Bedingung gemäß § 7 Abs. 3 Nr. 1 bis Nr. 4 UWG erfüllt sein.

Im Rahmen der bestehenden Kundenbeziehung kann die verantwortliche Stelle für den Absatz **eigener, ähnlicher Waren und Dienstleistungen** per E-Mail werben, ohne die ausdrückliche Einwilligung des Kunden einzuholen bis die weitere Nutzung untersagt wird. **Auf die Widerspruchsmöglichkeit** muss der Kunde jedoch **bereits bei Erhebung der E-Mail-Adresse** und bei jeder unaufgeforderten Zusendung **hingewiesen werden**. Der Hinweis auf das Widerspruchsrecht muss auch enthalten, dass für die Übersendung des Widerspruchs keine ungewöhnlichen Kosten entstehen.

5.3.3 Postwerbung

Für die klassische Briefwerbung können **Kontaktdaten ehemaliger Gäste** genutzt werden (Art. 6 Abs. 1 lit. f DSGVO – Berechtigtes Interesse des Verantwortlichen), soweit kein Widerspruch zu dessen Nutzung besteht. Es ist sicherzustellen, dass der Empfänger den Absender und die datenverarbeitende Stelle klar erkennen kann und ihm die Möglichkeit gegeben wird, weitere Werbezusendungen zu verweigern **(Hinweis auf das Widerspruchsrecht)**. Dieses kann in einem abschließenden Satz auf dem Werbebrief erfolgen.

Soweit Adressdaten gekauft wurden oder die Adressdaten aus einem öffentlichen Verzeichnis stammen, ist der zu Bewerbende gemäß Art. 14 DSGVO über die Speicherung seiner Daten zu informieren. Es empfiehlt sich zusätzlich, die Herkunft der Daten auf dem Werbebrief mit anzugeben.

5.4 Gästebewertung

Die Befragung von Gästen während und nach dem Aufenthalt im Hotel dient der Qualitätskontrolle und der kontinuierlichen Verbesserung von Serviceleistungen. Die Veröffentlichung von Gästebewertungen auf der eigenen Internetseite kann zusätzlich als Entscheidungshilfe für Interessenten dienen.

5.4.1 Gästefragebogen

Fragebögen sind ein klassisches Instrument zur Gästebefragung. Der Umfang der Fragen sollte angemessen sein, und sich direkt auf die Bewertung von Serviceleistungen im Hotel beziehen.

Die Abfrage von Adress- und Kontaktdaten des Gastes sowie die Bewertung der Leistungen obliegen der Freiwilligkeit. Dem Befragten ist ein entsprechender Hinweis auf dem Fragebogen gut sichtbar anzugeben.

Gästefragebögen sind an einer zentralen Stelle zu sammeln und auszuwerten. Die Verantwortlichen haben darauf zu achten, dass die ausgefüllten Fragebögen sensibel behandelt werden. Soweit der Gast den Fragebogen anonym ausgefüllt hat, ist die verarbeitende Stelle nicht berechtigt, an Hand einer Zimmernummer o.ä. einen Rückschluss auf den Gast durchzuführen.

5.4.2 Online-Bewertungen

Zunehmend wird den Gästen angeboten, ihre Hotelbewertung online abzugeben. Diese wird dann auf der Hotelwebseite veröffentlicht. Viele Hotel nutzen Tools von Dienstleistern, welche die Punkte (Ranking) einzelner Bewertungen sowohl von der hoteleigenen Webseite als auch von anderen Bewertungsportalen zusammenfassen.

Die Online-Bewertung ist anonymisiert durchzuführen. Fragen zur Person sind so zu formulieren, dass diese nur einer bestimmten Personengruppe zuzuordnen sind. Eine Rückschlussmöglichkeit auf die Person ist untersagt. Um auszuschließen, dass das Bewertungs-Tool missbraucht wird, sind dem zu Befragenden Zugangsdaten oder ein Link zu einem geschützten Account in geeigneter Form zu übergeben.

Beachten Sie bei der Beantwortung von Online-Bewertungen, dass Sie keine Daten anführen, welche Rückschlüsse auf den Gast zulassen (Name, Adresse, Tel.Nr.).

Wird für die Online-Befragung ein Drittanbieter in Anspruch genommen, hat sich der Hotelier vor Inbetriebnahme des Service von den technischen und organisatorischen Datenschutzmaßnahmen zu überzeugen. Eine Datenschutzvereinbarung ist mit dem Dienstleister abzuschließen.

5.5 Kundenbindungsprogramme

Kundenbindungsprogramme richten Leistungs- und Kommunikationsangebote an bestimmte Kundensegmente - und zwar über den eigentlichen Kaufprozess hinaus. Ein Kundenbindungsprogramm kann beispielsweise folgende Leistungen umfassen: Kundenclub, Bonus- oder Rabattsysteme, Mehrwertdienste oder Events.

Die genannten Leistungen lassen sich in Form einer Kundenkarte vereinigen. Kundenkarten sind ein gebräuchliches Medium zur Kundenbindung - die Vorlage der Karte, auf der persönliche Daten gespeichert sind, erleichtert beispielsweise wesentlich den Check-In der Stammgäste in den Hotels. Um die Attraktivität der Karte

für die Gäste zu gewährleisten, werden die Karten durch Rabatte, Bonusprogramme, Services und besondere Informationen angereichert.

Kundenkarten

Die Kundenkarte trägt als Marketing-Instrument wesentlich zur Kundenbindung bei. Um mit ihren Gästen langfristige Geschäftsbeziehungen zu sichern, können Kundenkarten genutzt werden.

Die Erhebung der erforderlichen Gastdaten erfolgt i.d.R. beim Hotelbesuch auf einem Anmeldebogen, kann aber auch Online erfolgen. Sie ist unabhängig von den bereits gespeicherten Daten in der Hotelsoftware durchzuführen. Der Umfang der abzufragenden Daten zum Gast sollte angemessen und zweckentsprechend sein (Datensparsamkeit). Der Gast ist auf die Speicherung seiner Daten als Stammgast, und über die Nutzung weiterer Servicedaten hinzuweisen, die mit seinen Stammdaten verknüpft werden können. Für die Datenverarbeitung und -nutzungsmöglichkeit nach dem Auschecken ist eine Einwilligungserklärung auf dem Anmeldebogen einzuholen, der Gast ist über die Datennutzung und sein Widerrufsrecht aufzuklären. In der Hotelsoftware ist der Datensatz zum Gast entsprechend zu kennzeichnen.

Für die Nutzung der Gastdaten innerhalb einer Hotelgruppe ist eine zusätzliche Einwilligungserklärung auf dem Anmeldebogen über die gemeinsame Nutzung einzuholen, die unabhängig von der zuvor abgegebenen Einwilligungserklärung ist. Der Gast ist auch hier über die Datennutzung, Datenweitergabe und sein Widerrufsrecht aufzuklären. In der Hotelsoftware ist der Datensatz zum Gast für die Datenfreigabe gegenüber verbundener Unternehmen zu kennzeichnen.

Nur unter Angabe der Kundennummer können die beteiligten Hotels auf die jeweiligen Gastdaten zugreifen. Die Nutzungsrechte in der Hotelsoftware sind restriktiv zu gestalten. Gestattet ist der Zugriff auf Stamm- und Servicedaten sowie die Hotelhistorie im eigenen Haus.

Bonusprogramme

Es gibt verschiedene Formen von Bonusprogrammen. Die gängigste ist die mit Bonusfunktion. Hier bietet eine Kundenkarte Leistungen, die nur für den Karteninhaber gelten und für diesen besonders günstig sind. Auf die mit der Karte gesammelten Umsätze wird dem Gast nachträglich eine Vergütung oder Prämie gewährt. Die Gewährung von Ansprüchen kann in Hotelgruppen übergreifend sein. Die Nutzungsrechte im Bonussystem sind restriktiv zu gestalten. Beteiligte Unternehmen dürfen Bonuspunkte gutschreiben bzw. einlösen, und die gesammelten Bonuspunkte summarisch lesen. Die Zusammenführung von Bonusdaten ist zu zentralisieren.

Für das Bonussystem ist eine zusätzliche Einwilligungserklärung einzuholen. Der Gast ist über die Datennutzung, Datenweitergabe und sein Widerrufsrecht aufzuklären.

Es ist zulässig, das Bonusprogramm mit der Kundenkarte zu verknüpfen.

Persönlicher Internet-Account

Geschäfts- und Stammkunden kann die Möglichkeit gegeben werden, in einem persönlichen Account Zimmerbuchungen vorzunehmen bzw. zu stornieren, und Bonuspunkte einzulösen.

Die Einrichtung und Verwaltung von Stamm- und Nutzungsdaten obliegt der Freiwilligkeit. Der Umfang von Pflichtfeldern sollte angemessen und zur Vertragserfüllung notwendig sein. Pflichtfelder sind zu kennzeichnen.

Dem Benutzer sind zur Anmeldung die Login-Daten und das Passwort mitzuteilen. Der Benutzer ist aufzufordern, bei der ersten Nutzung das Passwort zu ändern. Alle gespeicherten Daten sind vertraulich zu behandeln und vor dem Zugriff unbefugter Dritter zu schützen.

Für die Speicherung und Nutzung der personenbezogenen Daten ist eine Einwilligungserklärung direkt und formgerecht einzuholen. Die Anmeldung ist zu dokumentieren.

Es ist zulässig, den persönlichen Internet-Account mit der Kundenkarte und dem Bonusprogramm zu verknüpfen.

Für die Datenspeicherung und Nutzung im persönlichen Internet-Account ist eine zusätzliche Einwilligungserklärung einzuholen. Der Gast ist über sein Widerrufsrecht aufzuklären.

Gewinnaktionen und Verlosungen

Die Erhebung und Speicherung von Adress- und Kontaktdaten über Gäste und andere Interessenten zur Durchführung von Gewinnaktionen und Verlosungen ist an die durchgeführte Aktion gebunden. Ein Anspruch auf die Nutzung gespeicherter Daten nach der Beendigung der Aktion besteht nicht, es sei denn, der Teilnehmer hat diesem formgerecht zugestimmt.

Die Durchführung von Aktionen sind zeitlich zu begrenzen, die Gewinner sind zu dokumentieren. Soweit statistische Angaben aus der Aktion generiert werden sollen, sind diese zu anonymisieren und zusammenzufassen.

Bei der Speicherung von Adress- und Kontaktdaten ist sicherzustellen, dass niemand unbefugt Einsicht nehmen oder Kopien bzw. Ausdrucke anfertigen kann. Die gespeicherten Daten sind spätestens 6 Monate nach Beendigung der Aktion zu löschen.

- Bevor eine Marketingaktivität durchgeführt wird, sollte der Zweck der Aktivität geprüft und schriftlich fixiert werden.
- Speicherfristen zur Nutzung von Adressdaten zu Vertriebsaktivitäten sind festzulegen.
- Beim Internetauftritt sind gesetzliche Informationspflichten zu beachten. Die gesetzlichen Erfordernisse lt. TMG und UWG sind bei Webseite und E-Mail-Werbung einzuhalten.
- Werden Reservierungen über Ihre Webseite getätigt, so sollte die Anwendung der AGBs und der Datenschutzerklärung vor Vertragsabschluss durch den Gast aktiv bestätigt werden. Weiters sollten diese in den Sprachen, in denen die Webseite vorhanden ist, aufliegen, gespeichert und wiedergegeben werden können.
- Besonderes Augenmerk ist auf die Herkunft der Adressdaten und E-Mail-Adressen zu legen. Hier ist zu prüfen, ob die Daten verwendet werden dürfen oder ob die Daten für einen anderen Zweck erhoben wurden.
- Speicherfristen zur Nutzung von Adressdaten zu Vertriebsaktivitäten sind festzulegen.
- Bei Verwendung von personenbezogenen Cookies ist dies zumindest auf der Webseite anzuführen, zu bevorzugen ist eine Zustimmung durch den Besucher der Webseite.
- Einhaltung der Urheberrechte in allen Medien sind zu beachten.
- Beachtung des Widerspruchs- und Widerrufsrechts.
- Einwilligungserklärungen können zusammen mit Informationspflichten zur Nutzung von Adress- und Kontaktdaten zu Werbezwecke beim Antrag einer Kundenkarte berücksichtigt werden.

- ✓ Überprüfung der gesetzlichen Informationspflichten auf der Webseite, aber auch auf dem Geschäftspapier und in der E-Mail.
- ✓ Ist auf meiner Website die Information zur Streitbeilegung angeführt?
- ✓ Wo befinden sich die AGBs und Hinweise zur Verarbeitung personenenbezogener Daten (Datenschutzerklärung)? Sind diese in den entsprechenden Sprachen vorhanden? Können diese gespeichert und wiedergegeben werden?
- ✓ Hinweispflicht bei Verwendung von personenbezogenen Cookies bzw. Zustimmung durch den User implementieren.
- ✓ Kontrolle, ob bei allen Medien das Urhebergesetz eingehalten wird.
- ✓ Überprüfung des Newsletterversands.
- ✓ Gibt es eine Dokumentation aller Vertriebs- und Marketingaktivitäten?
- ✓ Wo werden Adress- und Kontaktlisten noch gespeichert (Excel-Dateien)?
- ✓ Wird ein Datenexport dokumentiert? Wer kann Gastdaten exportieren?

6 Datenverarbeitung im Auftrag

Zielfragen

- Was ist eine Datenverarbeitung im Auftrag?
- Welche gesetzlichen Anforderungen sind zu erfüllen?
- Darf ich jeden Dienstleister beauftragen?
- Welche Prüfpflichten habe ich?
- Was ist eine Datenschutzvereinbarung?
- Wer ist dafür verantwortlich, eine Datenschutzvereinbarung abzuschließen?
- Was kann passieren, wenn keine Vereinbarungen zum Datenschutz mit dem Dienstleister verabschiedet wurden?

Die Datenverarbeitung im Auftrag oder auch Auftragsverarbeitung ist die Erhebung, Speicherung, Verarbeitung, Nutzung oder Löschung von personenbezogenen Daten **durch einen Auftragnehmer** gemäß den Weisungen der verantwortlichen Stelle (Hotelier als Auftraggeber) auf Grundlage eines schriftlichen Vertrags. Mit anderen Worten: Wenn Sie einen Vertrag mit einem Dienstleister schließen bzw. geschlossen haben, der von Ihnen personenbezogene Daten erhält, um diese auf Ihre Anweisung hin zu nutzen, z.B. um Werbebriefe zu drucken und zu versenden oder um die Lohnverrechnung durchzuführen, dann handelt es sich um eine Datenverarbeitung im Auftrag. Das Versenden von Werbebriefe, bspw. über einen Lettershop ist noch ein einfaches Beispiel. So sprechen wir auch von einer Datenverarbeitung im Auftrag, wenn Sie Software-Applikationen, insbesondere webbasierte Tools, nutzen. Sobald bereits personenbezogene Daten auf Servern von Dienstleistern gespeichert werden, und der Dienstleister im Rahmen von Supportarbeiten Zugriff auf die in der Datenbank gespeicherten Daten haben kann, spricht der Gesetzgeber von einer Auftragsverarbeitung. Auch beim Hosting ist zu prüfen, ob der Dienstleister eventuell auf die Daten zugreifen kann. Vergessen Sie nicht, Administratoren haben oft weitreichende Zugriffsrechte! Somit wird auch (Fern-) Wartungsarbeiten ein hoher Stellenwert zugeschrieben. Wenn der Systemanbieter allein die Möglichkeit hat, personenbezogene Daten beim Support zu sehen (Kenntnisnahme), unterliegt das Auftragsverhältnis ebenfalls der Datenverarbeitung im Auftrag. Zu guter Letzt ist auch die Löschung bzw. eher die Vernichtung von Daten zu beachten. So sind die Aktenvernichtung, Vernichtung von Datenträgern oder Entsorgung von Computern ebenfalls zu berücksichtigen.

Die DSGVO regelt die Auftragsverarbeitung in Art. 28 ff. **Als Auftraggeber sind Sie dazu verpflichtet, die Anforderungen umzusetzen.** Anderenfalls können Bußgelder bis zu 10 Mio. € durch die Datenschutzaufsichtsbehörden verhängt werden.

Es ist empfehlenswert, über die bestehenden Verträge ein Vertrags-verzeichnis zu führen.

Prüfen Sie also alle **Auftragsverhältnisse und Verträge**, es müssen **Datenschutzvereinbarungen** abgeschlossen werden, wenn es sich um eine Datenverarbeitung im Auftrag handelt. Sollen also personenbezogene Daten im Auftrag verarbeitet werden (z.B. Fernwartung Hotelsoftware, Online-Reservierungssystem, Newsletterservice, Lohnbuchhaltung, aber auch Entsorgungsunternehmen), darf gemäß Art. 28 Abs. 1 DSGVO nur mit

Auftragnehmern gearbeitet werden, die hinreichende Garantien für eine **Verarbeitung nach den Grundsätzen der DSGVO** bieten. Dies erfordert eine **Prüfung der Auftragnehmer**, ob diese hinreichende Garantien und aktuelle technische und organisatorische Maßnahmen eingerichtet haben. In Abhängigkeit von der Höhe des Risikos für die Rechte und Freiheiten der Betroffenen sind die hinreichenden Garantien bzw. die Angemessenheit und Aktualität der technischen und organisatorischen Maßnahmen regelmäßig zu überprüfen.

Wird entgegen Art 28 DSGVO ein Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder sich nicht vor Beginn der Datenverarbeitung über die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt, so kann in diesem Falle die zuständige Aufsichtsbehörde mit einer Geldbuße bestrafen.

Der Hotelier bleibt als Auftraggeber auch bei den Stellen für ausreichende **Datensicherheit** verantwortlich, die unmittelbar oder mittelbar in ihrem Auftrag tätig werden. Über die Beauftragung ist ein **Vertrag nach den Vorgaben des Art. 28 Abs. 3 DSGVO** abzuschließen.

6.1 Abgrenzung der Datenverarbeitung im Auftrag

Datenschutzrechtlich zu unterscheiden sind beim Outsourcing die Auftragsverarbeitung und die Funktionsübertragung. Die Frage ob ein Outsourcing als **Auftragsverarbeitung** oder **Funktionsübertragung** (Datenübermittlung zu anderen Zwecken ohne Weisungsbefugnis) anzusehen ist, hängt von der jeweiligen rechtlichen Ausgestaltung ab und kann daher nur im Einzelfall beantwortet werden. Die rechtlichen Ausgestaltungsmöglichkeiten sind ähnlich vielfältig wie die tatsächlichen Erscheinungsformen des Outsourcings.

Die Funktionsübertragung ist ein Fachbegriff, um Sachverhalte zu beschreiben, bei denen die Vorschriften über die Datenverarbeitung im Auftrag nicht angewendet werden können.

Bei der **Datenverarbeitung im Auftrag** wird nicht die Aufgabe selbst, zu deren Zweck die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten erfolgt, ausgelagert, sondern lediglich der zur Aufgabenerledigung erforderliche Umgang mit den Daten. Der in Anspruch genommenen Serviceeinrichtung wird der Umgang mit den Daten nach Weisung und unter materieller Verantwortung des Auftraggebers übertragen. Die datenschutzrechtliche Verantwortung für die Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten verbleibt beim Auftraggeber. Er schreibt die technischen und organisatorischen Maßnahmen zur Datensicherheit beim Auftragnehmer vor.

Erkennungsmerkmale für Auftragsverarbeitung

- fehlende Entscheidungsbefugnis des Auftragnehmers,
- Weisungsgebundenheit des Auftragnehmers bezüglich dessen, was mit den Daten geschieht,
- Umgang nur mit Daten, die der Auftraggeber zur Verfügung stellt; es sei denn, der Auftrag ist auch auf die Erhebung personenbezogener Daten gerichtet,
- Ausschluss der Verarbeitung oder Nutzung der Daten zu eigenen Zwecken des Auftragnehmers,
- keine (vertragliche) Beziehung des Auftragnehmers zum Betroffenen,
- Auftragnehmer tritt (gegenüber dem Betroffenen) nicht in eigenem Namen auf.

Bei der **Funktionsübertragung** wird dagegen auch die der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zugrunde liegende Aufgabe ganz oder teilweise abgegeben. Die in Anspruch genommene Serviceeinrichtung erbringt - über die technische Durchführung des Umgangs mit personenbezogenen Daten hinaus - materielle Leistungen mit Hilfe der überlassenen Daten. Sie handelt hierbei **eigenverantwortlich**, auch **im Sinne des Datenschutzrechts**.

Erkennungsmerkmale für Funktionsübertragung

- Weisungsfreiheit des Dienstleisters bezüglich dessen, was mit den Daten geschieht,
- Überlassung von Nutzungsrechten an den Daten,
- eigenverantwortliche Sicherstellung von Zulässigkeit und Richtigkeit der Daten durch den Dienstleister, einschließlich des Sicherstellens der Rechte von Betroffenen (Benachrichtigungspflicht, Auskunftsanspruch),
- Handeln des Dienstleisters (gegenüber dem Betroffenen) im eigenen Namen,
- Entscheidungsbefugnis des Dienstleisters in der Sache.

Hotelreservierungsportale (OTAs), Steuerberater (soweit sie keine zusätzlichen Dienstleistungen ausführen), Inkassounternehmen (beitreiben von offenen Forderungen), Rechtsanwälte, Paketdienst zur Auslieferung von Ware an Kunden, Wirtschaftsprüfer oder der externe Betriebsarzt.

Sonderfall Wartung und Pflege

Einen Sonderfall bildet die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen. Solche Tätigkeiten sind z.B.

- Installation, Wartung, Pflege und Prüfung von Netzwerken, Hardware (einschließlich Telekommunikationsanlagen) und Software u.a. (Betriebssysteme, Anwendungen)
- Programmentwicklungen/-anpassungen/-umstellungen, Fehlersuche und Tests
- Durchführung einer Datenübernahme von einem System in ein anderes. (Migration)

Sie können direkt vor Ort oder per Fernwartung durchgeführt werden. Die Tätigkeiten sind nicht auf den Umgang mit personenbezogenen Daten gerichtet, allerdings ist die Kenntnisnahme von personenbezogenen Daten nicht immer ausgeschlossen. Daher ist gemäß Art. 28 DSGVO i.V.m. Art. 4 Nr. 2 DSGVO die Erbringung von (Fern-)Wartungs- und Pflegearbeiten den Regelungen zur Auftragsverarbeitung zu unterwerfen, soweit bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten unvermeidlich ist.

Mit Art. 4 Nr. 2 DSGVO bezeichnet der Ausdruck „Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Diese Definition erfüllt die Wartung eines IT-Systems in jedem Fall. Die Verarbeitung der personenbezogenen Daten erfolgt somit auch im Auftrag des Verantwortlichen. Auch nach dem gesetzlichen Schutzzweck kann ein solcher Vorgang nicht dem Anwendungsbereich der DSGVO entzogen werden, sofern er mit einer Zugriffsmöglichkeit auf die personenbezogenen Daten und damit mit einer Gefahr für das informationelle Selbstbestimmungsrecht der Betroffenen verbunden ist.

6.2 Auswahl des Dienstleisters

6.2.1 Prüfung des Leistungsumfangs

Bevor ein Vertrag mit einem Dienstleister o.ä. unterzeichnet werden kann, ist der Leistungsumfang von der verantwortlichen Stelle dahingehend zu prüfen, in wieweit der Auftragnehmer Kenntnis über personenbezogene Daten (Gast-, Mitarbeiter- oder Lieferantendaten) erlangen kann oder diese im Rahmen seiner Aufgaben erhebt, speichert, nutzt, übermittelt oder löscht.

Die aufgeführten Beispiele stellen nur einen Auszug dar. Es gilt immer zu prüfen, ob personenbezogene Daten in irgendeiner Form verarbeitet werden. Dieses können auch Netzwerk-protokolle oder IP-Adressen von Computern sein.

Beispiele nach System

Kenntnisnahme:	Hosting und/oder Fernwartung Hotelsoftware
	Reinigungspersonal (Gästelisten)
Erheben, Speichern und Übermitteln:	Online-Buchungssystem
	Lohnbuchhaltung
	Newsletterservice
Nutzen:	PR-Agentur (Mailing)
Löschen:	Aktenvernichtung
	Datenträgervernichtung

Im Anhang finden Sie eine **Checkliste** mit möglichen Auftragsverarbeitungen, wobei diese keinen Anspruch auf Vollständigkeit hat.

6.2.2 Besondere Prüfungspflichten im Rahmen der Datenschutz-Folgenabschätzung

Wenn eine Form der Verarbeitung von personenbezogenen Daten, insbesondere bei Verwendung neuer Technologien oder aufgrund des Umfangs, der Umstände und Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, muss der Verantwortliche gemäß Art. 35 DSGVO vorab eine Abschätzung der Folgen für den Schutz der personenbezogenen Daten der Betroffen durchführen. Das gilt selbstverständlich auch für den Fall, dass der Hotelier einen Dienstleister damit beauftragt, Daten zu erheben, zu speichern, zu verarbeiten, zu nutzen oder weiterzuleiten, die der Pflicht zur Datenschutz-Folgenabschätzung unterliegen. Vergleichen Sie hierzu Pkt. 3.3.

6.2.3 Berücksichtigung der Eignung

Es darf nur ein Auftragsverarbeiter beauftragt werden, wenn dieser **ausreichende und hinreichende Garantien** erbracht hat und die notwendigen technischen und organisatorischen Maßnahmen im Einklang mit den Anforderungen der DSGVO stehen. Als Beleg solcher Garantien können auch genehmigte Verhaltensregeln des Auftragsverarbeiters nach Art. 40 DSGVO oder Zertifizierungen nach Art. 42 DSGVO herangezogen werden.

Die technischen und organisatorischen Maßnahmen bzw. Garantien hat der Auftragsverarbeiter am Beginn des Vertragsverhältnisses beizubringen. Der Datenschutzbeauftragte führt eine entsprechende Prüfung durch.

Der Auftragnehmer ist vor Vertragsunterzeichnung unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Das Ergebnis ist zu dokumentieren.

6.3 Vertragsgestaltung und Vertragsabschluss

Der Vertrag kann in schriftlicher oder elektronischer Form abgefasst werden. Bei der Vertragsgestaltung sind auf Grundlage von Art. 28 Abs. 3 DSGVO folgende Gesichtspunkte zu beachten:

- Art und Umfang der übertragenen Datenverarbeitung oder -nutzung (Leistungsumfang) sind festzulegen.

Dazu sollten insbesondere konkret geregelt sein:

- Weisungsbefugnis des Auftraggebers/Verantwortlichen,
- Verpflichtung des Auftragnehmers, nur solche Personen bei der Verarbeitung und Nutzung personenbezogener Daten einzusetzen, die mit den Vorschriften des Datenschutzgesetzes vertraut gemacht und auf das Datengeheimnis verpflichtet worden sind,
- Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO zum Schutz der zur Verarbeitung übergebenen Daten vor einer unbefugten Verwertung, insbesondere zur Verhinderung des Missbrauchs von Daten durch unbefugten Zugriff, Verfälschung, Zerstörung, Verlust oder Preisgabe an Unbefugte.
- Verpflichtung des Auftragnehmers, Subunternehmen nur nach vorheriger Abstimmung mit dem Hotel einzusetzen,
- Verpflichtung zur Unterstützung der Umsetzung von Betroffenenrechte gemäß Art. 32 bis 36 DSGVO,
- Verpflichtung des Auftragnehmers zur Löschung/Rückgabe von personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen,
- Vereinbarung hinreichender Kontrollmöglichkeit, z.B. indem sich der Hotelier das Recht vorbehält, stichprobenweise Überprüfungen vorzunehmen,
- Führung eines Verfahrensverzeichnisses gemäß Art. 30 Abs. 2 DSGVO
- Verpflichtung des Auftragnehmers, Informationen, die ihm im Rahmen seiner Tätigkeit für das Hotel bekannt werden, weder zu verwerten noch Dritten zugänglich zu machen.

6.3.1 Abgrenzung der Leistung

Im ersten Schritt ist entsprechend den Merkmalen aus Pkt. 6.1 abzugrenzen, ob es sich bei der Dienstleistung um eine Auftragsverarbeitung oder eine Funktionsübertragung handelt. Soweit der Hotelier Einfluss auf die Datenverarbeitung und den Zugriff auf die eigenen Daten hat, ist von einer Auftragsverarbeitung auszugehen. Der

Auftragnehmer hat i.d.R. keine (vertragliche) Beziehung zum Betroffenen. Handelt es sich um eine Auftragsverarbeitung, so muss das Auftragsverhältnis gemäß Art. 28 DSGVO datenschutzrechtlich abgesichert werden.

Ist der Dienstleister weisungsfrei und handelt er im eigenen Namen gegenüber dem Betroffenen, kann von einer Funktionsübertragung ausgegangen werden. Handelt es sich um eine Funktionsübertragung, so müssen keine zusätzlichen datenschutzrechtlichen Vereinbarungen getroffen werden. Das Vertragsverhältnis ist zu dokumentieren.

6.3.2 Auswahl der Vertragsform

Soweit eine Auftragsverarbeitung im Sinne von Art. 28 DSGVO vorliegt, kommen unterschiedliche Verpflichtungen auf die Vertragsparteien zu. Durch den Gesetzgeber sind eng definierte Vorgaben an der Vertragsgestaltung entsprechend Pkt. 6.3 vorgegeben.

Als Vertragsformen kommen i.d.R. Dienstleistungs- oder Serviceverträge, Rahmenvereinbarungen im Zusammenhang mit einer kooperativen Zusammenarbeit sowie Vertragsbeziehungen mit Fremdpersonal im eigenen Hause in Betracht. Entsprechend ist das Unternehmen oder die Einzelperson als Auftragnehmer auf das Datengeheimnis durch das Hotel als Auftraggeber vor oder im Zuge des Vertragsabschlusses zu verpflichten. Sind die vertraglichen Anforderungen im abzuschließenden Vertragsentwurf nicht erfüllt, hat die vertragsführende Stelle des Hotels zusätzlich zum Vertrag den Auftragnehmer entsprechend mit einer Zusatzvereinbarung zu verpflichten.

Prüfen Sie ob und wenn ja welche Art des Vertrages mit Ihrem Auftragnehmer vorhanden ist. Dementsprechend ist dann zu berücksichtigen, ob lediglich eine Verpflichtung auf das Datengeheimnis, eine Vertraulichkeitsvereinbarung, eine Datenschutzvereinbarung oder sogar eine EU-Standardvertragsklausel abzuschließen ist.

Die nachfolgende Aufstellung hilft Ihnen bei der Entscheidungsfindung.

Vertragsarten	Vertragsformen zur Zusatzvereinbarung
Dienstleistungs- und Servicevertrag	Auftrag gemäß Art. 28 DSGVO Verpflichtung von Dritten – Vertragspartnern – auf das Datengeheimnis Vertraulichkeitsvereinbarung
Fremdpersonal	Verpflichtung von Dritten – Fremdpersonal – auf das Datengeheimnis
Rahmenvereinbarungen	Datenschutzvereinbarung / Zusatzvereinbarung
Datenübermittlung in Drittstaaten ohne angemessenen Datenschutzniveau (Drittländer außerhalb der EU/EWR)	EU-Standardvertragsklausel
Datenübermittlung in Drittstaaten mit angemessenen Datenschutzniveau (auch Privacy Shield)	Datenschutzvereinbarung (DEU/ENG)

6.3.3 Bestehende Verträge

Bereits geschlossene Verträge sind auf datenschutzrechtliche Anforderungen gemäß DSGVO zu überprüfen. Soweit die bestehenden Verträge nicht im Einklang mit Art. 28 DSGVO stehen, sind die Vertragspartner neu zu verpflichten.

6.3.4 Kündigung des Vertragsverhältnisses

Die vertragsführende Stelle hat mit Beendigung eines Vertragsverhältnisses folgende Schritte zu prüfen, umzusetzen und zu dokumentieren:

- Löschung von Zugangsrechten (Netzwerk, auch Fernwartung)
- Löschung von Benutzerrechten (Verfahren, Anwendungen, ...)
- Datenschutzgerechte Löschung/Vernichtung von Daten beim Auftragnehmer
- Rückgabe von Datenträgern und Unterlagen
- Schriftliche Bestätigung zu den durchgeführten Maßnahmen vom Auftragnehmer

- ❖ Wenn ein Dienstleister beauftragt wird, personenbezogene Daten für das Hotel zu erheben (Online-Reservierung auf eigener Webseite), zu speichern (Hosting), zu nutzen (Lettershop), weiterzuleiten (Mailservice) aber auch zu vernichten/löschen (Aktenvernichtung), handelt es sich in der Regel um eine Datenverarbeitung im Auftrag. Hinzu kommt auch die Möglichkeit der Kenntnisnahme, bspw. im Rahmen einer Fernwartung.
- ❖ Für die Datenverarbeitung gibt es strenge gesetzliche Vorgaben, für dessen Umsetzung der Hotelier verantwortlich ist.
- ❖ Der Hotelier bzw. der Datenschutzbeauftragte hat sich vor Beginn der Dienstleistung davon zu überzeugen, dass das Vertragsverhältnis nach internen und gesetzlichen Vorgaben abläuft.
- ❖ Auch bestehende Verträge sind zu berücksichtigen.
- ❖ Beim Ignorieren der Anforderungen kann sich der Hotelier schlechtesten Falls einem hohen Bußgeld oder erhebliche Schadensersatzforderungen gegenübersehen.

- ✓ Prüfung der Verträge! Kenne ich meine Dienstleister, die der Datenverarbeitung im Auftrag unterliegen?
- ✓ Vertragsgestaltung. Welche datenschutzrechtlichen Anforderungen berücksichtigen die bestehenden Verträge?
- ✓ Datenschutzvereinbarung. Wer nimmt Kontakt zum Dienstleister auf? Hat der Dienstleister eigene Datenschutzvereinbarungen?
- ✓ Dokumentation. Wie erfülle ich meine Dokumentationspflichten?
- ✓ Vertragsende. Hat der Dienstleister ein Recht, meine Daten zu behalten?

7 Videoüberwachung

Zielfragen

- Was ist eine Videoüberwachung?
- Was muss ich bei der Installation einer Videoüberwachung berücksichtigen?

7.1 Was ist eine Videoüberwachung?

Videoüberwachung ist die systematische, insbesondere fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt oder eine bestimmte Person betreffen, mittels technischer Bildaufnahme oder Bildübertragungsgerät. Sie wird in § 4 BDSGneu für die Überwachung in öffentlich zugänglichen Räumen geregelt. Eine Regelung in der DSGVO gibt es nicht.

Bevor eine Videoanlage in Betrieb genommen werden kann, ist diese durch den Datenschutzbeauftragten zu prüfen, um auszuschließen, dass Persönlichkeitsrechte durch die Aufzeichnungen verletzt werden. Der Datenschutzbeauftragte muss eine Datenschutz-Folgenabschätzung durchführen, die Videoüberwachungsanlage ist in das Verzeichnis für Verarbeitungstätigkeiten aufzunehmen.

Bei der Prüfung der Videoüberwachung sind insbesondere nachfolgende Kameratypen zu beachten:

- Analog-Aufzeichnungen
- Echtzeitüberwachung ohne Speicherung von Bildern
- Videoaufzeichnungen mit Speicherung von Bild und ggf. Ton
- Kamera-Dummys

Im Rahmen der Datenschutz-Folgenabschätzung sollten alle Kameras, egal welchen o.g. Typs einzeln aufgeführt und beschrieben werden. Es ist eine Übersicht zu führen, wo sich die jeweiligen Kameras befinden (ein Lageplan ist hier hilfreich). Zusätzlich sind zu jeder Kamera nachfolgende Kriterien aufzuführen:

- Bezeichnung
- Modell
- Auflösung
- Mikrofon [Ja/Nein]
- Schwenkbar [Ja/Nein]
- Neigbar [Ja/Nein]
- Zoom [Ja/Nein]
- Blickwinkel
- Aufzeichnungssystem
- Speicherdauer
- Installationsdatum
- Beobachter [z.B. IT/Rezeption]
- Zweck der Überwachung
- Foto von der Kamera
- Foto der Kennzeichnung
- Bildschirmausdruck (Screenshot)

Eine Checkliste zum Einsatz und Nutzung von Videokontrollsystemen finden Sie im Anhang.

In der Praxis werden die meisten Videoaufnahmen auf Festplattenrekordern o.ä. gespeichert. Der Hotelier hat sicherzustellen, dass kein Unbefugter an die Aufzeichnungen gelangt. Sowohl der Festplattenrekorder/Server/... als auch die Anwendung selbst sind mit einem starken Kennwortschutz zu versehen. Es empfiehlt sich, die Aufzeichnungen in einem verschlüsselten Bereich zu speichern.

7.2 Zulässige und unzulässige Videoüberwachungen

Am Beginn ist zu prüfen, ob das Ziel, das mit der Videoüberwachung erreicht werden soll, auch das **gelindeste zum Zweck führende Mittel** ist. Eine Videoüberwachung in öffentlichen Räumen kann ausschließlich zur Wahrnehmung des Hausrechts, zum Schutz des Eigentums gegenüber Dritten sowie zur Abwehr von Gefahren, wie die Verfolgung von strafbaren Handlungen, also zum Schutz der Mitarbeiter und des Eigentums gerechtfertigt werden. Die Auswertung der Videoaufzeichnungen darf nur anlassbezogen erfolgen. Eine Leistungs- und Verhaltenskontrolle von Mitarbeitern oder Anderen ist auszuschließen.

Sollte es daher andere Mittel geben, die die gleiche Wirkung haben, aber nicht in diesem Ausmaß in die Persönlichkeitsrechte der Betroffenen eingreifen, so sind dieses der Videoüberwachung vorzuziehen.

Eine Videoüberwachung kann nicht damit gerechtfertigt werden, dass das Eigentum der Gäste zu schützen ist. Es kommt oft vor, dass Koffer aus dem Empfangsbereich und Taschen, Jacken sowie mobile Geräte im Restaurant gestohlen werden. Die Aufklärung von Straftaten liegt im Hoheitsgebiet der Strafverfolgungsbehörden, für das Eigentum des Gastes ist dieser immer selbst verantwortlich, es sein denn, er hat es in die Obhut des Hotels gegeben (z.B. Kofferraum).

Es sind die schutzwürdigen Interessen der Betroffenen mit den Interessen des Hotels abzuwägen. Wenn folgende Punkte zu Gunsten des Hotels sprechen, so wird die Videoüberwachung rechtmäßig werden:

- Lebenswichtige Interessen einer Person liegen vor.
- Der Betroffene hat zugestimmt. (Videoeinverständniserklärung für Mitarbeiter in permanent überwachten Bereichen)
- Bestimmte Fakten rechtfertigen die Annahmen, dass der überwachte Bereich Ort/Ziel eines gefährlichen Angriffs werden könnte. (z.B. unübersichtliche Bereiche und Eingänge, der unmittelbar angrenzende Gehsteig bei Überwachung der Gebäudefassade, aber nicht darüber hinaus)
- Anwendbare Rechtsvorschriften oder gerichtliche Entscheidungen übertragen dem Hotelier spezielle Sorgfaltspflichten, zum Schutz des Objektes oder der überwachten Person.

Videoüberwachungen an Plätzen, die zum höchstpersönlichen Lebensbereich der Betroffenen zählen wie z.B. Gästezimmer, Umkleideräume, Sanitär und WC Anlagen, sind unzulässig. Aber auch im Gastronomiebereich, in der Lobby oder im Schwimmbad muss der Datenschutzbeauftragte im Rahmen der Datenschutz-Folgenabschätzung zwischen den Interessen der Betroffenen und des Hotels stark abwägen. Aufzeichnungen mit Ton sind in Bereichen, in denen Betroffene länger verweilen, ebenfalls unzulässig.

Eine **verdeckte Videoüberwachung** von Beschäftigten ist nur zulässig, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass Beschäftigte im Beschäftigungsverhältnis eine Straftat begangen

haben, die Erhebung zur Aufdeckung erforderlich ist und Art und Ausmaß der Erhebung im Hinblick auf den Zweck nicht unverhältnismäßig sind. Im Vorfeld ist die vermutete Straftat bei den Strafverfolgungsbehörden anzuzeigen.

7.3 Kennzeichnungspflicht

Die Durchführung einer Videoüberwachung ist durch das **Anbringen von Symbolen** oder mit deutlich lesbaren Aufschriften anzuzeigen (Kennzeichnungspflicht). Der Hinweis ist deutlich sichtbar anzubringen, er muss vor Betreten des überwachten Bereichs problemlos wahrnehmbar sein, damit die freie Entscheidung für oder gegen das Betreten möglich ist. Der Kennzeichnung muss ebenfalls **Name und Kontaktdaten der verantwortlichen Stelle** zu entnehmen sein.

Zu kennzeichnen sind insbesondere die Eingangsbereiche, auch beim Einsatz von **Kamera-Dummys**. Die Betroffenen müssen die Kennzeichnung frühzeitig erkennen können. Dementsprechend ist auch eine angemessene Größe zu beachten.

7.4 Protokollierungs- und Löschungspflicht

Genaue Speicherfristen wurden im BDSGneu nicht festgelegt. In § 4 Abs. 5 BDSGneu definiert der Gesetzgeber die Löschung so, dass die Daten unverzüglich zu löschen sind, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Die Datenschutz-Aufsichtsbehörden geben hier als Handlungsempfehlung, aufgenommene Daten binnen **72 Stunden** zu löschen. Ausgenommen davon sind Daten welche ggf. für Schutz- oder Beweissicherungszwecke länger benötigt werden. Bei Anfrage seitens der Polizei sind diese zu sichern, eine Herausgabe kann i.d.R. nur auf Grundlage einer richterlichen Anordnung erfolgen.

Ein jeder Verwendungsvorgang/Zugriff auf Videoaufzeichnungen ist lückenlos zu dokumentieren.

7.5 Auskunftsrecht

Betroffene haben das Recht, die Übermittlung einer Kopie der von ihnen gefertigten Aufnahmen anzufordern. Des Weiteren kann der Betroffene auch die Einsichtnahme auf die Lesegeräte des Hotels verlangen. Zuzüglich zu diesem, sind dem Betroffenen auch folgende Informationen wie die Herkunft, der Empfänger bzw. die Empfängerkreise von Übermittlungen, der Zweck und die Rechtsgrundlage sowie ggf. die Beauftragung eines Dienstleisters schriftlich zukommen zu lassen. Es steht dem Betroffenen frei, einer mündlichen Auskunftserklärung zuzustimmen.

Sollte eine Übermittlung der Daten auf Grund von überwiegender, berechtigter Interessen Dritter – wie z.B. aufgenommene Gäste oder Mitarbeiter des Hotels, nicht möglich sein, so ist das vom Betroffenen erfasste Verhalten schriftlich zu beschreiben. Es kann auch die Überwachung mit unkenntlich gemachten Personen übermittelt werden.

Es besteht seitens des Betroffenen die Pflicht, das Heraussuchen der Daten zu erleichtern, einen möglichst genauen Zeitraum und den Ort der Überwachung ist dem Hotelier mitzuteilen.

7.6 Zufällige Aufzeichnungen von strafbaren Handlungen

Sollten bei Aufnahmen zufällig Ereignisse aufgenommen werden, die nicht zum Zweck bzw. der Zulässigkeit der Videoüberwachung erfasst sind, so handelt es sich um einen Zufallstreffer. Sollte es sich dabei um gerichtlich strafbare Handlungen handeln, so können diese Daten an die zuständige Behörde oder das Gericht auf Grundlage einer richterlichen Anordnung übermittelt werden.

- ❖ Bei der Anfertigung von Videoaufnahmen handelt es sich um eine Erhebung, eine Speicherung und ggf. auch um eine Verarbeitung personenbezogener Bilddaten, die unter das Datenschutzrecht fallen.
- ❖ Es herrscht Kennzeichnungs-, Protokollierungs- und Löschungspflicht.

- ✓ Verfüge ich über eine Videoüberwachung? Wenn ja, erfülle ich alle gesetzlichen Anforderungen?
- ✓ Bei Implementierung, Prüfung an Hand der Checkliste zur Videoüberwachung. Datenschutz-Folgenabschätzung.
- ✓ Kennzeichnung der überwachten Bereiche.
- ✓ Erstellung von Vorlagen zur Protokollierung und Einführung von Standards zum Umgang mit der Videoüberwachungsanlage.

8 Datenschutz und Sicherheit - Regelungen im Hotel

Zielfragen

- Was ist zu regeln?
- Wer ist verantwortlich?
- Wie werden die Regeln überprüft?

Die DSGVO sieht vor, dass die technischen und organisatorischen Maßnahmen zu Datenschutz und Datensicherheit dokumentiert werden. Vergleiche hierzu auch Pkt. 1.3.

8.1 Angemessene Sicherheitsmaßnahmen

Als Verantwortlicher hat der Hotelier unter Beachtung des Verhältnismäßigkeitsgrundsatzes geeignete technische und organisatorische Maßnahmen zu treffen um sicherzustellen, dass die Verarbeitungen rechtmäßig verlaufen. Er hat solche Verarbeitungstechniken zu wählen, die den Datenschutzgrundsätzen der Datenminimierung und den Grundsätzen des Datenschutzes durch Technikgestaltung (data protection by desgin) oder durch datenschutzfreundliche Voreinstellungen (data protection by default) Rechnung tragen (Art. 25 DSGVO, Erwägungsgrund 78). Es sind interne Strategien und Regelungen festzulegen und Maßnahmen zu ergreifen. Kosten und Aufwand müssen im angemessenen Verhältnis zum Schutzziel stehen, das dem Risiko der Betroffenen gegenübersteht. Der Schutzbedarf bestimmt den Umfang der Sicherheitsmaßnahmen.

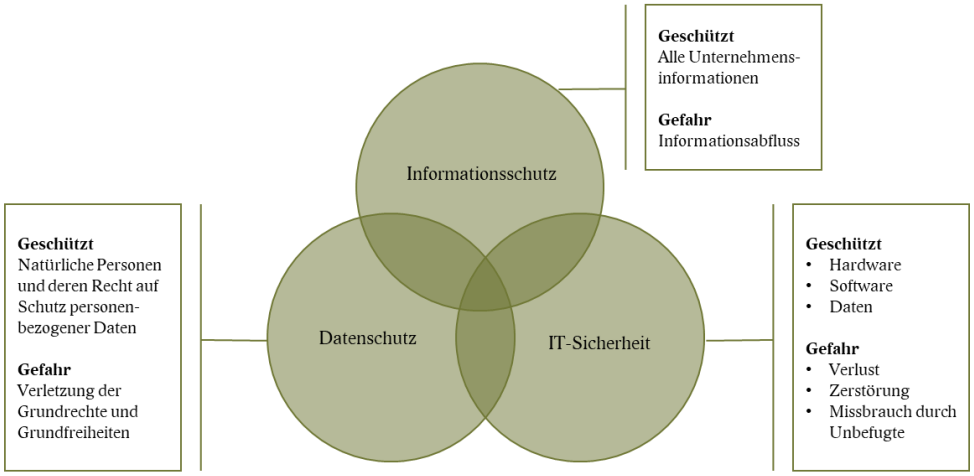

Abbildung 8 | Datenschutz & Datensicherheit

Quelle | in Anlehnung an DATAKONTEX GmbH

8.2 Datenschutzrichtlinien

Datenschutzrichtlinien folgen in der Regel den Dokumentenstrukturen aus dem Managementhandbuch (z.B. Qualitätsmanagement) und regeln mit den mitgeltenden Unterlagen die rechtlichen und die grundsätzlichen technischen und organisatorischen Maßnahmen zum Datenschutz. Sollte bei Ihnen kein Managementhandbuch implementiert sein, können Sie aus der im **Anhang** angeführten **Struktur einer Datenschutzrichtlinie** mögliche Inhalte entnehmen. Die Regeln zum Datenschutz sollten regelmäßig in einem internen Datenschutzaudit auf Einhaltung und Aktualität geprüft werden.

Weil ein wirksamer Datenschutz nicht alleine durch Regelungen und Bestimmungen erreicht werden kann, sondern von einem ausgeprägten Datenschutz- und Sicherheitsbewusstsein der Mitarbeiterinnen und Mitarbeiter getragen wird, sind diese zum Thema Datenschutz mittels der internen Regelungen zu sensibilisieren. Ziel sollte es sein, ihnen Informationen und Regelungen an die Hand zu geben, die es ermöglichen, die mit dem Betrieb komplexer und offener Datenverarbeitungs- und Kommunikationssysteme verbundenen Risiken zu erkennen und damit umzugehen.

Auf der Grundlage der Bewertung der datenschutzrechtlichen und betriebswirtschaftlichen Sensibilität der Daten und der anschließenden Einstufung in Schutz- und Vertraulichkeitsstufen sind die erforderlichen technischen und organisatorischen Maßnahmen zu definieren und zu beschreiben. So können ergänzende Richtlinie erlassen werden, insbesondere zu Verfahren, bei denen die Persönlichkeitsrechte von Betroffenen eingeschränkt werden können. Hierzu zählen auch Verfahren, die eine Leistungs- und Verhaltenskontrolle von Mitarbeitern bzw. das Profiling von Kunden zulassen.

Zusätzliche Richtlinien können sein:

- Nutzung von E-Mail und Internetdiensten im Hotel
- Nutzung von Telefondiensten
- Einsatz von Videoüberwachungssystemen
- Einsatz von Zeiterfassungssystemen
- Einsatz von elektronischen Türschließsystemen
- Sales & Marketing

Für Revisoren, Auditoren und auch für die Datenschutz-Aufsichtsbehörde besteht durch das Richtlinienwerk eine fundierte und schlüssige Möglichkeit, die Vollständigkeit, Notwendigkeit und Angemessenheit der technischen und organisatorischen Maßnahmen zu beurteilen.

8.3 IT-Sicherheitsrichtlinien

Die Datenverarbeitungssysteme einschließlich der gesamten IT-Infrastruktur (Server, Netzwerke, Arbeitsplatz-PCs etc.) und der Datenbestände zählen zur unternehmenskritischen Infrastruktur. Der Schutz dieser unternehmenskritischen IT-Infrastruktur und der Datenbestände gegen Bedrohungen aller Art, z.B. durch Schadsoftware wie Computerviren, Trojaner etc., Spionage, Missbrauch und Fehlbedienung, ist für jedes Unternehmen von großer Bedeutung. Es ist deshalb von großer Wichtigkeit, den sicheren und sachgemäßen Umgang mit allen

Arten von Informationstechnologie zu regeln und damit das Hotel vor Schaden zu schützen. Eine IT-Sicherheitsrichtlinie trägt dazu bei, den erforderlichen Schutz zu gewährleisten und den Aufwand für den Schutz der Grundkriterien „Verfügbarkeit, Vertraulichkeit, Authentizität, Revisionsfähigkeit und Integrität“ zu optimieren.

Zur Bestimmung der Sicherheitsmaßnahmen nach Art. 32 sind nach DSGVO folgende Schritte erforderlich:

1. Schutzbedarf feststellen
2. Risiken bewerten
3. Im Hinblick auf die Risiken sind verhältnismäßige Maßnahmen zu ergreifen
4. Nachweise sind zu erbringen

Damit unterstellt die DSGVO im Grundsatz, dass im Unternehmen ein IT-Sicherheitsmanagement umgesetzt wird. Maßnahmen sind in Regelungen zu beschreiben, denn ohne Regelung, die durch die Geschäftsleitung unterstützt wird, gibt es keine definierten Umsetzungsanforderungen für die IT und Mitarbeiter.

Sollten bei Ihnen im Hotel kein IT-Sicherheitsmanagement implementiert sein, können Sie aus der im **Anhang** aufgeführten **Struktur einer IT-Sicherheitsrichtlinie** mögliche Inhalte entnehmen. Die Regeln zur Datensicherheit sollten regelmäßig in einem internen IT-Sicherheitsaudit auf Einhaltung und Aktualität geprüft werden.

8.4 Phasen der Implementierung

Eine Implementierung von einer IT- und Datenschutzrichtlinie ist nur dann sinnvoll, wenn diese auf Ihr Hotel mit der Infrastruktur und der Arbeitsplatzumgebung abgestimmt ist und alle wichtigen Teilbereiche enthält. Die Phasen sind dabei wie folgt zu gestalten:

Abbildung 9 | Phasen der Implementierung einer IT und Datenschutz Policy

Quelle | in Anlehnung an R. Knyrim/ M. Oman, IT und Datenschutz-Policies in der Praxis

- ❖ Eine IT- und Datenschutzrichtlinie klärt in Ihrem Hotel datenschutzrechtliche Sicherheitsaspekte und ist, mit Wirkung der Datenschutzgrundverordnung, verpflichtend.
- ❖ Die Regeln zu Datenschutz und Datensicherheit sollten regelmäßig in einem internen Audit auf Einhaltung und Aktualität geprüft werden.

- ✓ Ist eine Datenschutzrichtlinie vorhanden? Wenn nein, Implementierung dieser.
- ✓ Ist ein IT-Sicherheitsmanagement vorhanden? Wenn nein, Implementierung dieses.
- ✓ Verantwortliche bestimmen, Datenschutzbeauftragten und ggf. IT-Sicherheitsbeauftragten berufen.
- ✓ Bildung eines Datenschutz-Teams (Datenschutzbeauftragter, IT-Leiter, HR, FO, Sales & Marketing, Vertreter der Hotelleitung, ggf. QM)
- ✓ Schulung der Mitarbeiter zu Inhalten der Richtlinien.

9 Anhang

Muster | Verzeichnis von Verarbeitungstätigkeiten

Checkliste | Prüfung der Inhalte der Datenschutzerklärung

Checkliste | Datenverarbeitung im Auftrag (mgl. Dienstleister)

Checkliste | Einsatz und Nutzung von Videokontrollsystemen

Muster | Inhalt einer Datenschutzrichtlinie

Muster | Inhalt einer IT-Sicherheitsrichtlinie

Abkürzungsverzeichnis

Abbildungsverzeichnis

Muster
Verzeichnis von Verarbeitungstätigkeiten

Hauptblatt

Angaben zum Verantwortlichen (Art. 30 Abs. 1 lit. a DSGVO)

1. Verantwortlicher (= Hotel/Abteilung) *[Name/Ladungsfähige Anschrift]*

2. Gesetzlicher Vertreter (= Geschäftsführung) *[Name/Kontaktdaten]*

3. Vertreter in der EU (gemäß Art. 27 DSGVO) [Name / Ladungsfähige Anschrift]

4. Datenschutzbeauftragter *[Name/Kontaktdaten]*

5. Regelungen zur Datensicherheit *[Verweis auf übergreifende IT-Sicherheitskonzepte, die grundsätzlich für alle Verarbeitungstätigkeiten gelten]*

6. Regelungen zur Datenlöschung *[Verweis auf übergreifende Löschkonzepte, die grundsätzlich für alle Verarbeitungstätigkeiten gelten]*

7. Sachverhalte zu Drittstaatenübermittlungen *[Verweis auf übergreifende Punkte wie Binding Corporate Rules, die grundsätzlich für alle Verarbeitungstätigkeiten gelten]*

Erläuterungen

Nr. 1	Verantwortlicher ist jede Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DSGVO) Angaben: Name/Firma, ladungsfähige Anschrift
Nr. 2	Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter Angaben: Namen der geschäftsführenden Personen
Nr. 3	Bei Unternehmen ohne Niederlassung in der Europäischen Union ist hier der benannte Vertreter des Verantwortlichen (Art. 4 Nr. 17 DSGVO, Art. 27 Abs. 1 DSGVO) anzugeben.
Nr. 4	Vom Verantwortlichen bestellter Datenschutzbeauftragter [Name, Kontaktdaten]
Nr. 5	Gegebenenfalls Verweise auf übergreifende Regelungen (*falls solche existieren, die grundsätzlich alle Verarbeitungen* betreffen) – Der Verweis an dieser Stelle auf übergreifende Regelungen entbindet nicht von der Dokumentation von ggf. erforderlichen Abweichungen zu den einzelnen Verarbeitungstätigkeiten. Verweis z.B. auf ein IT-Sicherheitskonzept, das alle Verarbeitungstätigkeiten einschließt. Eventuell auch Verweise auf relevante Dokumente eines ISMS nach ISO 27001.
Nr. 6	Verweis auf Löschkonzepte, die grundsätzlich für alle Verarbeitungen gelten.
Nr. 7	Ein Verweis Regelungen zur Drittstaatenübermittlung sind hier sinnvoll, wenn alle oder die Mehrzahl der Verarbeitungen hierdurch geregelt werden, z.B. durch Binding Corporate Rules.

Verzeichnis von Verarbeitungstätigkeiten

Anlage Nr. _____

Angaben zur Verarbeitungstätigkeit und zur Verantwortlichkeit (Art. 30 Abs. 1 lit. b DSGVO)

1. Bezeichnung der Verarbeitungstätigkeit 2. Verantwortlicher Fachbereich/verantwortliche Führungskraft (optionaler Inhalt) 3. Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen

Angaben zur Verarbeitungstätigkeit

4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit

5. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit

6. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DSGVO)	
6.1 Betroffene Personengruppen	6.2 Kategorien personenbezogener Daten

7. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden (Art. 30 Abs. 1 lit. d DS-GVO)

   [interne, externe – auch im Konzern, eingebundene Dienstleister]

8. Datenübermittlungen in Drittländer oder internationale Organisationen (Art. 30 Abs. 1 e DSGVO)

   Übermittlung

   ☐ Ja

   ☐ Nein

   Name des Drittlandes / der internationalen Organisation (DSGVO)

   --- Optionale Angaben ---

   Ggf. vereinbarte Garantien

   ☐ Anerkannter Drittstaat

   ☐ EU-Standardvertragsklausel

   ☐ Aufsichtsbehördlich genehmigter Vertrag

   ☐ Binding Corporate Rules (BCR)

   ☐ Andere:

   --- Ende optionale Angaben ---

   Garantien zum Schutz der personenbezogenen Daten im Drittland, soweit weder eine Anerkennung des Datenschutzniveaus, EU-Standardverträge noch BCR vorliegen:

9. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 lit. f DSGVO)

10. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DSGVO)
10.1 Art der eingesetzten DV-Anlagen und Software (optional) - DV-Anlagen - Software (und ggf. Unterprogramme) - Schnittstellen
10.2 Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DSGVO) - [Bezug zum IT-Sicherheitskonzept, Abweichungen bzw. Ergänzungen] *oder: Verweis auf Datenschutz-Zertifizierung etc.*

----- *Optionale Angaben* ----

Weitere Dokumentationen zur Verarbeitungstätigkeit

z. B.: - *zu Informationspflichten* - *zu Verträgen mit Dienstleistern* - *zu Vereinbarungen zur gemeinsamen Verantwortung* - *zu durchgeführten Datenschutzfolgeabschätzungen zur Verarbeitungstätigkeit oder einzelnen Verarbeitungsschritten*

----- *Ende Optionale Angaben*----

Erläuterungen

Nr. 1	Eindeutige Bezeichnung der dokumentierten Verarbeitung/der Verarbeitungstätigkeit auf Grundlage eines Fachprozesses. Es sollte eine im Unternehmen geläufige Bezeichnung des Fachprozesses gewählt werden. Beispiele: - Kundenverwaltung (Hotelmanagementsystem, PMS) - Reservierungssystem (Online-Reservierung) - Mitarbeiterverwaltung (Personalverwaltungssystem, Zeiterfassungssystem, Lohnabrechnung, ...) - Customer-Relationship-Management (CRM) - Newsletterservice
Nr. 2	Nach der Unternehmensorganisation für die konkrete Verarbeitungstätigkeit verantwortlicher Fachbereich/verantwortliche Führungskraft (*sofern möglich und sinnvoll, zumindest als Funktionsbezeichnung*)
Nr. 3	Falls mehrere Verantwortliche gemeinsam für die Verarbeitungstätigkeiten verantwortlich sind, bspw. innerhalb einer Unternehmensgruppe, sind hier Name und Kontaktdaten des/der weiteren Verantwortlichen anzugeben (Firma/ladungsfähige Anschrift; Art. 30 Abs. 1 Lit. a DSGVO, Art. 26 Abs. 1 DSGVO)
Nr. 4	Beispiele: - Verarbeitungstätigkeit: „Kundenverwaltung“; verfolgte Zweckbestimmungen: „Auftragsbearbeitung, Buchhaltung und Inkasso“ - Verarbeitungstätigkeit: „Customer-Relationship-Management“; verfolgte Zweckbestimmungen: „Dokumentation und Verwaltung von Kundenbeziehungen, Marketing, Neukundenakquise, Kundenbindungsmaßnahmen, Kundenberatung, Beschwerdemanagement, Kündigungsprozess“ Eine Verarbeitungstätigkeit (aus der Anwendung des BDSG als „Verfahren“ vertraut) kann mehrere Teil-Geschäftsprozesse zusammenfassen. Dementsprechend kann eine Verarbeitung auch mehrere Zwecke umfassen, sodass auch mehrere Zweckbestimmungen angegeben werden können. Die erforderliche Detailtiefe hängt von der Geschäftstätigkeit des Verantwortlichen ab. Es können neben dem Fachprozess auch begleitende mitarbeiterbezogene Unterstützungsprozesse vorliegen wie z.B. zur Personalführung/ Einsatzplanung. Diese können entweder als Teil einer anderen Verarbeitung, oder als eigene Verarbeitung beschrieben sein.

Nr. 5	Die Nennung der einschlägigen Rechtsgrundlage ist für Dokumentationspflichten und die Gewährleistung von Transparenzpflichten ggü. betroffenen Personen notwendig.
Nr. 6	Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DSGVO)
Nr. 6.1	Als betroffene Personengruppen kommen beispielsweise Kunden, Interessenten, Arbeitnehmer, Schuldner, Versicherungsnehmer usw. in Betracht.
Nr. 6.2	Den einzelnen Personengruppen sind die jeweils auf sie bezogenen verwendeten Daten oder Datenkategorien zuzuordnen. Damit sind keine personenbezogenen Daten, sondern "Datenbezeichnungen"/ Datenkategorien gemeint (z.B. „Adresse“, „Geburtsdatum“, „Bankverbindung“). Werden solche Datenkategorien angegeben, so müssen diese so konkret wie möglich sein. Nicht ausreichend, da zu allgemein, sind etwa Angaben wie „Kundendaten“ oder ähnliches. Beispiele: - Kunden: Adressdaten, Kontaktkoordinaten (einschl. Telefon-, Fax-und E-Mail-Daten), Geburtsdatum, Vertragsdaten, Bonitätsdaten, Betreuungsinformationen einschließl. Kundenentwicklung, Produkt- bzw. Vertragsinteresse, Statistikdaten, Abrechnungs- und Leistungsdaten, Bankverbindung - Beschäftigtendaten (Lohn und Gehalt): Kontaktdaten, Bankverbindung, Sozialversicherungsdaten, etc.
Nr. 7	Empfängerkategorien sind insbesondere am Prozess beteiligte weitere Stellen des Unternehmens/Konzerns oder andere Gruppen von Personen oder Stellen, die Daten – ggf. über Schnittstellen – erhalten z.B. in den Prozess eingebundene weitere Fachabteilungen, Vertragspartner, Kunden, Behörden, Versicherungen, Auftragsverarbeiter (z.B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter, Anwendungsentwicklung, Cloud Service Provider) usw.
Nr. 8	Drittländer sind solche außerhalb der EU/des EWR Beispiele für internationale Organisationen: Institutionen der UNO, der EU Geeignete Garantien beim Empfänger sind grundsätzlich erforderlich, falls für den Drittstaat kein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO vorliegt. Solche Garantien können gem. Art. 46 DSGVO durch verbindliche interne Datenschutzvorschriften (BCR) oder EU-Standardverträge erbracht werden. Liegt keine der genannten Garantien vor, sind hier andere getroffene Garantien zu dokumentieren (Art. 49 Abs. 1. UAbs. 2 DSGVO).

Nr. 9	Anzugeben sind hier die konkreten Aufbewahrungs-/Löschfristen, die in Verarbeitungstätigkeiten implementiert sind, bezogen auf einzelne Verarbeitungsschritte, falls unterschiedlich. Soweit diese in einem Löschkonzept dokumentiert sind, reicht der konkrete Verweis auf das vorhandene und in der Verarbeitungstätigkeit umgesetzte Löschkonzept aus.
Nr. 10	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DSGVO)
Nr. 10.1	Optional kann an dieser Stelle eine knappe Beschreibung der technischen Infrastruktur wie der technischen und organisatorischen Sicherheitsmaßnahmen angegeben werden, um ein besseres Verständnis der allgemeinen Beschreibung der technischen und organisatorischen Maßnahmen (siehe 10.2.) zu ermöglichen.
Nr. 10.2	Soweit sich die technischen und organisatorischen Maßnahmen schon aus vorhandenen Sicherheitsrichtlinien/Konzepten/Zertifizierungen ergeben, ist ein konkreter Verweis hierauf ausreichend. Insbesondere sind hier Abweichungen zu einem übergreifenden Sicherheitskonzept (**siehe Hauptblatt Nr. 6**) zu dokumentieren. Wenn eine Datenschutz-Folgenabschätzung für die Verarbeitung hohe Risiken ausweist, so sind die zur Bewältigung dieser Risiken getroffenen Sicherheitsvorkehrungen für die Verarbeitung in der Datenschutz-Folgenabschätzung zu dokumentieren. (Art. 35 Abs. 7 lit. d DSGVO). Ein Verweis auf das Vorhandensein einer Datenschutz-Folgenabschätzung ist eine sinnvolle optionale Angabe (siehe unten).
Optional	Im Hinblick auf die vielfältigen Nachweispflichten, denen das Unternehmen im Datenschutz unterliegt, kann es sinnvoll sein, weitere Aspekte zur Verarbeitungstätigkeit zu dokumentieren. Diese sind nur intern zu verwenden. Zu diesen zusätzlichen Dokumentationen, die sinnvollerweise hier erfolgen, gehören z. B. • *Angaben zur Zusammenstellung der Informationspflichten (insbes. Artt. 13,14 DSGVO)* • *Verträge mit Dienstleistern (Art. 28 DSGVO)* • *Vereinbarungen zur gemeinsamen Verantwortung (Art. 26 DSGVO)* • *Eine Bewertung der Risiken der Verarbeitungstätigkeit für die Rechte und Freiheiten natürlicher Personen* • *durchgeführte Datenschutz-Folgenabschätzungen zur Verarbeitungstätigkeit oder einzelnen Verarbeitungsschritten (Art. 35 DSGVO)*

Checkliste
Prüfung der Inhalte der Datenschutzerklärung

Diese Checkliste unterstützt Sie bei der Erstellung der Datenschutzerklärung. Sie erhebt keinen Anspruch auf Richtigkeit, Vollständigkeit und Beständigkeit. Ziehen Sie zur Erstellung Ihren IT Fachmann sowie Ihren Anwalt zu Rate.

Allgemeine Angaben

1. Wer betreibt die Internetseite?

   Name und Kontaktdaten des Verantwortlichen, ggf. Datenschutzbeauftragten

Erhebung und Verarbeitung personenbezogener Daten

2. Werden personenbezogene Daten über die Webseite erhoben und verarbeitet?

   Erläutern Sie in diesem Zusammenhang die Kategorien der zu erhebenden Daten (Vor- und Nachname, Adress- und Kontaktdaten, Zahlungsdaten, Buchungsdaten)

3. Erheben Sie oder Ihr Webspace Provider Zugriffs- und Protokolldaten?

   Wenn ja, so ist anzuführen, wer und welche Daten erhoben werden und was mit den Daten geschieht.

4. Bieten Sie Kontaktmöglichkeiten an (z.B. Kontaktanfrage, Blog)?

   Wenn ja, dann ist anzuführen, welche Daten genutzt werden, was mit den Daten geschieht (Zweck, Rechtsgrundlage, Löschfrist). Es ist zusätzlich darauf zu verweisen, dass für die Bearbeitung der Anfrage die Daten gespeichert werden.

5. Bieten Sie die Möglichkeit, über ein Online-Reservierungssystem zu buchen?

   Wenn ja, dann ist anzuführen, welche Daten genutzt werden, was mit den Daten geschieht (Zweck, Rechtsgrundlage, Löschfrist). Sollte der Service über einen Drittanbieter angeboten werden, so ist dieser ebenfalls anzuführen.

6. Bieten Sie die Möglichkeit, einen Newsletter zu abonnieren an?

   Wenn ja, dann ist anzuführen, welche Daten erhoben werden, was mit den Daten geschieht (Zweck) und dem Hinweis auf Widerruf bei Einwilligung. Sollte der Service über einen Drittanbieter angeboten werden, so ist dieser ebenfalls anzuführen.

7. Möchten Sie die E-Mail-Adresse zur Kontaktaufnahme für eine Online-Bewertung nutzen?

   Wenn ja, dann ist anzuführen, welche Daten genutzt werden, was mit den Daten geschieht (Zweck, ggf. Zweckerweiterung wie anonymisierte Auswertung, Rechtsgrundlage, Löschfrist) und dem Hinweis auf Widerruf. Sollte der Service über einen Drittanbieter angeboten werden, so ist dieser ebenfalls anzuführen.

8. Bieten Sie den Nutzern Ihrer Webseite ein Gutscheinsystem an?

   Wenn ja, dann ist anzuführen, welche Daten genutzt werden, was mit den Daten geschieht (Zweck, Rechtsgrundlage, Löschfrist). Sollte der Service über einen Drittanbieter angeboten werden, so ist dieser ebenfalls anzuführen.

9. ... weitere Systeme, in denen personenbezogene Daten über die Webseite erhoben werden, sind zu berücksichtigen

10. Bieten Sie eine Registrierfunktion an (z.B. für Stammgäste)?

    Wenn ja, führen Sie an, was der Zweck der Registrierung ist. Welche Daten aufgenommen werden und was genau mit diesen Daten geschieht.

11. Bieten Sie ein Bewerberportal an?

    Wenn ja, dann ist anzuführen, welche Daten genutzt werden, was mit den Daten geschieht (Zweck, Rechtsgrundlage, Löschfrist). Sollte der Service über einen Drittanbieter angeboten werden, so ist dieser ebenfalls anzuführen.

Weitergabe von personenbezogene Daten an Dritte

12. Beabsichtigen Sie, Gastdaten innerhalb eines Unternehmensverbundes weiterzugeben?

    Wenn ja, dann ist anzuführen, welche Daten die verbundenen Hotels sehen und nutzen können und die Tatsache, dass Gästewünsche jeglicher Art gespeichert werden, um die Wünsche des Gastes zu erfüllen. Der Nutzer ist über den Zweck, die Rechtsgrundlage und sein Widerspruchsrecht gegen die Datenoffenbarung zu informieren.

13. Beabsichtigen Sie, Gastdaten an ein Franchise-Unternehmen weiterzugeben?

    Wenn ja, dann ist anzuführen, welche Daten dem Franchiser übermittelt werden. Der Nutzer ist über den Zweck, die Rechtsgrundlage und sein Widerspruchsrecht gegen die Datenübermittlung zu informieren.

14. Beauftragen Sie Dritte um Dienstleistungen für den Gast zu erfüllen? (z.B. Buchung von Stadtrundfahrten, Abholung vom Flughafen)

    Wenn ja, informieren Sie den Nutzer, dass Sie Daten nur dann an Dritte weitergegeben werden, sofern dies zur Erbringung von Dienstleistungen erforderlich ist, und dass die Partner die Daten lediglich für die Erfüllung des Auftrages nutzen.

15. Beabsichtigen Sie, personenbezogene Daten an weitere Dritte weiterzugeben?

    Wenn ja, dann ist anzuführen, welche Daten an welchen Dritten (z.B. Bonusprogramm, Tischreservierung, ...) übermittelt werden. Der Nutzer ist über den Zweck, die Rechtsgrundlage und sein Widerspruchsrecht gegen die Datenübermittlung zu informieren.

Instrumente zur Webseitenoptimierung und Analyse des Nutzungsverhaltens

16. Binden Sie fremde Inhalte wie z.B. Google Maps, RSS Feeds oder Grafiken auf Ihrer Webseite ein?

    Wenn ja, Hinweis darauf, dass diese die IP Adresse des Nutzers speichern. Dass kein Einfluss darauf besteht, ob diese Drittanbieter die IP Adresse z.B. für statistische Zwecke speichern, dass jedoch falls dies bekannt ist der Nutzer darauf hingewiesen wird.

17. Speichern Sie Cookies auf den Rechnern der Nutzer?

    Wenn ja erklären Sie was Cookies sind. Führen Sie an, welche Cookies sie nutzen und wozu diese dienen (z.B. Wiedererkennung, Werbung, Tracking, Systemoptimierung) bzw. was sie machen. Erklären Sie dem Nutzer wie diese zu deaktivieren sind.

18. Verwenden Sie Google Analytics oder andere Analyse- und Trackingtools?

    Wenn ja, so sind diese entsprechend anzuführen. Hierzu finden Sie standardisierte Texte im Internet.

19. Haben Sie Social Plugins (z.B. Facebook) integriert?

    Wenn ja, so ist eine Formulierung betreffend der Datenverarbeitung in Bezug auf das Plugin anzuführen (Funktion, was macht es und wozu ist es vorhanden).

Rechte der Betroffenen

20. Informieren Sie den Nutzer der Webseite, welche Rechte er bezüglich der Verarbeitung seiner Daten wie wahrnehmen kann.

    - *Auskunft*
    - *Löschung*
    - *Berichtigung*
    - *Widerspruch*

21. Informieren Sie den Nutzer der Webseite über sein Beschwerderecht bei einer Aufsichtsbehörde.

Datensicherheit

22. Informieren Sie den Nutzer der Webseite über getroffene technische und organisatorische Sicherheitsvorkehrungen.

    - *Verschlüsselung*
    - *Zusammenarbeit mit Zahlungsdienstleistern*
    - *Datenschutzvereinbarungen mit Dienstleistern*

Checkliste
Datenverarbeitung im Auftrag (mgl. Dienstleister)

- ☐ Hotelsoftware (Fernwartung, Hosting) .....
- ☐ CRM (Fernwartung, Hosting) .....
- ☐ Personalverwaltung/Lohnbuchhaltung.....
- ☐ IT-Support.....
- ☐ Telekommunikations-Anlage.....
- ☐ Online-Buchungssystem (Reservierung, Tisch, etc.) .....
- ☐ Webseitenbetreuung/Hosting.....
- ☐ Newsletterservice.....
- ☐ Online-Bewertung .....
- ☐ Cloud-Dienste (z.B. Office 365) .....
- ☐ onlinebasierte Zeiterfassung .....
- ☐ Call-Center .....
- ☐ Systemwartung (Video, Türschließsystem, ...) .....
- ☐ Datensicherung.....
- ☐ externer Nachtdienst.....
- ☐ Consulting.....
- ☐ Archivierung.....
- ☐ Aktenvernichtung.....
- ☐ Mail/Spamdienst.....
- ☐ Pre-Stay E-Mail .....
- ☐ Tracking Webseite (z.B. Google Analytics) .....
- ☐ ....

Checkliste
Einsatz und Nutzung von Videokontrollsystemen

23. Welche **Räumlichkeiten/Objekte** sollen videoüberwacht werden?

▪

24. Was ist der Zweck der Datenspeicherung?

▪

25. Wie erfolgt die Speicherung der Daten?

☐ analog ☐ digital

26. Werden die gespeicherten Daten **verschlüsselt**?

☐ ja ☐ nein

Bemerkungen:

27. Werden auch **Tondaten** erfasst?

☐ ja ☐ nein

Bemerkungen:

28. Wie lang ist der **Aufzeichnungszeitraum bzw. die Speicherfrist**?

_____

29. In welchen Zeiträumen wird videoüberwacht?

☐ rund um die Uhr ☐ Bewegungsmelder ☐ vorgegebene Zeiten _____

☐ außerhalb der Geschäftszeiten ☐ nur nachts

30. Wo befindet sich der **Server** mit den Aufzeichnungen?

_____

31. Wer hat das Recht, auf die Aufzeichnungen **zuzugreifen**?

_____

32. Wie ist der **Zugriff** geregelt?

☐ Benutzer ☐ Passwort ☐ keine Zugriffsregelung

Bemerkungen:

33. Werden **Mitarbeiterdaten** erfasst?

☐ ja ☐ nein

☐ regelmäßig ☐ unregelmäßig

Bemerkungen:

34. Sind die Kamerapositionen **schwenkbar**?

☐ ja ☐ nein

Bemerkungen:

35. Hat es an den zu überwachenden Orten schon einmal Fälle einer **besonderen Gefährdung** gegeben (Diebstahl, Einbrüche, Überfall, Vandalismus)?

☐ ja ☐ nein

Bemerkungen:

36. Welche Maßnahmen wurden bzw. werden bereits zur Gefahrenabwehr ergriffen?

☐ Einsatz von Sicherheitspersonal ☐ Alarmanlage

☐ Zugangskontrollsystem ☐ Echtzeitkamera

Bemerkungen:

Anlage: Übersichtsplan + Screenshots bzw. vorab Fotos vom Ausschnitt der Aufzeichnung + Fotos der installierten Kameras

.....

Ort, Datum

.....

Unterschrift, Stempel

Muster zum Inhalt einer Datenschutzrichtlinie

Muster zum Inhalt einer IT-Sicherheitsrichtlinie

Präambel

1 Regelungsgegenstand

2 Allgemeine Regelungen

2.1 Zuständigkeit und Verantwortung

2.1.1 IT-Sicherheitsbeauftragter

2.1.2 IT-Support

2.1.3 Administratoren

2.1.4 Benutzer

2.2 Anwendungsbereich und Grundlagen für den Umgang mit IT-Systemen

2.2.1 Anwendungsbereich

2.2.2 Zweckbindung der Systeme und Arbeitsmittel

2.2.3 Tele- und Heimarbeitsplätze

2.2.4 Einsatz und Freigabe von Datenverarbeitungsverfahren

2.2.4.1 Sachlogische Prüfung

2.2.4.2 Technische Testung

2.2.4.3 Einrichtung der Verfahren

2.2.4.4 Datenübernahme

2.2.4.5 Freigabe zur Anwendung

2.2.4.6 Aufbewahrung der Testergebnisse und der Dokumentationen

2.2.5 Verwaltung und Administration der Datenverarbeitungsverfahren

2.2.5.1 Verwaltung der Datenverarbeitungsverfahren

2.2.5.2 Administrationsrechte

2.2.5.3 Nachweis der Programmidentität

2.2.5.4 Überwachung von Schnittstellen und Zugängen

Ihr Weg zur Implementierung der DSGVO

Quelle: In Anlehnung an R. Knyrim, Auswirkungen der EU-Datenschutz-Grundverordnung und wie Sie sich am besten darauf vorbereiten

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
AGG	Allgemeines Gleichbehandlungsgesetz
BCR	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
BDSGneu	Neues Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BMG	Bundesmeldegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BYOD	Bring Your Own Device
CRM	Customer-Relationship-Management
DSB	Datenschutzbeauftragter
DSGVO	Datenschutz-Grundverordnung
DSMS	Datenschutzmanagementsystem
EU	Europäische Union
FO	Front Office
GoBS	Grundsätzen ordnungsgemäßer DV-gestützter Buchführungssysteme
HR	Human Resource
ISMS	Information Security Management System
IT	Informationstechnik
LAN	Local Area Network
OS	Online-Streitbeilegung
PC	Personal Computer
PCI DSS	Payment Card Industry Data Security Standard
PMS	Property Management System
PR	Public Relation
QM	Qualitätsmanagement
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
VVT	Verzeichnis von Verarbeitungstätigkeiten
WLAN	Wireless Local Area Network

Abbildungsverzeichnis