Leitfaden

Datenschutz in der Hotellerie

Ihr Partner im Datenschutz

Herausgeber

DataSolution LUD GmbH
Isarstr. 13
D-14974 Ludwigsfelde

Ansprechpartner

Andreas Thurmann
T: +49 (0) 3378.202513
M: mail@ds-lud.de.de
W: www.datenschutzberater365.de

Titelbild

#50802651 – Fotolia
#67174943 – Fotolia

Copyright

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, zumeist 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.

Der Leitfaden soll Sie dabei unterstützen, die Ihnen bevorstehenden Aufgaben zum Datenschutz, aber auch zur Datensicherheit, zu meistern. Im ersten Teil möchten wir den theoretischen Teil zum Datenschutz betrachten, um danach branchenspezifische Anforderungen zu beschreiben.

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

Seit 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 **BDSG** genannt). Jedoch sind auch für die elektronische Kommunikation das **Telekommunikationsgesetz** (in weiterer Folge TKG), das **Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz** (in weiterer Folge TDDDG) 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 (z.B. in Hotelsoftware) sowie für die nichtautomatisierte Verarbeitung (Reservierungsordner, Ordner mit Zahlungsbelegen) personenbezogener Daten. Personenbezogene Daten sind alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person (auch betroffene Person/ Betroffener genannt) 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 (Software, Datenbank aber auch Papier) ausgeführte Tätigkeit im Zusammenhang mit **personenbezogenen Daten** wie das

- Erheben
- Erfassen
- Organisation
- Ordnen
- Speichern
- Anpassen oder Verändern
- Auslesen
- Abfragen
- Verwenden/Nutzen
- Weitergeben durch Übermittlung
- Abgleichen oder Verknüpfen
- Einschränken oder Löschen/Vernichten

von personenbezogenen Daten.

Räumlich gilt die DSGVO in der Europäischen Union, unabhängig davon, ob die Verarbeitung innerhalb oder außerhalb der EU stattfindet. Die DSGVO schützt die Daten von EU-Bürgern.

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 = Es muss einen Grund zur Datenverarbeitung geben!**

  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).

- **Datenminimierung = Nur so viel wie erforderlich!**

  Die Erhebung von personenbezogenen 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 = Aufbewahrungsfristen - Daten sind nach einer bestimmten Zeit zu löschen!**

  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 = Sicherheit in der Datenverarbeitung**

  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 zunächst 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 vorhanden ist, 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 sicherzustellen sind. Nachfolgende Grafik veranschaulicht die Anforderungen.

Bedingungen der Einwilligung (Art. 7 DSGVO)

1.4 Datenschutzorganisation

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.

Datenschutz-Management System nach DSGVO

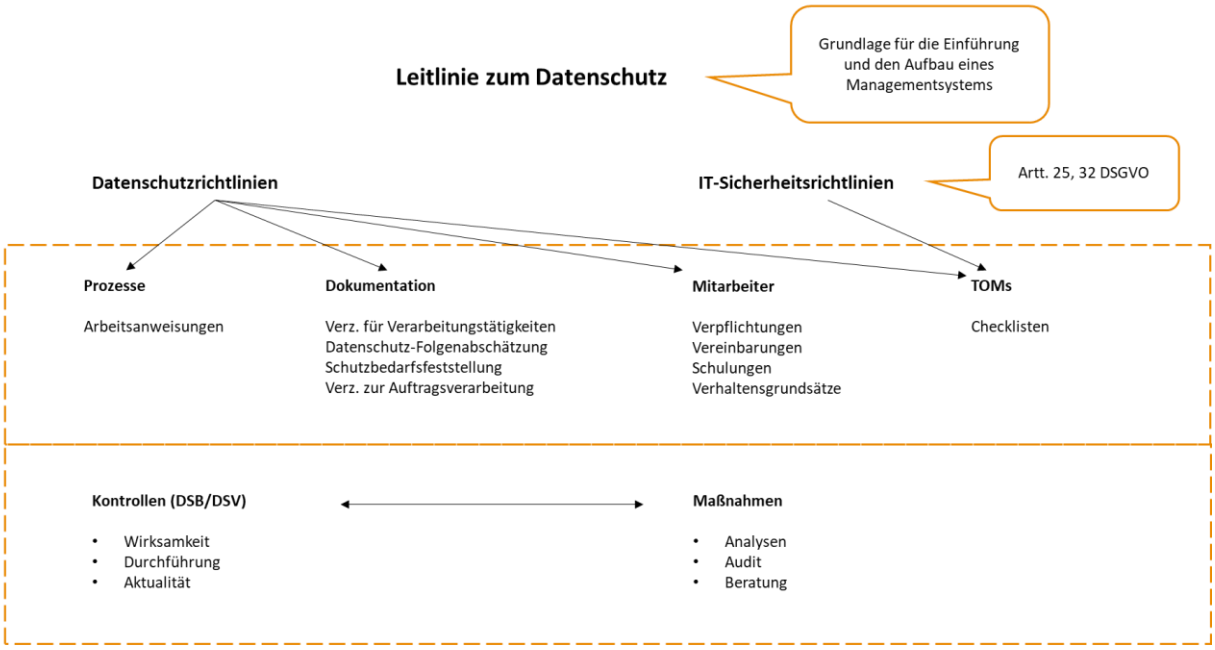

Abbildung 2 | Schematische Darstellung eines Datenschutz-Management-Systems

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.

Es 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 genutzter oder zu kaufender Software, Speicherort, …)
  - Durchführung von Kontrollen
    (Ist-Analyse, Audit, Maßnahmenplan)
- **Datenschutzrechtliche Dokumentationspflichten, wie:**
  - Verpflichtung Mitarbeiter auf das **Datengeheimnis** bzw. auf die **Vertraulichkeit**
  - Sensibilisierung und Schulung von **Mitarbeitern**
  - **Datenschutzrichtlinien** (interne Regelungen mit Weisungscharakter für Mitarbeiter im Hotel, wie Datenschutz und Datensicherheit im Unternehmen integriert und aufgebaut ist.)

- Prozesse zur Wahrung der **Betroffenenrechte (insbesondere Auskunft und Löschung)** und zum **Datenpannenmanagement**
- Führen des **Verzeichnisses von Verarbeitungstätigkeiten (VVT)** inkl. Zweckbestimmung, Grundlage der Verarbeitung und Durchführung einer Risikobewertung
- Durchzuführende **Schutzbedarfsfeststellung, Transfer Impact Assessment (TIA)** und **Datenschutz-Folgenabschätzungen** für die einzelnen Datenverarbeitungsverfahren
- Verpflichtung von Dienstleistern im Rahmen der **Datenverarbeitung im Auftrag** (Outsourcing, wie Hosting und/oder (Fern-)Wartung von Software (PMS), Lohnbuchhaltung, Onlinebuchungssystem auf der Webseite, IT-Support, …)
- Beschreibung von **technischen und organisatorischen Maßnahmen (TOM)** (z.B. innerbetriebliche Anweisungen und Prozessabläufe, Datensicherheitsmaßnahmen wie Verschlüsselung und Passwortmanagement)
- nachweisliche **Überprüfung von Datenschutzmaßnahmen** (Datenschutzaudits)

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.

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

So ist der Schutzbedarf bei der Speicherung von Bank- und Kreditkartendaten (PCI DSS Normen) wesentlich höher anzusetzen als beim Speichern von Angebotsanfragen. 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** für die Betroffenen und dem Unternehmen.
- Festlegung geeigneter **technischer und organisatorischer 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).

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

Als im Detail geregelte Dokumentationspflicht zu nennen ist unter anderem das

- **Verzeichnis von Verarbeitungstätigkeiten**
- **Verzeichnis für Auftragsverarbeitung** (Übersicht zu den Auftragnehmern bzw. Auftraggebern im Rahmen einer Datenverarbeitung im Auftrag)

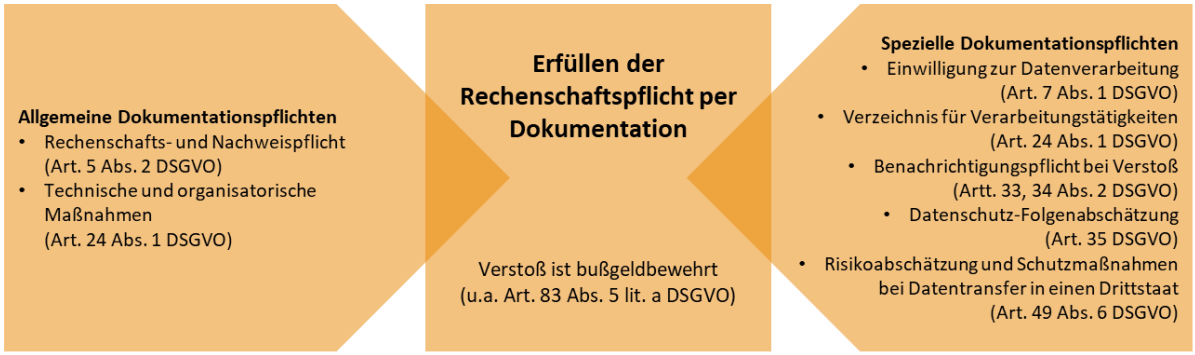

Abbildung 3 | Dokumentationspflichten

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 (z.B. Hosting oder Softwareanbieter aus den USA), 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 Transparenzregelungen** gegenüber den Betroffenen.

Als Hotelier müssen Sie jederzeit in der Lage sein, die Rechtmäßigkeit der 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.

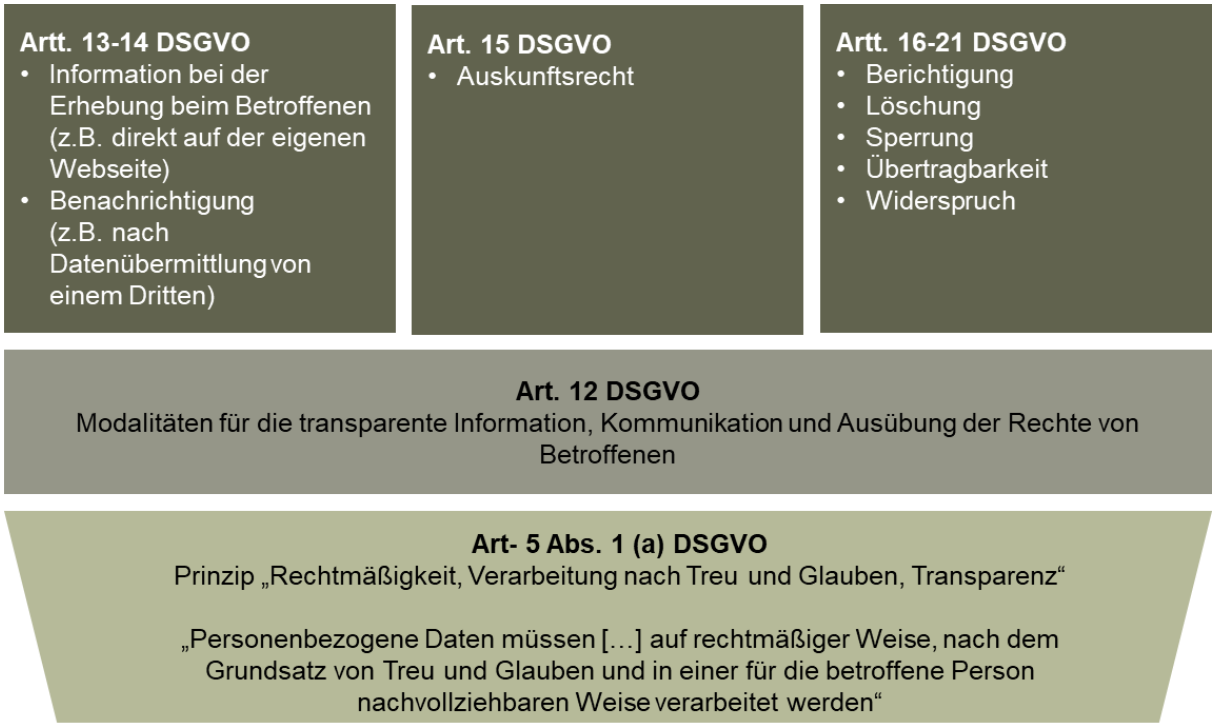

Abbildung 4 | Transparente Verarbeitung

Die DSGVO enthält umfangreichere und detailliertere **Regelungen zu Informationspflichten** als zuvor, 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 bei der erstmaligen Datenerhebung. 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).

Von sich aus tätig werden muss der Hotelier gegenüber den Betroffenen 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).

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.

Allgemeine Informationspflichten

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

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

Sollten Adress- und/oder Kontaktdaten nicht bekannt sein, weil bspw. ein Gast über ein OTA gebucht hat, so kann diesem am Tag der Anreise ein Informationsschreiben zur Datenverarbeitung an der Rezeption angeboten werden (Aufsteller, Aushang oder Bereitstellung eines Ausdrucks).

Es empfiehlt sich zudem in jeder E-Mail-Signatur (ausgehende E-Mail) einen Satz zum vertraulichen Umgang mit personenbezogenen Daten hinzuzufügen. Ein Medienbruch ist möglich, also die Verlinkung auf die Datenschutzerklärung der eigenen Webseite. Diese sollte dann aber mehr Verarbeitungsvorgänge beschreiben, also nur bei der Datenverarbeitung über die Webseite erforderlich, z.B. Stellenausschreibungen.

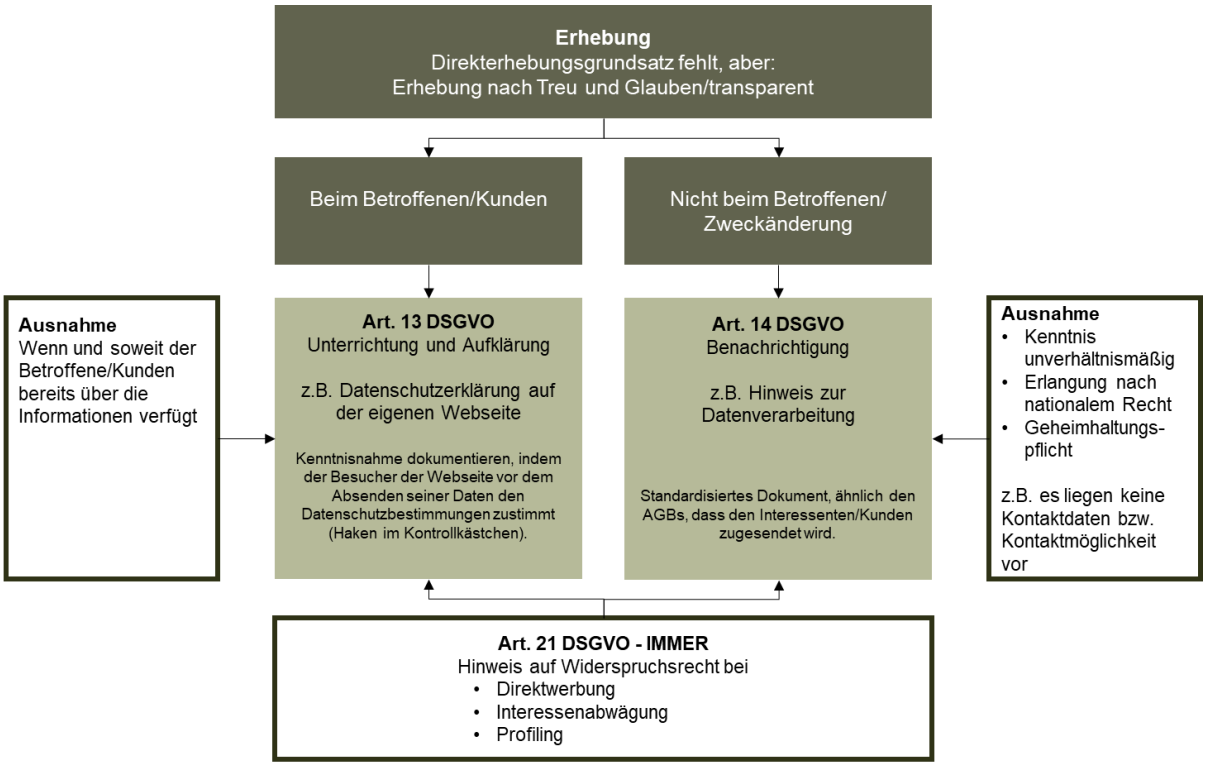

Abbildung 5 | Information bei der Erhebung von personenbezogenen Daten

Werden die Daten zur 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.

Informationspflichten bei Datenschutzpanne

Verletzungen des Schutzes personenbezogener Daten (z.B. Hackerangriff, Datenverlust oder Datendiebstahl, 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.

Als Hotelier müssen Sie eine Risikobewertung anhand der Eintrittswahrscheinlichkeit des Eintretens für Einschränkungen der Persönlichkeitsrechte und den Schaden für den Betroffenen nachweislich durchführen.

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**.

Als Hotelier müssen Sie zusätzlich **allen weiteren Empfängern der Daten** jeden Antrag auf Berichtigung, Löschung oder Einschränkung der Verarbeitung **mitteilen** (Art. 19 DSGVO).

Zur Wahrnehmung seiner Rechte kann sich jede Person an eine beliebige Stelle im Hotel wenden und um Auskunft oder die Löschung 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/Arbeitsanweisungen, 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.

Nehmen Sie jede Anfrage, die sich auf das Datenschutzgesetz oder die DSGVO bezieht, ernst. Bei Nichtbearbeitung der Anfrage kann sich der Betroffene an die zuständige Aufsichtsbehörde für Datenschutz wenden und sich beschweren. In diesem Fall müssen Sie gut begründen können, warum die Anfrage nicht beantwortet wurde.

Jede Person, die ihre Betroffenenrechte wahrnimmt, hat sich im Vorfeld zu identifizieren (Art. 12 Abs. 6 DSGVO). Dafür hat der Anfragende im Zweifel (z.B. bei einer telefonischen Anfrage oder über eine Fantasie-Mail-Adresse) seine Identität mit z.B. einer Ausweiskopie zu bestätigen, wenn er nicht über seine genutzte E-Mail-Adresse identifiziert werden kann.

Eine Ausweiskopie/Foto vom Ausweis darf zur Identifikation nur in begründeten Ausnahmen verlangt werden und ist durch den Anfragenden durch ein sicheres Datenverarbeitungsverfahren (z.B. verschlüsselte Bereitstellung in einer Privat Cloud) bereitzustellen, sofern nicht der Postweg gewünscht wird. Nach der Identifikation ist die Kopie unverzüglich zu löschen bzw. zu vernichten.

Definieren Sie intern Prozesse und Verantwortliche zur Bearbeitung der Anfragen, es empfiehlt sich eine Zentralisierung der Bearbeitung.

Auskunftsrecht

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, anderenfalls ist eine Negativauskunft zu geben.

Auf Verlangen des Betroffenen (Gast, Newsletterempfänger, …) 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 auf umfangreiche 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 | Recht auf Auskunft (Art. 15 DSGVO)

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.

Der Anfragende hat eine Mitwirkungspflicht, wenn die auskunftserteilende Stelle darum ersucht. Damit soll vermieden werden, dass ein unverhältnismäßiger, finanzieller als auch zeitlicher Aufwand entsteht.

Es empfiehlt sich, dem Anfragenden eine Eingangsbestätigung zuzuschicken. Handelt es sich um komplexere Begehren kann diese Frist um zwei weitere Monate verlängert werden. Darüber ist der Betroffene zu informieren.

Dokumentieren Sie jede Auskunftsanfrage für 3 Jahre. Danach ist sie zu löschen.

Richtigstellung und Löschung

Hotels sind verpflichtet, nur korrekte Daten über den Gast zu speichern. Der Gast oder eine andere Person (Mitarbeiter) hat jederzeit das Recht, die Berichtigung sowie im Hinblick auf den Zweck die Vervollständigung seiner 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.

Prüfen Sie, ob die vom Hotel genutzten Softwareanwendungen, insbesondere das:

- PMS und Onlinereservierungssystem
- Tischreservierungs- und/oder Gutscheinbestellsystem
- Recruiting-System
- Personalverwaltungssystem (auch ePersonalakte) oder
- elektronische Zeiterfassungssystem

in den Admin-Einstellungen die Möglichkeit anbieten, dass nach einer festzulegenden Frist die Daten gelöscht bzw. anonymisiert werden können. Nehmen Sie hier die entsprechenden Einstellungen vor!

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.

Der Hotelier ist nicht verpflichtet, im Internetauftritt das Bild eines Beschäftigten automatisch zu löschen, wenn dieser auf einem Gruppenbild abgebildet ist. Allerdings muss er auf Antrag des Beschäftigten das Bild von der Webseite herunternehmen oder den Beschäftigten unkenntlich machen.

Es kommt regelmäßig vor, dass der Name eines (ehemaligen) Beschäftigten im Zusammenhang mit dem Hotel „gegoogelt“ werden kann. Auch hier ist zunächst der Hotelier dafür verantwortlich, dass der Suchlink bei Google entfernt wird, wenn dieses der Antragsteller verlangt. In der Praxis ist das allerdings schwierig, da Google nur persönliche Löschanträge bearbeitet. Verweigert also Google die Löschung, so ist der Antragsteller darüber zu informieren. Ihm sind die weiteren Optionen zur Löschung zu benennen.

Der Verantwortliche muss 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 gelten die oben genannten Fristen, in der die Bearbeitung und Antwort an den Betroffenen zu erfolgen hat.

Bei der Veröffentlichung von Informationen zu Personen auf der Webseite oder in den Sozialen Medien sollte stets darauf geachtet werden, dass die Rechte, insbesondere das Recht am eigenen Bild, beachtet werden! Eine Veröffentlichung, unabhängig ob es sich um die eigenen Mitarbeiter oder andere Personen handelt, ist nur mit einer formgerechten Einwilligung zulässig.

Einschränkung der Verarbeitung (Sperrung)

Jede 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 (Gastkarte im PMS auf inaktiv setzen) 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.

Heben Sie als Verantwortliche die Einschränkung auf, haben Sie den Betroffenen im Vorfeld zu informieren. Die Frist entspricht der Fristsetzung der anderen Betroffenenrechte.

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 Antragstellers 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 Daten dazu verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten. Insbesondere handelt es sich hier um eine Analyse bezüglich persönlicher Leistungen, der wirtschaftlichen 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 eine Person der Nutzung oder Übermittlung ihrer Daten z.B. für Zwecke der Werbung, hat das Hotel durch geeignete organisatorische bzw. technische Maßnahmen sicherzustellen, dass ihrem Recht entsprochen wird. Neben den datenschutzrechtlichen Sanktionen kann der Antragsteller zivilrechtlich gegen die Nichtbeachtung des Widerspruchs vorgehen.

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

Nehmen Sie jeden Werbewiderspruch ernst und verzichten Sie auf weitere Kontakte. Im besten Fall erhalten Sie eine anwaltliche Unterlassungserklärung (ca. 800 EURO pro Fall), wenn es schlecht läuft, dann verhängt die Aufsichtsbehörde für Datenschutz ein Bußgeld, welches schnell auf einen 5 – 6-stelligen Betrag verhängt wird. Diesen Ärger kann man sich ersparen.

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.

Das Kontrollsystem

Der **Betroffene** in seiner Eigenschaft als Bürger, Arbeitnehmer, Kunde (Gast), Internetnutzer usw. soll in die Lage versetzt werden, seine Daten selbst zu kontrollieren. Man spricht hier auch von der **informationellen Selbstbestimmung**. Dabei hat er bereits bei der Erhebung seiner Daten oder – soweit die Daten nicht bei ihm erhoben wurden – durch Benachrichtigung durch den Verantwortlichen umfangreiche Kenntnis zur Datenverarbeitung zu erhalten, insbesondere über Art der verarbeiteten Daten, die Zwecke der Verarbeitung und seine Rechte.

Wurde der Betroffene bereits zu einem früheren Zeitpunkt über die Verarbeitung seiner Daten informiert, so muss dieser nicht im wiederholten Fall neu informiert werden. Wurden Daten zu einer Person bereits vor dem 25.05.2018 (DSGVO tritt in Kraft) gespeichert, entfällt auch hier die Informationspflicht /Stichtagsregelung in der DSGVO).

Sind die Daten zu beanstanden, so hat der Betroffene, wie bereits beschrieben, 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.

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. Wenn kein Datenschutzbeauftragter bestellt werden muss, in Deutschland ist das beispielsweise der Fall, wenn weniger als 20 Beschäftigte (inkl. Geschäftsleitung bzw. Inhaber) mit der regelmäßigen Verarbeitung von personenbezogenen Daten beschäftigt sind, dann ist für die Umsetzung der datenschutzrechtlichen Anforderungen die Geschäftsleitung bzw. Hotelleitung verantwortlich. In dieser Funktion kann sie auch einen **Datenschutzverantwortlichen** benennen.

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**, sofern einer gewählt wurde, 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.

Der Datenschutzbeauftragte

Unternehmen haben nach § 38 BDSG einen betrieblichen Datenschutzbeauftragten (DSB) zu bestellen, wenn **20 Mitarbeiter und mehr** personenbezogene Daten erheben, speichern, nutzen, verarbeiten und/oder löschen.

Zu beachten ist, dass die Mitarbeiterzahl im Hotel, aber auch in einer Pension oder in einem Restaurant im Hinblick auf die Bestellpflicht dann irrelevant ist, wenn dort Datenschutz-Folgenabschätzungen vorgenommen werden muss. In diesem Fall besteht die Pflicht zur Bestellung eines DSB unabhängig von der Anzahl der Beschäftigten. Datenschutz-Folgenabschätzungen sind beispielsweise dann durchzuführen, wenn eine systematische Videoüberwachung erfolgt oder wenn Daten besonderer Kategorien wie Gesundheitsdaten umfangreich verarbeitet werden.

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 (Datenschutz-Management-System),

die für die Umsetzung von datenschutzrechtlichen, 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. Er wird 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 bringen kann.

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.

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, insbesondere zum Verzeichnis für Verarbeitungstätigkeiten 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**. 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 BDSG) gegenüber.

Seitdem die DSGVO in Kraft getreten ist, haben die Aufsichtsbehörden zahlreiche Bußgelder, teilweise in Millionenhöhe verhängt. Grundlage der Bußgelder waren oftmals Verstöße gegen die Grundsätze zum Datenschutz (Art. 5 DSGVO), Missachtung von Betroffenenrechten (Artt. 12 ff. DSGVO) und unzureichend umgesetzte technische und organisatorische Maßnahmen.

Als Hotelier sollte es Ihr Ziel sein, dass keine Person sich bei der Aufsichtsbehörde beschwert. Oftmals reicht es schon aus, dass man sich persönlich um die Probleme kümmert, insbesondere die Wahrnehmung von Betroffenenrechte sollten auch entsprechend gewürdigt werden. Anderenfalls kann es teuer werden.

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

2 Umgang mit Gastdaten

Als Hotelier dürfen Sie nur jene Daten Ihrer Gäste speichern und verwenden, die Sie für die Erfüllung des Beherbergungsvertrags benötigen. Auch die Datenspeicherung und -verarbeitung im Rahmen einer Reservierung ist ohne Einwilligung zulässig. Es 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 Anforderungen an die Hotelsoftware

Die zentrale Speicherung und Verwaltung von Gastdaten erfolgt in der Regel 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. Welche Funktionalitäten und gesetzliche Anforderungen Sie auf jeden Fall prüfen sollten, werden nachfolgend beschrieben:

1. 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? Kleine Hotels oder Pensionen haben andere Anforderungen als Häuser mit 50 oder mehr Zimmern. Während kleine Häuser eher ein schlankes, **webbasiertes Hotelverwaltungssystem** einsetzen, arbeiten größere Hotels und Hotelketten mit einem **Property Management System (PMS)**. Hier kann sich das System in einem Rechenzentrum einer Hotelgruppe bzw. im Serverraum des Hotels befinden oder bei einem Dienstleister gehostet sein.

   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.

Mit dem EuGH Urteil aus 2020 zur Datenübermittlung in ein unsicheres Drittland (Schrems II) muss für Datenverarbeiter wie z.B. Amazon AWS oder Oracle mit Rechenzentren in Europa sichergestellt werden, dass ein Zugriff auf die gehosteten Daten durch Behörden unterbunden wird. Die Daten sollten verschlüsselt werden, entweder auf Server- oder Datenbankebene. Gleiches gilt für personenbezogene Daten, die direkt in einem unsicheren Drittland gespeichert werden.

Bei der Bewertung des Systemanbieters sind ebenso auch die Subunternehmen zu betrachten. Eine Prüfung der Datenverarbeitung schließt diese mit ein, der Systemanbieter muss darlegen, warum er nicht auf ein anderes System innerhalb der EU zurückgreift bzw. wie die Datenverarbeitung abgesichert wird. Das Vorhandensein von Vereinbarungen bzw. Standarddatenschutzklauseln wird nicht ausreichen, Papier ist geduldig!

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 eigenen Datenschutzvereinbarung. Sollten er Ihnen keine bereitstellen können, sind das schon die ersten Hinweise darauf, dass der Datenschutz bei ihm keinen hohen Stellenwert hat. Andererseits ist der Auftragsverarbeiter auch nicht verpflichtet, 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. Es empfiehlt sich, den Zugriff auf Gastdaten spätestens ein Monat nach Abreise (es gibt keine Forderungen mehr seitens des Hotels) für die meisten Benutzer des Hotelmanagement Systems zu entziehen, also automatisiert zu sperren. Zulässig wäre der Zugriff durch die Reservierung sowie Sales und Marketing.

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.

In einer Hotelsoftware lässt sich das schwer darstellen, da bei wiederholten Besuchen 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 nach 10 Jahren zu löschen.

4. Insbesondere **Hotelketten** setzen ein PMS mit dem Ziel ein, auf eine **gemeinsame Datenquelle** zuzugreifen. So sollen mehrere Hotels die Möglichkeit erhalten, auf bereits gespeicherte Gastdaten aus einem 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, ein sogenanntes Joint Controller Agreement, 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.

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

2.2 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, achten Sie auf die Grundeinstellungen.

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 bei der erstmaligen Speicherung 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). **Elektronische Reservierungsordner**, also die Ablage von Reservierungsunterlagen auf einem Fileserver, sind genauso zu behandeln, wie die Papierakte. Die Daten dürfen dem Front Office erst zum Anreisetag zur Verfügung gestellt werden und sollten spätestens nach 14 Tagen archiviert werden, also in ein Verzeichnis kopiert werden, wo der Zugriff stark eingeschränkt ist.

2.3 Check-In

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.

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

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 prüfen Sie, ob eventuell eine Einwilligung durch den Betroffenen benötigt wird. 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!

Im Herbst 2019 wurde das Bürokratieentlastungsgesetz (BEG) III verabschiedet. Ein Punkt des BEG III war die Digitalisierung des Meldescheins, welches eine große Erleichterung im Umgang mit dem Meldeschein in den Beherbergungsstätten bringen sollte. Neben dem traditionellen Papier-Meldeschein besteht seit 2020 die Möglichkeit, Ihren Gästen diesen komplett elektronisch anzubieten. Allerdings ist es hier mit einer einfachen Unterschrift z.B. auf dem Tablet leider nicht getan.

Die erhobenen Daten können nur dann ausschließlich elektronisch gespeichert werden, wenn…

1. … „durch die beherbergte Person zugleich ein kartengebundener Zahlungsvorgang mit einer starken Kundenauthentifizierung ausgelöst wird“ (§29 Abs. 5 Pkt. 1 BMG), wie beispielsweise durch eine Zahlung mit Kreditkarte. Dabei müssen drei Punkte erfüllt werden:
   - Zahlungsdienstleister müssen neben dem bisherigen Impuls „Zahlung erfolgreich“ auch einen „SCA durchgeführt“ (ausgeschrieben: Strong Customer Authentication = starke Kundenauthentifizierung) zur Verfügung stellen.
   - Das Property Management System (PMS) der Unterkunft und der Zahlungsanbieter müssen über eine Schnittstelle miteinander kommunizieren.
   - Das PMS muss die „zweckgebundene Zuordnungsnummer für wiederkehrende Zahlungen“ (den sogenannten Token, also eine bestimmte Folge verschlüsselter Zeichen, die der Identifikation von Benutzern dienen) zwölf Monate abrufbar halten und zwingend im PMS speichern.

Problem:

- Bei Kostenübernahmen durch Firmen, Vereine etc. kommt diese Variante in der Regel nicht in Frage, da die Kreditkarten auf einen anderen Namen laufen. Weiterhin ist dieses Verfahren bei vielen ausländischen Kreditkarten nicht möglich (fehlende 2-Faktor-Authentifizierung) sowie bei Barzahlern.
- Es ist eine Schnittstelle zwischen PMS und elektronischem Zahlungssystem erforderlich.

2. … oder die Identifikation des Gastes mittels eines elektronischen Identitätsnachweises (elektronische Funktion des Personalausweises (eID-Funktion) erfolgt.

- Hierfür ist ein entsprechendes Lesegerät erforderlich, welches nur die gem. § 30 Abs. 2 BMG erforderlichen Daten ausliest und speichert.
- Der Gast muss einen PIN eingeben, damit die Daten ausgelesen werden können oder persönlich den Personalausweis zum Einlesen übergeben.

Problem:

- Es wird ein entsprechendes Lesegerät benötigt, ein Scan des Ausweises ist unzulässig.
- Der Gast muss die online-Ausweisfunktion freigeschaltet und einen PIN bereit haben.
- Die Nutzung der eID-Funktion des Ausweises ist noch nicht sehr verbreitet.
- Für deutsche Gäste ist es bisher nicht erforderlich einen Ausweis im Hotel vorzuzeigen.

Im Herbst 2024 wurde das Bürokratieentlastungsgesetz (BEG) IV verabschiedet. Ein Punkt des BEG IV war der Wegfall des Meldescheines für deutsche Staatsbürger zum 01.01.2025. Für Bürger ohne deutsche Staasbürgerschaft bleibt alles wie gehabt.

Vorteil:

- Deutsche Staatsbürger müssen ab 01.01.2025 keinen Meldeschein mehr ausfüllen und handschriftlich unterschreiben. Auch die Authentifizierung über Kreditkarte oder ePersonalausweis entfällt.
- Der Online Check-In wird sich für deutsche Staatsbürger einfacher gestalten, da die Authentifizierung wegfällt. Somit gibt es keine Hürden mehr wie z.B. die Angabe der Kreditkartennummer beim Check-In.
- Es müssen wesentlich weniger Meldescheine erstellt und aufbewahrt werden.

Nachteil:

- Es muss eine Trennung zwischen inländische und ausländische Gäste vorgenommen werden. Diese ist i.d.R. nicht so leicht vorzunehmen, wenn keine weiteren Daten vom Gast vorliegen als Name und Reservierungsdaten.
- Bisher war neben Art. 6 Abs. 1 lit. b DSGVO (Vertragsverhältnis) das Bundesmeldegesetz die Rechtsgrundlage, um Adress- und Kontaktdaten vom Gast zu erhalten. Es müssen andere Wege gefunden werden, um an die Daten der Gäste zu kommen. Es wird wohl kein Hotelier darauf verzichten wollen, seinen Gast zu kennen. Für Betrug und Hausfriedensbruch ständen ansonsten alle Tore offen.

Die Digitalisierung des Meldescheins für ausländische Gäste hat hohe Hürden und jede Beherbergungsstätte muss abwägen, ob die Umstellung mit derzeitiger Gesetzeslage von Vorteil ist. Achten Sie darauf, dass das System die genannten Anforderungen zum Identitätsnachweis erfüllt. Eine elektronische Unterschrift sieht das Bundesmeldegesetz nicht vor. Zudem ist das Hochladen von Personalausweisen bei ausländischen Gästen sehr kritisch zu hinterfragen. I.d.R. fehlt hierzu die Rechtsgrundlage. Eine Einwilligung wird nicht ausreichen. Beachten Sie die Verhältnismäßigkeit!

Legen Sie letztendlich ein Augenmerk auf die Speicherung und Löschung der elektronischen Meldescheine, insbesondere bei Übermittlung via E-Mail. Ein unbefugter Zugriff ist zu verhindern, die gespeicherten Daten sind nach 1 Jahr zu löschen. Mit dem Systemanbieter ist ein sogenannter Auftragsverarbeitungsvertrag (AVV) nach den Vorgaben von Art. 28 DSGVO abzuschließen.

Auch wenn es bereits Systemanbieter gibt, die das Ausfüllen eines elektronischen Meldescheins über eine App möglich machen und der Gast „theoretisch“ ohne an die Rezeption zu gehen einchecken kann, und sein Zimmer über das Smartphone öffnen kann, so bleibt bei ausländischen Gästen immer noch die Verpflichtung, die Meldedaten mit einem Personaldokument abzugleichen.

Denken Sie stets daran, über den Meldeschein auch über die Datenverarbeitung zu informieren.

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 Bundesdatenschutzgesetz (BDSG). 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 auf dem Händler- und Kundenbeleg.

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.

Das Erstellen einer Kopie eines Personaldokumentes bedarf einer formgerechten Einwilligung gemäß Artt. 6 lit. a, 7 DSGVO i.V.m. § 20 Abs. 2 PAuswG. Dabei ist aber zu prüfen, ob es überhaupt erforderlich ist, auch mit Einwilligung des Gastes eine Kopie zu erstellen. Der Abgleich von Personaldokumenten mit dem Meldeschein sollte in den meisten Fällen ausreichen, das Interesse der verantwortlichen Stelle steht dem Persönlichkeitsrecht entgegen.

2.4 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 BMG haben alle Personen am Tag der Ankunft einen besonderen Meldeschein handschriftlich zu unterschreiben. Fehlende Pflichtangaben sind zu ergänzen.
2. Abweichend von § 29 Abs. 2 Satz 1 BMG kann die Meldepflicht auf Grundlage von § 29 Abs. 5 BMG mit Zustimmung der beherbergten Person auch dadurch erfüllt werden, dass die in § 30 Abs. 2 BMG genannten Daten elektronisch erhoben werden und die beherbergte Person deren Richtigkeit und Vollständigkeit am Tag der Ankunft durch ein starkes Authentifizierungsverfahren bestätigt.
3. Mitreisende Angehörige sind nur der Zahl nach anzugeben.
4. 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.
5. Folgende Daten sind Pflichtangaben:
   a. Datum der Ankunft und der voraussichtlichen Abreise
   b. Familienname
   c. Vornamen

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.

d. Geburtsdatum

e. Staatsangehörigkeiten

f. Anschrift

g. Zahl der Mitreisenden und ihre Staatsangehörigkeit (bei Reisegruppen)

h. Seriennummer des anerkannten, gültigen Passes bei ausländischen Gästen

6. 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.
7. Durch Landes- und Kommunalrecht kann bestimmt werden, welche zusätzlichen Daten bzgl. Fremdenverkehrs- und Kurbeiträgen notwendig sind.
8. Die Meldescheine sind vom Tag der Anreise 1 Jahr aufzubewahren und innerhalb von 3 Monaten nach Ablauf der Aufbewahrungsfrist zu vernichten.
9. Die Meldescheine sind so aufzubewahren, dass kein Unbefugter Einsicht nehmen kann. Elektronische Meldescheine sind verschlüsselt zu speichern, die Zugriffsrechte sind stark einzuschränken.
10. 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.

2.5 Kreditkartendaten

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.

Es gibt eine 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.

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)
- ausgedruckte Kreditkartendaten immer unter Verschluss aufbewahrt werden. (Rechnungen, Archiv, Reservierungsunterlagen, …)

2.6 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“)

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. Des Weiteren empfehlen wir, dass in der Datenschutzerklärung auf der Webseite und 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 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) zu beachten. Insbesondere sind die Pflicht zur Wahrung des **Fernmeldegeheimnisses** (§ 3 TDDDG) zu beachten.

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. Zu beachten ist § 4 BDSG.

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.

2.7 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. Hier bietet sich ein Opt-out auf dem Meldeschein an. Der Gast erhält die Möglichkeit, der Nutzung der E-Mail-Adresse zum Zusenden einer Bewertungs-Mail zu widersprechen.

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 können sensible Daten wie Kreditkartennummern abgelegt sein. 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.

3 Mitarbeiterdaten

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 BDSG 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 BDSG 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

Im Rahmen der 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 Fristen nach den individuellen Verhältnissen festzulegen sind. Zweckmäßig ist es, die Personalakte bei Ausscheiden eines Mitarbeiters auszudünnen und nicht mehr erforderliche Unterlagen zu vernichten.

Grundsatz der Erforderlichkeit

Beschäftigtendaten dürfen erhoben, gespeichert, verarbeitet und genutzt werden, wenn dies erforderlich ist. Der Begriff der Erforderlichkeit ist ein unbestimmter Rechtsbegriff und bedarf deshalb immer der näheren Betrachtung und Interpretation. Grundsätzlich dürfen nicht mehr Daten erhoben, gespeichert und verarbeitet werden, als zur Erfüllung der jeweiligen Aufgabe benötigt werden.

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

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 bzw. die Personalsachbearbeiter nach eigenem Ermessen.

Informationspflichten bei der Datenerhebung

Mit der Datenerhebung und -speicherung ist der Mitarbeiter gemäß Artt. 13, 14 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 oder Hotelgruppe 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 Gruppenverbund 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 gruppenübergreifende 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.

3.1 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 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 hochgeladen 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.

Gemäß dem Allgemeinen Gleichbehandlungsgesetz (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.

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.

Um im Falle einer Klage den Entlastungsbeweis führen zu können, empfiehlt es sich deshalb, zumindest die entscheidungserheblichen Auszüge aus der Bewerbung innerhalb einer Stellenausschreibung, die Kriterien für das Auswahlverfahren und die Entscheidungsgründe über **die Bewerbung für einen angemessenen Zeitraum (6 Monate) 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.

Anders wäre es, wenn der Bewerber erklärt hat, mit einer längeren Speicherung einverstanden zu sein, bis für ihn eine geeignete Stelle gefunden wurde.

Eine Weiterleitung von Bewerbungen (z.B. innerhalb von gruppenangehörigen Unternehmen) an eine Schwestergesellschaft oder an die Muttergesellschaft ist ebenfalls 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.

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."

Ansonsten wird je nach Speicherungsform seine Bewerbung nach Ablauf der nach dem AGG angemessenen Frist gelöscht, vernichtet oder zurückgegeben. Zu berücksichtigen ist auch, ob die Bewerbungsunterlagen an Personen außerhalb des Personalbüros, bspw. Abteilungsleiter, weitergeleitet wurden. Gerade bei der Weiterleitung von E-Mails sind auch diese zu löschen. Belehren Sie diesbezüglich die Empfänger und stellen Sie klare Regelungen auf.

Auch Bewerber sind über die Verarbeitung ihrer Daten zu informieren. Da die Bewerber i.d.R. den ersten Schritt machen und ihre Bewerbung in den meisten Fällen per Mail zusenden, bietet es sich an, die Hinweise in die Datenschutzerklärung auf der Webseite zu hinterlegen. Mit jeder Stellenausschreibung und Antwort-Mail von der Personalabteilung kann dem Bewerber ein Hinweis zur Datenverarbeitung mit Link auf die Datenschutzerklärung angeboten werden. Sollte auf der Webseite ein Formular hinterlegt sein, so ist durch den Bewerber vor dem Versenden bzw. Hochladen seiner Daten die Kenntnisnahme der Datenschutzbestimmungen zu bestätigen.

Auch für „Online" Recruiting-Tools gelten die Anforderungen am Umgang mit Bewerberdaten. Der Bewerber ist zum Zeitpunkt der Datenerhebung über die Datenverarbeitung gemäß Art. 13 DSGVO zu informieren und hat die Kenntnisnahme zu bestätigen. Die Daten sind nach einer festzulegenden Frist nach der Absage automatisiert zu löschen. Die Einwilligungen zur längeren Aufbewahrung (Talentpool) oder Weitergabe an verbundene Hotels kann der Bewerber elektronisch abgeben.

3.2 Personalakte

In der Privatwirtschaft gibt es keine Formvorschriften über das Führen von Personalakten. Form und Gestaltung der Personalakten obliegen deshalb der Gestaltungsfreiheit des Hoteliers bzw. der Personalabteilung.

Die Führung der Personalakten wird von folgenden Grundprinzipien bestimmt:

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

Vertraulichkeit der Personalunterlagen

Personalakten sind **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.

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

Wenn 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.

Bei elektronisch abgelegte Beschäftigtendaten ist sicherzustellen, dass kein unbefugter Zugriff auf diese Daten und Dateien erfolgen kann. Stark eingeschränkte Zugriffsrechte auf dem Fileserver reichen nicht aus, da es dem Administrator trotzdem möglich sein wird, auf diese Daten zuzugreifen. Sofern eine Datenablage im Netzwerk erfolgt, ist eine Verschlüsselung der Dateien, des Verzeichnisses oder Laufwerks sicherzustellen.

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 es keine gesetzliche Verpflichtung zur Führung einer Personalakte gibt, 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 neben diesen Nachweisdokumenten in die Personalakte aufgenommen werden. Grundsatz ist, dass alle Beschäftigten gleichbehandelt werden müssen.

Bei der Einstellung eines Mitarbeiters werden gern Dokumente, wie der **Personalausweis** oder der **Sozialversicherungsausweis** abgefragt. Für die Ablage einer Kopie in der Personalakte gibt es für diese Dokumente keine Gesetzesgrundlage. Möchte die Personalabteilung derartige Dokumente in der Personalakte ablegen oder Scannen, so bedarf das der formgerechten Einwilligung.

Ein **polizeiliches Führungszeugnis** darf nur abgefragt werden, wenn die Mitarbeiter eine Obhutspflicht in ihrer Tätigkeit erfüllen müssen, bspw. die Betreuung von Kindern oder Auszubildende.

Unrichtige Daten, bspw. bei Änderung der Wohnanschrift, sind zu berichtigen bzw. zu entfernen, wenn der Mitarbeiter darlegt, dass diese falsch sind. 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 Fragebögen 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 angemessen, 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.

3.3 Elektronische Personalakte

Für das Führen von elektronischen Personalakten oder Dateiablagen im Rahmen der Personaldatenverarbeitung gelten besondere datenschutzrechtliche Anforderungen insbesondere an den Zugriffsschutz. Da die Personalakten einem besonderen Vertraulichkeitsschutz unterliegen, sind die Zugriffsberechtigungen differenziert zu regeln. Folgende Zugriffsberechtigungen müssen regelbar sein:

- Zugriff auf Daten und Unterlagen, z.B. für den Beschäftigten im Rahmen einer Akteneinsicht
- eingeschränkter Zugriff auf ausgewählte Unterlagen, z.B. für die Fachvorgesetzten
- 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 Beschäftigten 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 aufzubewahren sind, 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. Datenschutzrechtlich ist sicherzustellen, 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.

Es sollte die Möglichkeit, von gespeicherten Dokumenten Kopien herzustellen, eingeschränkt werden. 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, 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 Beschäftigten 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.

3.4 Arbeitsvertrag inkl. Verpflichtungen und Vereinbarungen

Mit Abschluss des Arbeitsvertrages ist jeder Beschäftigte, der die Möglichkeit hat, personenbezogene Daten zu verarbeiten, auch zur Kenntnis zu nehmen, auf die **Vertraulichkeit** (früher 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 zur Vertraulichkeit ergibt sich die **Pflicht zu Schulungen**.

Neben der Verpflichtung empfiehlt es sich mit den Beschäftigten weitere Vereinbarungen zur Nutzung der IT- und Kommunikationsdienste zu treffen.

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 Beschäftigten 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 die Zustimmung der betroffenen Person einzuholen. Die Zustimmung sollte schriftlich und ggf. befristet für einen bestimmten Zeitraum eingeholt werden. Es empfiehlt sich Einverständniserklärungen und Nutzungsvereinbarungen mit den Mitarbeitern abzuschließen.

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.

Privatnutzung – JA oder NEIN

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

Wenn die Privatnutzung erlaubt ist, können Persönlichkeitsrechte eher berührt werden, wenn z.B. Kontrollen zur Überprüfung der Einhaltung der Nutzungsbestimmungen durchgeführt werden und im Zuge dessen auch Daten aus der Privatsphäre des Beschäftigten ausgewertet werden könnten.

Es sollten klare Regelungen für die Beschäftigten aufgestellt werden, die über ihre Rechten und Pflichten informierten. Es ist empfehlenswert, dass eine klare Trennung von dienstlicher und privater E-Mail-Kommunikation geregelt wird. Das Versenden von privaten Mails über den betrieblichen E-Mail-Account sollte untersagt werden. Für die Internetnutzung empfiehlt es sich, eine private Nutzung unter definierten 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.

3.5 Lohnabrechnung

Wird ein externes Lohnabrechnungsbüro beauftragt, so kann die Beauftragung der Datenverarbeitung im Auftrag unterliegen. Es ist zu prüfen, ob das Lohnabrechnungsbüro eine Steuerkanzlei oder ein Unternehmen aus der Privatwirtschaft ist. Abzuschließen sind Datenschutzvereinbarungen mit Unternehmen aus der Privatwirtschaft. 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.

Wird die Lohnbuchhaltung durch ein Lohnsteuerbüro bzw. durch eine Steuerkanzlei durchgeführt, entfällt die Verpflichtung zum Abschluss einer Vereinbarung zum Datenschutz. Hingegen muss bspw. mit DATEV eine Vereinbarung nach Art. 28 DSGVO abgeschlossen werden. Fragen Sie nach einen AVV.

4 Informationspflichten bei Verstoß gegen den Datenschutz

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 die verantwortliche Stelle **auch die betroffene Person** ohne unangemessene Verzögerung **benachrichtigen**.

Unzulässige Speicherung personenbezogener Daten

Wenn ein Mitarbeiter oder Dritter feststellt oder vermutet, dass die Speicherung von personenbezogenen Daten unzulässig ist, ist zu prüfen, ob eine unerlaubte Speicherung vorliegt. Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind zu löschen, wenn:

- ihre Speicherung unzulässig ist oder
- ihr Verwendungszweck zur Erfüllung einer Aufgabe entfällt.

Bevor Daten gelöscht werden, ist zu prüfen, ob es relevante Aufbewahrungsfristen gibt. Sollte dieses zutreffen, sind die Daten zu sperren.

Einsicht in sensible Daten

Wenn ein Mitarbeiter oder Dritter vermutet oder feststellt, dass eine unbefugte Kenntnisnahme vorliegt, ist zu prüfen, ob ein Verstoß gegen die Vertraulichkeit personenbezogener Daten vorliegt. Wenn sensible Daten verloren gegangen oder gestohlen wurden, ist vom Datenschutzbeauftragten zu prüfen, ob die Aufsichtsbehörde für Datenschutz über den Verlust informiert werden muss. Mitarbeiter sind auf den vertraulichen Umgang mit betrieblichen und personenbezogenen Daten zu sensibilisieren bzw. zu verpflichten. Regelmäßige Überprüfungen in Form von Begehungen und Audits sind durch den Datenschutzbeauftragten durchzuführen und zu dokumentieren. Verschlüsselungstechnologien für Notebooks, Datenträger und sensible Daten im Netzwerk sind bereitzustellen. Es ist zu prüfen, ob Passwortmanager einzusetzen sind, wenn Passwortlisten nicht ausreichend geschützt sind und kein regelmäßiger Passwortwechsel stattfindet.

Unerlaubte Datenübermittlung

Wenn ein Mitarbeiter oder Dritter vermutet oder feststellt, dass eine unerlaubte Datenübermittlung stattgefunden hat, ist zu prüfen, ob ein Verstoß gegen die Vertraulichkeit personenbezogener Daten vorliegt. Mit dem Empfänger ist eine Vertragsgrundlage (Dienstleistungsvertrag und/oder Datenschutzvereinbarung bzw. ein EU-Standardvertrag bei Drittländern ohne ausreichendes Datenschutzniveau) nachträglich zu vereinbaren. Es ist zu prüfen, wie bei Bedarf eine Einverständniserklärung zur Datenübermittlung beim Betroffenen eingeholt werden kann. Mitarbeiter sind zu informieren bzw. zu belehren. Wenn sensible Daten übermittelt wurden, ist vom Datenschutzbeauftragten zu prüfen, ob die Aufsichtsbehörde für Datenschutz über die Übermittlung informiert werden muss.

Verlust von Daten

Wenn ein Mitarbeiter oder Dritter feststellt, dass es zu einem Datenverlust gekommen ist, ist zu prüfen, ob ein Verstoß gegen die Vertraulichkeit personenbezogener Daten vorliegt. Es ist zu prüfen, ob weitere Institutionen oder die Betroffenen über den Verlust der Daten informiert werden müssen. Entsprechend ist zu handeln. Die Sicherheitsanforderungen müssen neu bewertet und ggf. angepasst werden.

Hackerangriff

Wenn ein Mitarbeiter oder Dritter feststellt, dass es zu einem Hackerangriff gekommen ist, ist zu prüfen, ob ein Verstoß gegen die Vertraulichkeit personenbezogener Daten vorliegt. Die Aufsichtsbehörde für Datenschutz ist im Fall eines nachgewiesenen Hackerangriffs über den Vorfall zu informieren. Es ist zu prüfen, ob weitere Institutionen oder die Betroffenen über den Verlust der Daten informiert werden müssen. Entsprechend ist zu handeln. Die Sicherheitsanforderungen müssen neu bewertet und ggf. angepasst werden.

Vernichtung von Daten

Wenn ein Mitarbeiter oder Dritter feststellt, dass es zur Vernichtung von Daten gekommen ist, ist zu prüfen, ob ein Verstoß gegen die Vertraulichkeit personenbezogener Daten vorliegt. Es ist zu prüfen, ob die Aufsichtsbehörde für Datenschutz, weitere Institutionen oder die Betroffenen über den Verlust der Daten informiert werden müssen. Entsprechend ist zu handeln.

5 Auskunftspflichten

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.

5.1 Gast

Wird eine Auskunftsanfrage an eine Abteilung im Hotel (insbesondere Direktion, Empfang, Reservierung oder Sales & Marketing) gestellt, so ist diese innerhalb von einem Monat zu erteilen. Bei komplexen Angaben kann die Frist um zwei Monate verlängert werden, wobei der Betroffene darüber zu informieren ist. Bei der Beantwortung der Auskunftsanfrage ist auf dem Umfang entsprechend Art. 15 DSGVO Bezug zu nehmen. Die Auskunft ist schriftlich (in Briefform oder per Mail, wenn die E-Mail-Adresse verifiziert werden kann, 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.

Bei Zweifel an der Identität (z.B. unbekannte Kontaktdaten wie E-Mail-Adresse) des Anfragenden ist eine Identitätsprüfung durchzuführen (über eine Ausweiskopie mit geschwärzten Passagen, insb. Foto).

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. Diese sollten sich allerdings nicht auf allgemeine Angaben, wie dem Geburtsdatum oder Wohnort beziehen. Im Zweifelsfall ist die Auskunft am Telefon zu verweigern und schriftlich zuzustellen.

5.2 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.** Das Einverständnis ist anlassbezogen direkt beim Betroffenen schriftlich einzuholen, z.B. mittels einer Schweigepflichtentbindungserklärung.

Auf Grundlage von **§ 24 Abs. 1 Nr. 1 BDSG** 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.

5.3 Unternehmen und nichtöffentliche Einrichtungen

Für Unternehmen aus dem nichtöffentlichen Bereich (wie Verbände, Versicherungen, Anwälte, etc.) 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 BDSG 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.

5.4 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.

6 Sales & Marketing

6.1 Internetauftritt

Nutzer von Webseiten und firmeneigenen Social-Media-Diensten (Facebook Fanpage etc.) sind rechtzeitig und in geeigneter Form auf die Speicherung, Nutzung und Übermittlung von personenbezogenen Daten an Dritte hinzuweisen. Ein **Impressum** gemäß § 5 Digitale-Dienste-Gesetz (DDG) sowie eine **Datenschutzerklärung** im Sinne Artt. 13, 14 DSGVO sind so einzubinden, dass sie **von jeder Seite aus abrufbar** sind.

Informationspflichten

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

Gemäß § 5 DDG 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 sind genau und in verständlicher Form zu beschreiben. Seiner **zusätzlichen Informationspflicht** kommt der Webseitenbetreiber in einer **Datenschutzerklärung** nach.

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.

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 AGB zu integrieren, sondern diese sollte als eigene Seite im Internetauftritt erscheinen.

Urheberrechtsschutz

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

Sollten 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, ist das Recht des Gastes oder auch Mitarbeiters am eigenen Bild gem. §§ 22, 23 KunstUrhG zu beachten. Für diese Fälle wird immer eine individuelle Einwilligungserklärung vom Abgebildeten benötigt. 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.

Verwendung von Cookies auf der Webseite

Wenn auf Ihrer Webseite **Cookies** oder andere **Scripte** verwendet werden, ist dies dem **Nutzer mitzuteilen**. §§ 25, 26 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) regeln die Pflicht zum Einsatz von Consent Managern (Cookiebanner). Sowohl die Nutzung von **Analyse- und/oder Trackingtools** als auch die Nutzung von Cookies, Scripten und Add-on, welche Daten beim Aufruf der Webseite an Dritte übermitteln, bedürfen der **Einwilligung durch den Webseitenbesucher**. Einwilligungsfrei sind nur Cookies und Scripte, welche für die Darstellung der Webseite notwendig sind.

Für das Einwilligungsmanagement ist eine **Consent Manager Plattform (CMP)** auf der Webseite oder im GoogleTagManager einzubinden. Mit der Einbindung des Consent Managers muss auch geprüft werden, ob eventuell Dienste von Drittanbietern mit eingebunden wurden. Der Consent Manager deckt diese in der Regel nicht mit ab, da der Aufruf der Dienste über eine andere Internetplattform erfolgt. In diesem Fall ist eine Klärung mit dem Dienstleister erforderlich. Es empfiehlt sich, entweder die einwilligungspflichtigen Tracking- und Marketingdienste vom Systemanbieter entfernen zu lassen oder die Einbindung einer eigenen Consent Lösung durch den Dienstleister zu veranlassen. Nachfolgend die wichtigsten Funktionalitäten, welche Sie bei der Auswahl eines geeigneten Consent Manager prüfen sollten:

- Der Consent Manager sollte zu jeder Zeit von jeder Seite aus erreichbar sein.
- Die Einstellungen, die man als Nutzer tätigt, sollten zu einem späteren Zeitpunkt ohne große Probleme geändert werden können. Dies ist erforderlich, wenn beim Surfen auf der Webseite festgestellt werden sollte, dass zuvor abgewählte Dienst wie z.B. Google Maps oder YouTube für die weiter Nutzung notwendig sind.

- Die Anforderungen an eine gleichrangige und gleichfarbige Gestaltung der Auswahlbutton sollten unterstützt werden.
- Cookies sind in Gruppen zu kategorisieren.
- Eine individuelle Auswahl innerhalb einer Kategorie sollte möglich sein. Es sollte jedem Nutzer möglich sein, individuell Cookies zuzulassen oder abzuwählen. Die Grundeinstellung sollte zunächst alle, außer die technisch notwendigen Cookies blockieren.
- Zusätzliche Informationen zu den eingesetzten Cookies sollten abrufbar sein. Der Nutzer ist über deren Zweck zu informieren, um in der Lage zu sein, eine Entscheidung zu treffen.
- Es sollte ein Link zur Datenschutzerklärung der Webseite und eventuell zum CMP-Anbieter vorhanden sein. Von Vorteil ist es, wenn der Consent Manager zudem eine integrierte Cookie Policy anbietet, um auf einen Blick Informationen zu den eingesetzten Cookies inkl. der Speicherdauer zu erhalten.
- Der Google Tag Manager stellen Anbieter schnell vor immer neuen Herausforderungen. Soweit bspw. der Google Tag Manager auf der Webseite zum Einsatz kommt/kommen soll, ist bei der Wahl des Consent Managers zu prüfen, ob dieser entweder (I) den Google Tag Manager komplett blockiert, (II) im HTML-Code eingebunden werden kann oder (III) im Google Tag Manager eingebunden werden kann.
- Änderungen auf der Webseite sollten regelmäßig geprüft werden, sog. Cookie-Crawler kommen hier zum Einsatz.

Texte sollten im Consent Manager durch den Webseitenbetreiber individuell angepasst werden können. Das kann für die rechtskonforme Information erforderlich sein.

Am 01.10.2019 hat der Europäische Gerichtshof (EuGH) ein Grundsatzurteil zur Verwendung von Cookies getroffen, am 28.05.2020 wurde das Urteil durch den BGH bestätigt. Demnach ist der Einsatz von „nicht notwendigen Cookies“ nur noch mit einer aktiven Einwilligung gestattet. **Sowohl die gewöhnlichen Cookie-Banner mit Bestätigung der Kenntnisnahme zur Verwendung von Cookies als auch mit einem Haken voreingestellte *Consent-Manager* sind unzulässig! Der Button für „Alle Cookies zulassen“ darf nicht hervorgehoben sein.**

WICHTIG | Werbe- und Tracking-Cookies dürfen nicht schon aktiv sein bzw. gespeichert werden, bevor der Webseitenbesucher sich gegen deren Verwendung entscheiden kann. Vielmehr muss der Webseitenbesucher aktiv einwilligen.

6.2 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 LinkedIn-Accounts, Blogs, Facebook-Fanseiten etc.) sollten immer mit der Hotelleitung bzw. wenn vorhanden mit dem Bereich Sales & Marketing, eCommerce 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 DDG sowie ein Link auf die Datenschutzerklärung der eigenen Webseite ist einzubinden. In der Datenschutzerklärung sind die Social Media Dienste zu beschreiben.

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.

6.3 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 Gäste) 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 zu Bewerbenden (z.B.

Gast) 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 Werbungsempfänger die 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.

E-Mail-Werbung (Newsletter)

Die Nutzung der E-Mail-Adresse für einen **Newsletterservice** bedarf der schriftlichen Einverständniserklärung des Empfängers, 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 Interessent muss selbst aktiv werden, zum Beispiel mit dem aktiven Setzen eines Hakens oder Kreuzes und/oder seiner Unterschrift einwilligen. An dieser Stelle muss der Interessent gelichzeitig auf sein Widerrufsrecht hingewiesen werden. Die elektronische Einwilligung muss vom angegebenen Empfänger stammen. Als einzige anerkannte elektronische 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 Unternehmensverbundes 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 Empfänger über seine Widerrufsrechte aufgeklärt wird. Die Bestellung und Abbestellung des Newsletters inkl. der Einwilligungserklärung sind zu dokumentieren.

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.“*

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.

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

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.

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.

6.4 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.

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.

Online-Bewertungen

In der Regel 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.

6.5 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. DDG und UWG sind bei Webseite und E-Mail-Werbung einzuhalten.
- Werden Reservierungen über Ihre Webseite getätigt, so sollte die Anwendung der AGB 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.

7 Verzeichnis von Verarbeitungstätigkeiten

Gemäß Art. 30 DSGVO i.V.m Erwägungsgrund 82 hat die verantwortliche Stelle, also der Arzt bzw. die Arztpraxis im Rahmen seiner Dokumentationspflichten ein **Verzeichnis von Verarbeitungstätigkeiten (VVT)** zu führen. Weiterhin kann die zuständige Aufsichtsbehörde die Vorlage verlangen, um die betreffenden Stellen hoheitlich zu kontrollieren.

Was ist ein Verzeichnis für Verarbeitungstätigkeiten?

In einem Verzeichnis für Verarbeitungstätigkeiten werden alle Verfahren und Prozesse, in denen personenbezogene Daten verarbeitet werden, beschrieben. Standardverfahren in der Hotellerie können sein:

- Gastdatenverwaltung
- Reservierung / Buchung, auch Tischreservierung
- Online Check-In
- Kundengewinnung
- Gutscheinsystem
- Onlinebewertung
- Newsletter
- Mahnwesen / Inkasso

aber auch:

- Mitarbeiterverwaltung
- Bewerbungsverfahren
- Elektronische Arbeitszeiterfassung
- Lohn- und Gehaltsabrechnung
- Benutzerverwaltung
- E-Mail-Kommunikation
- Videokontrollsystem
- Webseite

Das VVT kann auch als Grundlage für **Datenschutzaudits** (Verfahrensaudit) und **Risikobewertungen** (Schutzbedarfsfeststellung) 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.

Für das Verzeichnis für Verarbeitungstätigkeiten muss zunächst ermittelt werden, in welchen Fällen personenbezogene Daten von z.B. Gästen 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. PMS, Online-Reservierungssystem, Zeiterfassungssystem, Personalverwaltungssystem, Videoüberwachung, …) bestehen.

7.1 Inhalte

Das VVT ist 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 (Schutzbedarfsfeststellung) bzw. eine zusätzliche Strukturierung, die festhält, welche Verarbeitungen ggf. eine Datenschutz-Folgenabschätzung erfordern und welche nicht. Daneben können die durchgeführten Prüfungen aufgenommen werden.

7.2 Datenschutz-Folgenabschätzung

Eine **Datenschutz-Folgenabschätzung** ist gemäß Art. 35 DSGVO immer dann durchzuführen, wenn 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

Datenschutz-Folgenabschätzungen sind dann durchzuführen, wenn eine systematische Videoüberwachung im Hotel bzw. auf dem gesamten Gelände erfolgt.

Auf die Aufsichtsbehörden kommt die 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. Die Datenschutz-Folgenabschätzung dient 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.

8 Datenverarbeitung im Auftrag

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 Werbebriefen, 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 ist 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 durch die Datenschutzaufsichtsbehörden verhängt werden.

Es ist empfehlenswert, über die bestehenden Verträge ein Vertragsverzeichnis zu führen.

Zu prüfen sind 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.

8.1 Abgrenzung der Datenverarbeitung im Auftrag

Datenschutzrechtlich zu unterscheiden sind beim Outsourcing die Datenverarbeitung im Auftrag sowie in eigener oder gemeinsamer Verantwortlichkeit. Die Frage, ob ein Outsourcing als **Auftragsverarbeitung** oder **eigener Verantwortlichkeit** (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.

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 **eigenen Verantwortlichkeit** wird dagegen auch die der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zugrundeliegende 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 die eigene Verantwortlichkeit:

- 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.

Tätigkeiten in eigener Verantwortung können in der Regel die Einbeziehung eines:

- Berufsgeheimnisträgers (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer),
- Inkassobüros mit Forderungsübertragung,
- Postdienstes für den Brieftransport,
- Personalvermittlers nach Auftrag von Stellensuchenden oder Arbeitgebern,
- Internet-Plattformbetreibers zur Vermittlung zwischen Anbietern und Nachfragern, die sich auf der Plattform treffen können,
- TKG-Dienstleisters, es sei denn, darüber hinaus gehende Zusatzdienste wie Auslagerung einer betrieblichen Telefonanlage oder Cloudspeicherlösungen usw.,
- Versicherungs-/Finanzmaklers, -vermittlers im Rahmen des Kundenvertrags,
- Handelsvertreters im Rahmen ihrer Beratungstätigkeit und Vertragsvermittlungen,
- Schulungsveranstalters oder an das Tagungshotel,
- Zahlungsdienstleisters für elektronische Zahlungen (Transport von Zahlungsdaten, Geldwäsche- und Betrugsprüfung nach ZAG und den Mindestanforderungen der BaFin),
- Reisebüros aufgrund Kundenvertrags vermittelte Leistungsanbieter, wie Hotels, Mietwagenfirmen, Fluggesellschaften, Busunternehmen, Versicherungen usw.

Keine Auftragsverarbeitung liegt ferner vor, wenn **gemeinsame Verantwortlichkeit nach Art. 26 DSGVO** gegeben ist, d.h. wenn mehrere Verantwortliche gemeinsam über die Verarbeitungszwecke und -mittel entscheiden. Hierunter können je nach Gestaltung eine Reihe von Verarbeitungen fallen, die bisweilen unter eigene Verantwortlichkeit eingestuft werden können, etwa gemeinsame Verwaltung bestimmter Datenkategorien (z.B. „Stammdaten“) für bestimmte gleichlaufende Geschäftszwecke.

Insbesondere in Hotelgruppen ist davon auszugehen, dass eine gemeinsame Verantwortung in der Datenverarbeitung vorliegt, wenn alle Hotels auf eine zentrale Gastdatenbank zugreifen.

In der zu treffenden Vereinbarung, auch Joint Controller Agreement genannt, ist festzulegen, wie der Zugriff in welchem Umfang erfolgen darf. So sollte jedes Hotel nur seine eigene Historie zum Gast einsehen können.

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.

8.2 Auswahl des Dienstleisters

Prüfung des Leistungsumfangs

Bevor ein Vertrag mit einem Dienstleister unterzeichnet werden kann, ist der Leistungsumfang von der verantwortlichen Stelle, also dem Hotel, dahingehend zu prüfen, in wieweit der Dienstleister als 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 Netzwerkprotokolle 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

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.

Transfer Impact Assessment (TIA)

Ein Transfer Impact Assessment (TIA) ist im Rahmen der Datenverarbeitung im Auftrag bei einem **Datentransfer** in Länder **außerhalb der EU/EWR (Drittlandstransfer) bzw. bei Nutzung von Dienstleistern mit Geschäftssitz in einem Land außerhalb der EU/EWR** durchzuführen. Auch wenn personenbezogene Daten durch Dienstleister oder Systemanbieter aus einem unsicheren Drittland (Staaten ohne Angemessenheitsbeschluss) auf dem europäischen Territorium verarbeitet werden (z.B. Hosting), ist eine TIA durchzuführen. Grundlage zum durchzuführenden Verfahren bildet Klausel 14 der EU-Standardvertragsklauseln (SCC), welche im Juni 2021 durch die EU veröffentlicht wurden. Ist ein US-Dienstleister im **Data Privacy Framework**, dem früheren Privacy Shield, zertifiziert, entfällt die EU-Standardvertragsklausel (SCC) und die TIA. Hier reicht ein DPA aus. Es empfiehlt sich aber dennoch ein DPA + SCC abzuschließen, da nicht sichergestellt werden kann, dass das Data Privacy Framework rechtskräftig bleibt.

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.

8.3 Drittlandtransfer – Auftragnehmer in unsicheren Drittstaaten

In Anlehnung an das Schrems II- Urteil (2020), mit dem das Privacy Shield vom EuGH für ungültig erklärt wurde, hat der European Data Protection Bord (EDPB) eine Guideline zum Transfer personenbezogener Daten in Drittländer herausgegeben.

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_de.pdf

In diesen Empfehlungen geht es um den Datentransfer in Länder, die lt. der EU kein angemessenes Datenschutzniveau nachweisen. Damit ausdrücklich verbunden sind die Möglichkeiten der Aufsichtsbehörden, Verarbeitungen, die in einem Drittland stattfinden, z.B. bei der

Nutzung von Cloud-Diensten, zu untersagen und ggf. Bußgelder zu verhängen, wenn keine ausreichenden Sicherheiten geboten werden.

Die Instrumente zur Absicherung des Datentransfers finden sich in Art. 46 DSGVO wieder:

- Standard-Datenschutzklauseln (SCCs)
- verbindliche Unternehmensregeln (BCR)
- Verhaltenskodizes
- Zertifizierungsmechanismen
- Ad-hoc-Vertragsklauseln

Es wird in den Guidelines, bekräftigt durch das EuGH-Urteil, darauf hingewiesen, dass die EU-Standardvertragsklauseln (SCC) ohne zusätzliche Sicherheitsmaßnahmen nicht ausreichend sind und einer genauen Prüfung bedürfen.

Unabhängig davon, welches Instrument nach Artikel 46 DSGVO eingesetzt wird, muss sichergestellt werden, dass das Datenschutzniveau der DSGVO erreicht wird.

Abgesehen von den Garantien des Art. 46 DSGVO gibt es gem. Art. 49 DSGVO einige Ausnahmen, die einen Drittlandtransfer ermöglichen. Die wichtigsten Punkte sind:

- die betroffene Person hat ausdrücklich eingewilligt
- die Übermittlung ist zur Erfüllung des Vertrages zwingend erforderlich
- die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig
- die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich

Bevor sich jedoch auf eine Ausnahmeregelung nach Art. 49 DSGVO berufen werden kann, muss geprüft werden, ob eine Übertragung die strengen Bedingungen erfüllt, die diese Bestimmung für jeden einzelnen Fall vorsieht.

Zur Prüfung und Dokumentation, ob der Datentransfer in ein Drittland, durch ausreichende Garantien abgesichert ist, sind folgende Schritte erforderlich:

1. **Den Datentransfer kennen**

   Um eine Prüfung durchführen zu können, ist es zunächst erforderlich die Datenflüsse herauszufinden und zu dokumentieren. Dazu kann das Verzeichnis für Verarbeitungstätigkeiten dienen. Dieses ist auf Vollständigkeit zu prüfen hinsichtlich der Datenkategorien, Empfänger und verwendeten Systeme. Denken Sie daran, dass der Fernzugriff aus einem Drittland (z.B. in Supportsituationen) und/oder die Speicherung in einer außerhalb des EWR gelegenen Cloud ebenfalls als Übertragung gilt.

2. **Identifizierung der Dienstleister und der abgeschlossenen Vereinbarungen**

   In der Übersicht der verwendeten Dienstleister ist die Art der Vereinbarung (z.B. EU-Standardvertragsklausel) und das Land festzuhalten, in dem der Dienstleister sitzt, bzw. in welches die Daten übertragen werden. Dabei sind auch die Subunternehmen von verwendeten Dienstleistern zu berücksichtigen, selbst wenn sich diese in der EU befinden.

3. **Prüfung, ob die abgeschlossenen Vereinbarungen ausreichen**

   Das Transfer-Instrument muss sicherstellen, dass das durch das DSGVO garantierte Schutzniveau durch den Transfer nicht untergraben wird. Dies ist nicht der Fall, wenn der Datenimporteur aufgrund von Rechtsvorschriften und Praktiken des Drittlandes an der Erfüllung seiner Verpflichtungen gehindert wird.

Durch die Befragung der Dienstleister kann ermittelt werden, welchen Gesetzen und Verpflichtungen dieser unterliegt. Dazu sollte ein entsprechender Fragebogen an die Dienstleister versendet werden.

4. **Beurteilung der Risiken des Datentransfers für die Betroffenen**

   In einer Schutzeinstufung kann ermittelt werden, welche Datenkategorien verarbeitet werden, ausgehend von den Verfahren. Somit wird dokumentiert, wie hoch das Risiko für den Betroffenen bzgl. der Datenübermittlung ist und welche zusätzlichen geeigneten Maßnahmen getroffen wurden. Es sollte dabei auch geprüft werden, ob es Alternativen in der EU gibt und falls nicht, ist dies ausreichend zu begründen.

   Diese Beurteilung und die von Ihnen ausgewählten und umgesetzten zusätzlichen Maßnahmen sind auf Anfrage der zuständigen Aufsichtsbehörde zur Verfügung zu stellen.

5. **Festlegung zusätzlicher Maßnahmen**

   Von Fall zu Fall ist zu ermitteln, welche zusätzlichen Maßnahmen für eine Reihe von Transfers in ein bestimmtes Drittland wirksam sein könnten. Diese Maßnahmen können folgende sein:

   - Ausreichende und sichere Verschlüsselung der Daten während des Transfers und bei der Speicherung. Dabei hat der Dienstleister keine Entschlüsselungsmöglichkeit.
   - Sichere Pseudonymisierung oder Anonymisierung der Daten
   - Splitting der Daten oder Verarbeitung durch mehrere Dienstleister, so dass kein Personenbezug eines einzelnen Dienstleisters möglich ist.
   - Absicherung der Daten durch spezielle Gesetzgebungen im Drittland (z.B. Gesundheitsdaten)
   - Zusätzliche vertragliche Vereinbarungen, wobei zu beachten ist, dass diese im Allgemeinen nicht geeignet sind, die Behörden des Drittlandes zu binden, wenn sie nicht Vertragspartei sind.
   - Transparenzverpflichtungen; Offenlegung von Anfragen von Behörden z.B. im Bereich der nachrichtendienstlichen Aufklärung (Transparenzbericht des Dienstleisters)
   - Erklärung des Dienstleisters, dass er nicht absichtlich Backdoors oder eine ähnliche Programmierung geschaffen hat, die für den Zugriff auf das System und/oder personenbezogene Daten verwendet werden könnten

Die EU-Kommission wird in 2021 neue EU-Standard-Datenschutzklauseln für unterschiedliche Verarbeitungstätigkeiten erstellen, die den Datentransfer in Drittländer besser absichern. Sobald diese veröffentlicht wurden, haben Sie 1 Jahr Zeit, alte Vereinbarungen in neue umzuwandeln.

8.4 Vertragsgestaltung und Vertragsabschluss

Der Vertrag bzw. vielmehr die zusätzliche Vereinbarung zum 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.

Die Gesellschaft für Datenschutz und Datensicherheit (GDD) hat auf ihrer Webseite in der Praxishilfe IV zur DSGVO den Entwurf einer Vereinbarung zum Datenschutz nach Art. 28 DSGVO veröffentlicht. Dieser ist aber an die speziellen Gegebenheiten anzupassen.

Link:

https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo

Ebenfalls empfiehlt sich Nutzung der EU-Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7. Dieser Vertrag kann zwischen Auftraggeber und Auftragnehmer genutzt werden, wen diese gemeinsam ihren Firmensitz innerhalb der EU/EWR oder in einem sicheren Drittland haben. Texte im Vertragstext dürfen nicht angepasst werden. Zur Detailierung des Vertragsverhältnisses dienen die vorgegebenen Anhänge. Weitere Konkretisierungen sind möglich.

Link:

https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32021D0915

Abgrenzung der Leistung

Im ersten Schritt ist entsprechend den Merkmalen aus Pkt. 7.1 abzugrenzen, ob es sich bei der Dienstleistung um eine Auftragsverarbeitung oder eine eigene oder gemeinsame Verantwortlichkeit 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.

Als Auftraggeber sind immer Sie dafür verantwortlich, dass eine Vereinbarung zur Datenverarbeitung im Auftrag abgeschlossen wird. Sie können vorab prüfen, ob Vereinbarungen im gesetzlichen Umfang schon im bestehenden Vertrag und/oder deren Anlagen geregelt sind.

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 vorgegeben.

Als Vertragsformen kommen i.d.R. Dienstleistungs- oder Serviceverträge im Rahmen von IT-Systemen, Rahmenvereinbarungen im Zusammenhang mit einer kooperativen Zusammenarbeit aber auch Vertragsbeziehungen mit Fremdpersonal im eigenen Hause in Betracht. Entsprechend ist das Unternehmen oder die Einzelperson als Auftragnehmer auf - die Vertraulichkeit durch das Hotel als Auftraggeber vor oder im Zuge des Vertragsabschlusses 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 die Vertraulichkeit, eine Vertraulichkeitsvereinbarung, eine Datenschutzvereinbarung oder sogar eine EU-Standarddatenschutzklausel abzuschließen ist.

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. Die nachfolgende Aufstellung hilft Ihnen bei der Entscheidungsfindung.

Vertragsarten	Vertragsformen zur Zusatzvereinbarung
Dienstleistungs- und Servicevertrag	Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO EU-Standardvertragsklauseln mit Stand zum 04. Juni 2021 Vertraulichkeitsvereinbarung
Fremdpersonal	Verpflichtung von Dritten – Fremdpersonal – auf die Vertraulichkeit
Rahmenvereinbarungen	Datenschutzvereinbarung / Zusatzvereinbarung Joint Controller Agreement (Art. 26 Vereinbarung)
Datenübermittlung in Drittstaaten ohne angemessenen Datenschutzniveau (Drittländer außerhalb der EU/EWR)	EU-Standardvertragsklausel mit Stand zum 04. Juni 2021
Datenübermittlung in Drittstaaten mit angemessenen Datenschutzniveau (auch Privacy Shield)	Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO EU-Standardvertragsklauseln mit Stand zum 04. Juni 2021

Es empfiehlt sich, im ersten Schritt beim Dienstleister einen Entwurf zur abzuschließenden Datenschutzvereinbarung anzufragen. Die Dienstleister bieten i.d.R. eine eigene Vereinbarung an, um den eigenen Verwaltungsaufwand zu minimieren. Die Vereinbarung ist dann aber nicht einfach zu unterzeichnen, sie muss geprüft werden, ob diese alle erforderlichen Angaben gemäß Art. 28 DSGVO enthalten. Anderenfalls sind Anpassungen vorzunehmen.

Datenschutzvereinbarungen können sowohl elektronisch als Bestandteil eines elektronisch abgeschlossenen Vertrages oder als Ergänzung zu einem schriftlichen Vertrag separat elektronisch signiert werden.

8.5 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

9 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 BDSG 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)

9.1 Zulässige und unzulässige Videoüberwachungen

Es 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 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.

9.2 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.

9.3 Protokollierungs- und Löschungspflicht

Genaue Speicherfristen wurden im BDSG nicht festgelegt. In § 4 Abs. 5 BDSG 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.

9.4 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.

9.5 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.

10 Datenschutz und Sicherheit - Regelungen im Hotel

Die DSGVO sieht vor, dass die technischen und organisatorischen Maßnahmen zu Datenschutz und Datensicherheit dokumentiert werden.

10.1 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.

10.2 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. Die Regeln zum Datenschutz sollten regelmäßig in einem internen Datenschutzaudit auf Einhaltung und Aktualität geprüft werden.

Weil ein wirksamer Datenschutz nicht allein durch Regelungen und Bestimmungen erreicht werden kann, sondern von einem ausgeprägten Datenschutz- und Sicherheitsbewusstsein der 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 Elektronischen Arbeitszeiterfassungssystemen
- Einsatz von elektronischen Türschließsystemen

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.

10.3 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.

Die Regeln zur Datensicherheit sollten regelmäßig in einem internen IT-Sicherheitsaudit auf Einhaltung und Aktualität geprüft werden.

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
AGG	Allgemeines Gleichbehandlungsgesetz
BCR	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BMG	Bundesmeldegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
CRM	Customer-Relationship-Management
DDG	Digitale-Dienste-Gesetz
DPF	Data Privacy Framework
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
SCC	EU-Standardvertragsklauseln
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
TIA	Transfer Impact Assessment
TKG	Telekommunikationsgesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
VVT	Verzeichnis von Verarbeitungstätigkeiten
WLAN	Wireless Local Area Network