LEITFADEN

DATENSCHUTZ IN DER HOTELLERIE

STAND FEBRUAR 2020

IMPRESSUM

Medieninhaber und Herausgeber:

ÖSTERREICHISCHE HOTELIERVEREINIGUNG I Hofburg, A-1010 Wien
T: +43 1 533 09 52 I office@oehv.at I www.oehv.at
www.facebook.com/hoteliervereinigung

vertreten durch: Dr. Markus Gratzer, ÖHV-Generalsekretär

Koordination: Mag. Maria Wottawa

2. Auflage

Autoren:

H3 Hotel Training & Beratung e.U.
A-3553 Schiltern | Obere Straße 26
T: + 43 664 504 68 28
office@h3training.at
www.h3training.at

DataSolution Thurmann GbR
D-14974 Ludwigsfelde | Isarstraße 13
T: + 49 3378 20 25 13
mail@hoteldatenschutz.de
www.hoteldatenschutz.de

Grafik, Design:

Birgit Rieger I www.br-design.at

Copyright:

DataSolution Thurmann GbR 2017

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung der Ersteller zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Die Österreichische Hoteliervereinigung hat die Nutzungsrechte zur Veröffentlichung dieser Publikation. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen bei DataSolution Thurmann GbR.

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

EDITORIAL

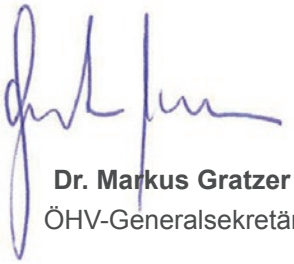
Mit 25. Mai 2018 trat die Datenschutzgrundverordnung (DSGVO) in Kraft. Sie ist für jedes Unternehmen in Österreich und somit auch für die Hotellerie bindend und geltendes Recht in allen EU-Mitgliedstaaten. Aufgrund von Öffnungsklauseln konnten zusätzlich durch die einzelnen EU-Länder länderspezifische Detailregelungen erlassen werden, die allerdings das Datenschutzniveau der DSGVO nicht unterlaufen dürfen. In Österreich gilt es damit, neben der DSGVO auch die Vorgaben aus dem Datenschutzgesetz (DSG), welches adaptiert wurde, zu beachten.

Das Grundrecht auf Datenschutz schützt nicht Daten, sondern Menschen, im Mittelpunkt stehen daher personenbezogene Daten. Die betroffene Person hat umfassende Rechte, die das operative Arbeiten nicht einfacher machen. In der Hotellerie stehen daher Gästedaten aber auch Mitarbeiterdaten im Zentrum! Der damit verbundene Aufwand darf nicht unterschätzt werden.

Sie finden in diesem Leitfaden viele Praxisthemen vom Check-in über das Check-out bis zu Gästebewertungen und Kundenbindungsprogramme. Hinsichtlich Mitarbeiter gehen die Themen von den Bewerberdaten über den elektronischen Personalakt bis zum Austritt der Mitarbeiter. Weiters bietet der Leitfaden auch einen Wegweiser für die Umsetzung in der Praxis und entsprechende Muster und Vorlagen an.

Dieser Leitfaden liegt bereits in der 2. Auflage vor und soll Sie dabei unterstützen, die laufenden Aufgaben im Datenschutz gut zu meistern.

Für eine STARKE Hotellerie.



Dr. Markus Gratzer
ÖHV-Generalsekretär

Wien, im Dezember 2019

INHALT

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
ArbVG	Arbeitsverfassungsgesetz
AVRAG	Arbeitsvertragsrechts Anpassungsgesetz
BCR	Binding Corporate Rules
BYOD	Bring Your Own Device
CRM	Customer-Relationship-Management
DB	Datenschutzbeauftragte()
DSB	Datenschutzbehörde
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung
DSMS	Datenschutzmanagementsystem
DVR	Datenverarbeitungsregister
DSG	Datenschutzgesetz
DSK	Datenschutzkoordinator
ECG	E-Commerce Gesetz
EU	Europäische Union
FO	Front Office
GIBG	Gleichbehandlungsgesetz
GoBD	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff
HR	Human Resource
IT	Informationstechnik
ISMS	Information Security Management System
MedienG	Mediengesetz
PC	Personal Computer
PCI DSS	Payment Card Industry Data Security Standard
PMS	Property Management System
PR	Public Relation
QM	Qualitätsmanagement
TKG	Telekommunikationsgesetz
UWG	Unlauterer Wettbewerb Gesetz
VVT	Verzeichnis von Verarbeitungstätigkeiten

1. Das Datenschutzrecht

ZIELFRAGEN:

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

Im Mai 2018 trat das Datenschutzrecht die EU-Datenschutz-Grundverordnung (in weiterer Folge DSGVO) zusammen mit den Erwägungsgründen und dem überarbeiteten Datenschutzgesetz, dem **Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten** (in weiterer Folge DSG) in Kraft. Jedoch sind für die elektronische Kommunikation, auch das **Telekommunikationsgesetz 2003** (in weiterer Folge TKG) und das **E-Commerce Gesetz** (in weiterer Folge ECG) für das Anbahnen und Abwickeln von Geschäften im Internet von Bedeutung.

1.1. Anwendungsbereich der DSGVO

Die DSGVO gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen.

Personenbezogene Daten sind alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person (betroffene Person/Betroffener) beziehen. Bestimmbar ist eine Person z.B. über Telefonnummer, Gesicht auf einem Foto, IP-Adresse etc. Unter Verarbeitung versteht man das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Weitergabe durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung personenbezogener Daten mit oder ohne Hilfe automatisierter Verfahren.

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

1.2. Grundsätze der Datenverarbeitung

Bei der Verarbeitung personenbezogener Daten ist von folgenden in Art. 5 DSGVO festgelegten Grundsätzen auszugehen:

- **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**
  Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für den Gast und Mitarbeiter nachvollziehbaren Weise verarbeitet werden. Der Betroffene ist unaufgefordert über den Umfang und die Zwecke der Verarbeitung zu informieren, um eine faire und transparente Verarbeitung zu gewährleisten. Zudem sind die betroffenen Personen über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu informieren und darüber aufzuklären, wie sie ihre diesbezüglichen Rechte geltend machen können (z.B. Datenschutzerklärung auf der eigenen Webseite).
- **Zweckbindung**
  Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (z.B. an die Mailadresse, welche Sie bei der Reservierung erhalten haben, darf nicht ohne weiteres ein Newsletter versendet werden. Ausnahmeregelungen siehe unter Kapitel 5.3.3).
- **Datenminimierung**
  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**
  Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (z.B. Löschung von Gastdaten).
- **Integrität und Vertraulichkeit**
  Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet. Durch geeignete technische und organisatorische Maßnahmen soll auch sichergestellt werden, dass Unbefugte keinen Zugriff auf die Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können (z.B. Benutzerrechte im Hotelreservierungssystem, Zugang zu PCs).

1.3. Rechtmäßigkeit der Datenverarbeitung

Art. 6 DSGVO hält fest, dass jede Verarbeitung personenbezogener Daten in jeder Phase auf Grund des damit verbundenen Eingriffs in das Persönlichkeitsrecht einer Erlaubnis bedarf.

Jegliche Verarbeitung personenbezogener Daten ist grundsätzlich verboten, soweit sie nicht aufgrund **einer der nachfolgenden Ausnahmen** zulässig ist. Das Prüfschema für die Zulässigkeit einer Datenverarbeitung ist daher wie folgt:

1. Werden die Daten zur Erfüllung einer **gesetzlichen Bestimmung** benötigt? (z.B. Gästeverzeichnisblatt).
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.
3. Wenn weder eine gesetzliche Vorgabe noch ein Vertragsverhältnis vorliegt, dann benötigen Sie eine **Einwilligung** (Art. 7 DSGVO) zur Verarbeitung der personenbezogenen Daten (z.B. Anmeldung zum Newsletterservice über die Webseite). Folgende Punkte sind bei einer Einholung der Einwilligung zu beachten:

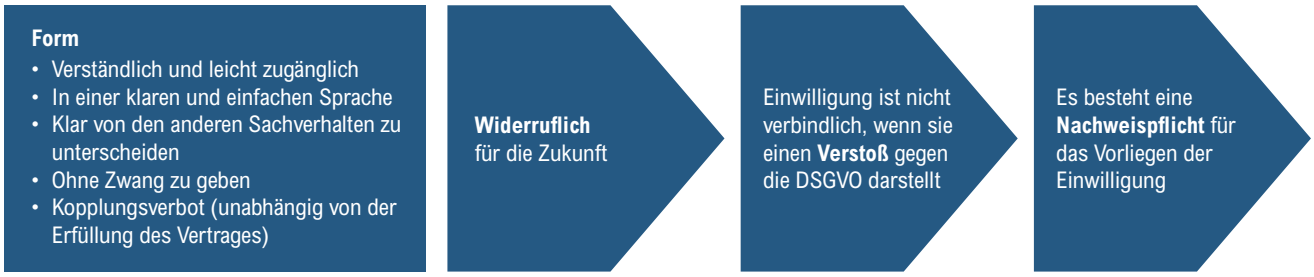


Abbildung 1 | Bedingung der Einwilligung (Art. 7 DSGVO)
Quelle: in Anlehnung an DATAKONTEXT GmbH

4. Sie können zusätzlich personenbezogene Daten verarbeiten, wenn **das überwiegende berechtigte Interesse** des Verantwortlichen oder eines Dritten überwiegt, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person den Schutz personenbezogener Daten erfordern. (Der Hotelier hat darzulegen, wieso die jeweilige Erhebung, Verwendung oder Verarbeitung der Daten erforderlich ist, worin ihre Bedeutung für die Interessenswahrung besteht und welche Interessen dies konkret sind. So ist z.B. eine Videoüberwachung in Umkleiden oder Saunabereichen verboten, da hier die Privatsphäre der Personen dem Schutzbedürfnis des Betreibers überwiegt.)

Vorhandene Einwilligungsklärungen sind zu prüfen, ob diese der DSGVO entsprechen. Ist das nicht der Fall, so sind neue Einwilligungserklärungen einzuholen.

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

HINWEIS | Ist die Verarbeitung personenbezogener Daten nicht 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.

1.4. Datenschutzorganisation und IT-Sicherheit

Die Organisation des Datenschutzes liegt in der Verantwortung des Hoteliers, insbesondere der Hotelleitung und der Geschäftsführung.

Es muss im Hinblick auf die sogenannte Rechenschaftspflicht jederzeit möglich sein, die Rechtskonformität der Verarbeitung sowohl in rechtlicher wie auch in technischer und organisatorischer Sicht nachweisen zu können. Hieraus ergeben sich die unterschiedlichsten Dokumentations- und Nachweisanforderungen, die gemeinsam das sog. Datenschutzmanagementsystem (DSMS) darstellen.

Regelungen hinsichtlich der

- Zuweisung von Zuständigkeiten (Wer ist im Hotel verantwortlich und zuständig?)
- Einsatz datenschutzfreundlicher Technologien (Anforderung an Software, Speicherort, …)
- Durchführung von Kontrollen (Ist-Analyse, Audit, Maßnahmenplan)

Datenschutzrechtliche Dokumentationspflichten (Datenschutzhandbuch) wie:

- Datenschutzrichtlinien (interne Regelungen mit Weisungscharakter für Mitarbeiter im Hotel wie Datenschutz und Datensicherheit im Unternehmen integriert und aufgebaut ist. Mehr dazu im Kapitel 8.2)
- Führen des Verzeichnisses von Verarbeitungstätigkeiten inkl. Zweckbestimmung, Grundlage der Verarbeitung und Durchführung einer Risikobewertung
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Verpflichtung von Dienstleistern im Rahmen der Datenverarbeitung im Auftrag
- Sensibilisierung und Schulung von Mitarbeitern
- Prozesse zur Wahrung der Betroffenenrechte und zum Datenpannenmanagement
- durchzuführende Datenschutz-Folgenabschätzungen
- Beschreibung von technischen und organisatorischen Maßnahmen
- nachweisliche Überprüfung von Datenschutzmaßnahmen

Obige Dokumentations- und Nachweisanforderungen dienen dazu ein Schutzniveau zu gewährleisten, das dem Risiko für die Rechte und Freiheiten der von Personen gespeicherten Daten angemessen, aber auch verhältnismäßig ist. Welche technischen und organisatori-

schen Maßnahmen zu treffen sind, bestimmt der Schutzbedarf der zu speichernden Daten. So ist der Schutzbedarf bei der Speicherung von Bank- und Kreditkartendaten (PCI DSS Normen) wesentlich höher anzusetzen, als beim Speichern von Interessentendaten. Der Schutzbedarf bestimmt den Umfang der Sicherheitsmaßnahmen, wobei der Grundsatz der Verhältnismäßigkeit im Hinblick auf das Risiko und der Eintrittswahrscheinlichkeit anzuwenden ist. Die Bewertung der Verhältnismäßigkeit setzt somit eine Risikobewertung voraus, insbesondere in den Schutzzielen: Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme. So stellt bspw. der Einsatz von Cloud-Technologien anders geartete Anforderungen an Datensicherungsmaßnahmen, als bei herkömmlichen Client-Server Lösungen.

Zur Bestimmung der Sicherheitsmaßnahmen sind nach der DSGVO folgende Schritte erforderlich:

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

1.5. Rechenschaftspflichten durch Dokumentation

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

Tieferstehende Grafik verdeutlicht die Erfüllung der Rechenschaftspflichten durch Dokumentation.

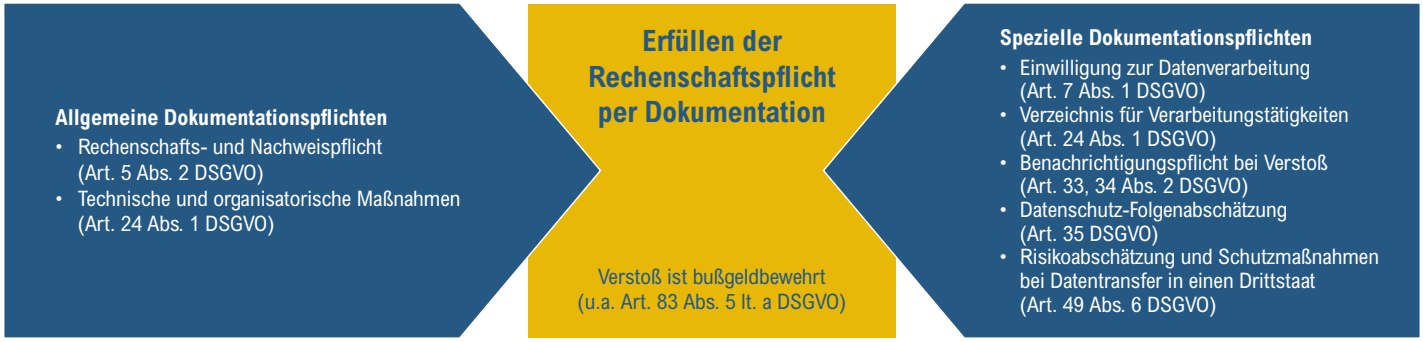


Abbildung 2 | Dokumentationspflichten
Quelle: in Anlehnung an DATAKONTEXT GmbH

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

Als im Detail geregelte Dokumentationspflicht zu nennen ist unter anderem das **Verzeichnis von Verarbeitungstätigkeiten** und das **Verzeichnis für Auftragsverarbeitung**.

Für bestimmte Verarbeitungen ist abhängig von dem Risiko, das mit einer Verarbeitung verbunden ist, vor ihrer Einführung eine **Datenschutz-Folgenabschätzung** durchzuführen.

Bei einem **Datentransfer in einen Drittstaat**, welcher als unsicher gilt, sind die Risikoabschätzung und die ergriffenen Schutzmaßnahmen zu dokumentieren und im Verfahrensverzeichnis aufzuzeigen.

Kommt es zu einem Datenmissbrauch ist dieser der Datenschutzbehörde und den Betroffenen **mitzuteilen**. Dies sowie die ergriffenen Abwehrmaßnahmen sind festzuhalten.

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

1.6. Transparenzvorgaben

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

Die DSGVO enthält erheblich umfangreichere und detailliertere Regelungen zu Informationspflichten als bisher, welche die Transparenz gegenüber den betroffenen Personen herstellen. Von sich aus tätig werden muss der Hotelier bei:

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

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

1.6.1. Allgemeine Informationspflichten

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

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

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

- Name und Kontaktdaten des Datenschutzverantwortlichen bzw. des Datenschutzbeauftragten
- 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 (Siehe dazu Punkt 1.7.)
- 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

Es muss nicht nochmals informiert werden, wenn die betroffene Person über die Informationen bereits verfügt.

Wenn die Daten nicht direkt erhoben werden, so muss die Information nach Art. 14 Abs. 3 DSGVO grundsätzlich innerhalb einer angemessenen Frist, spätestens jedoch nach einem Monat erteilt werden. Werden die Daten allerdings 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.

HINWEIS | Bei Verstößen gegen diese Bestimmung drohen Geldbußen. Wie die Umsetzung in die Praxis erfolgen kann, sehen Sie in den weiteren Kapiteln.

1.6.2. Informationspflicht bei Datenschutzpannen

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 Datenschutzbehörde gemeldet werden. Eine Ausnahme besteht, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten des Betroffenen führt (vgl. Art. 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.

Besonders zu schützende Daten sind gemäß Art. 9 Abs. 1 DSGVO Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit sowie die Verarbeitung von genetischen Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben bzw. der sexuellen Orientierung des Betroffenen.

Auch bei Daten die

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

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

1.7. Rechte der Betroffenen

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

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

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

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

1.7.1. Recht auf Auskunft

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

Auf Verlangen des Betroffenen ist der Hotelier verpflichtet, eine Kopie der personenbezogenen Daten (Datenauszug), die Gegenstand der Verarbeitung sind, unentgeltlich zur Verfügung zu stellen. Das Auskunftsrecht darf Interessen Dritter, wie z.B. das Recht am eigenen Bild (Videoüberwachung) nicht beeinträchtigen. Allerdings darf dem Betroffenen durch die pauschale Berufung auf Rechte Dritter nicht jegliche Auskunft verweigert werden. Sofern sich der Auskunftsanspruch allerdings auf große Datenmengen bezieht, kann der Hotelier verlangen, dass der Betroffene präzisiert, auf welche Informationen oder welche Verarbeitungsvorgänge sich sein Ersuchen bezieht.

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

- die **personenbezogenen Daten**, die den Anfragenden betreffen sowie die **Kategorien** zu der sie gehören (z.B. 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.

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 Einlangen. Handelt es sich um komplexere Begehren kann diese Frist um zwei Monate verlängert werden. Davon ist der Betroffene zu informieren.

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

1.7.2. Recht auf Richtigstellung und Löschung

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

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

- der **Zweck** der Speicherung **weggefallen** ist,
- der Betroffene seine **Einwilligung widerrufen** hat und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt,
- der Betroffene **Widerspruch** gegen die Verarbeitung eingelegt hat und keine vorrangig berechtigten Gründe für die Verarbeitung vorliegen oder
- die Speicherung unzulässig ist.
- Die **Löschungsverpflichtung** bei Wegfall des Zwecks der Datenverarbeitung **entfällt**, sofern satzungsmäßige oder vertragliche **Aufbewahrungsvorschriften** der Löschung entgegenstehen. Eine **Ausnahme** besteht, soweit die Verarbeitung zur **Ausübung der freien Meinungsäußerung** erforderlich ist sowie **Rechtsansprüche** geltend gemacht, auszuüben oder zu verteidigen sind.

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

Auch hier gelten die Fristen wie beim Auskunftsrecht.

1.7.3. Recht auf Einschränkung der Verarbeitung (Sperrung)

Eine Person kann in bestimmten Fällen auch die Einschränkung der Verarbeitung verlangen (Art. 18 DSGVO) – zum Beispiel, wenn das Hotel die Daten nicht mehr länger benötigt, allerdings der Gast zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Die Frist entspricht der Fristsetzung der anderen Betroffenenrechte.

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

Wurde die Verarbeitung auf Antrag eingeschränkt, dürfen diese personenbezogenen Daten – von ihrer Speicherung abgesehen – nur

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

Hebt der Verantwortliche die Einschränkung auf, hat er den Betroffenen im Vorfeld zu informieren.

1.7.4. Recht auf Widerspruch

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

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 personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten. Insbesondere handelt es sich hier um eine Analyse bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, Kaufverhalten, Lebensumstände (Wohnort, Haus oder Mietwohnung, …), aber auch persönliche Vorlieben und Interessen, Zuverlässigkeit u.v.m., um Vorhersagen im zukünftigen Verhalten zu treffen. Der Empfänger von Werbung ist ausdrücklich, in verständlicher Form und getrennt von jeglicher anderen Information auf das Widerspruchsrecht hinzuweisen (Art. 21 Abs. 4 DSGVO).

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

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

1.8. Kontrolle und Rechtsschutz

Die Datenschutzbehörde, Verbraucherverbände (z.B. Konsumentenschutzverband), der Datenschutzbeauftragte, wenn bestellt, aber auch Betriebsräte und der Betroffene selbst kontrollieren die Einhaltung des Datenschutzes.

1.8.1. Das Kontrollsystem

Der **Betroffene** in seiner Eigenschaft als Bürger, Arbeitnehmer, Kunde (Gast), Internetnutzer usw. kontrolliert seine Daten selbst. Dabei erhält er bereits bei der Erhebung seiner Daten oder – soweit die Daten nicht bei ihm erhoben wurden – durch Benachrichtigung durch den Verantwortlichen umfangreiche Kenntnis, insbesondere über Art der verarbeiteten Daten, die Zwecke der Verarbeitung und seine Rechte. Jeder Betroffene hat das Recht seine Betroffenenrechte geltend zu machen. Siehe dazu Kapitel 1.7.

Betroffene können zur Durchsetzung ihrer Rechte „eine Einrichtung, Organisationen oder Vereinigung ohne Gewinnerzielungsabsicht beauftragen in ihrem Namen eine Beschwerde einzureichen“, siehe dazu § 28 DSG.

Der **Datenschutzbeauftragte** – sofern er bestellt bzw. lt. DSG verpflichtend bestellt werden musste.

Die **Datenschutzbehörde** überwacht die Ausführung der DSGVO und des DSG.

Schließlich sind dem **Betriebsrat** durch das Arbeitsverfassungsgesetz (ArbVG) im Bereich Personalwesen ähnliche Überwachungsbefugnisse zugewiesen, wie dem Datenschutzbeauftragten. Der Betriebsrat gestaltet die vom Arbeitgeber gewünschte Verarbeitung maßgebend über Betriebsvereinbarungen mit.

1.8.2. Der Datenschutzbeauftragte

Die DSGVO sieht keine generell verpflichtende Bestellung eines Datenschutzbeauftragten (DB) vor. Das entbindet allerdings nicht die Geschäftsführung, alle datenschutzrechtlichen Anforderungen im Betrieb umzusetzen.

Behörden oder öffentliche Stellen, Unternehmen deren Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine **umfangreiche regelmäßige und systematische Beobachtung** von betroffenen Personen erforderlich macht (z.B. Kreditauskunfteien, Banken, Versicherungen) sowie **Unternehmen, welche eine besondere Kategorie von Daten** verarbeiten (Krankenhausträger, Kurkliniken), müssen einen Datenschutzbeauftragten stellen. **Besondere Kategorien von Daten** sind Daten über die rassische und ethnische Herkunft, Daten über politische Meinung, religiöse, weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung, **Gesundheitsdaten**, Daten zum Sexualleben oder zur sexuellen Orientierung.

Aus dieser Formulierung ist zu schließen, dass in einem Stadthotel oder Ferienhotel kein Datenschutzbeauftragter verpflichtend zu bestellen ist. Allerdings ist in einem Kurhotel, wenn die Kerntätigkeit darin liegt, Gesundheitsdaten zu erfassen, damit eine Behandlung bestmöglich durchgeführt wird und somit die Dienstleistung erbracht werden kann, die Bestellung eines Datenschutzbeauftragten gemäß Art. 37 Abs. 1 lit. c DSGVO verpflichtend durchzuführen.

Als DB kann sowohl ein Mitarbeiter des Unternehmens als auch ein externer Dienstleister bestellt werden. Eine externe Bestellung bringt nicht nur hinsichtlich der Fachkunde und Haftungsfrage, sondern auch in der Transparenz der Kosten Vorteile mit sich. Von Vorteil bei der internen Auswahl ist, dass der eigene Mitarbeiter i.d.R. das Unternehmen mit seinen betrieblichen Abläufen kennt und dieser im Unternehmen bekannt ist.

Aufgabe des DB 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, die für die Umsetzung von technischen und organisatorischen Maßnahmen der DSGVO erforderlich sind, zu unterstützen. Die DSGVO benennt insbesondere folgende Aufgaben:

- Unterrichtung und Beratung hinsichtlich der Datenschutzpflichten des Unternehmens und der Beschäftigten
- Ratgeber für Betroffene (Gäste, Mitarbeiter und Lieferanten) zu allen Fragen der Verarbeitung ihrer Daten und der Wahrnehmung ihrer Rechte Es obliegt ihm eine besondere Verschwiegenheitspflicht über die Identität des Betroffenen, der sich an ihn wendet.

- Überwachung hinsichtlich
  - der Einhaltung der DSGVO und anderer Rechtsvorschriften
  - der „Strategien“ 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

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.

HINWEIS | Es kann jedes Unternehmen freiwillig ein DB bestellen. Hierbei ist jedoch zu beachten, dass bei Bestellung und Benennung eines DB auch die Verpflichtungen anfallen, welche sich aus der DSGVO und dem DSG ergeben. Wenn im Hotel sich jemand des Themas Datenschutz annehmen soll, kann diese Person z.B. auch als Datenschutzkoordinator bezeichnet werden und es sollte eindeutig klargestellt werden, dass diese Person kein DB im Sinne der DSGVO ist.

1.8.3. Die Aufsichtsbehörde

In Österreich fungiert die Datenschutzbehörde (DSB) unabhängig als nationale Aufsichtsbehörde.

Die Aufgaben der DSB ergeben sich unmittelbar aus Art. 57 DSGVO. Die wesentlichsten und für uns relevantesten sind:

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

Die Beratungsaufgabe aus der DSGVO wird mit § 21 DSG konkretisiert und zwar durch die Aufgaben der Beratung des Gesetzgebers, der Vorsprache (Anhörung) bei Gesetzesänderungen die den Datenschutz unmittelbar betreffen, der Erstellung der Liste für die Verarbeitungsvorgänge, für die eine DSFA zu erfolgen hat und der Übermittlung dieser an den Europäischen Datenschutzausschuss.

1.8.4. Instrumente der Selbstregulierung

Neben spezialgesetzlichen Regelungen eröffnet die DSGVO 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.

1.9. Sanktionen bei Datenschutzverstößen

Jede Person hat die Möglichkeit, bei einem vermuteten Verstoß gegen datenschutzrechtliche Bestimmungen und einer damit verbundenen Verletzung eigener Rechte, **Beschwerde bei der DSB** einzulegen (siehe dazu § 24 DSG). 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.

Ein Datenschutzverstoß wird von der DSB nur auf Antrag verfolgt. So kann es lange gut gehen, mit personenbezogenen Daten wissentlich bzw. unwissentlich unsachgemäß umzugehen. 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, die unautorisierte Kontaktaufnahme zu Marketingzwecken sowie überhaupt jegliche Form der rechtswidrigen Datenverarbeitung. Erst wenn es dann zu spät ist, sieht man sich neben möglichen Imageverlusten auch hohen Geldstrafen und Schadenersatzansprüchen gegenüber.

Die Sanktionsbestimmungen der DSGVO richten sich grundsätzlich gegen Verantwortliche bzw. Auftraggeber, also gegen die Unternehmen selbst. Sanktionen gegen natürliche Personen: bei geringfügigen Verstößen oder im Fall einer unverhältnismäßigen Belastung kann anstelle einer Geldbuße eine Verwarnung ausgesprochen werden (Erwägungsgrundsatz 148). Die Geschäftsführung ist verantwortlich und haftet persönlich bei Verstößen gegen die datenschutzrechtlichen Bestimmungen, wenn sie keine Maßnahmen zum Datenschutz getroffen hat.

- Datenschutz dient dem Schutz natürlicher Personen (insbesondere Interessenten, Gäste, Mitarbeiter und Firmenkontakte) bei der Verarbeitung und Übermittlung von Daten, um deren Persönlichkeitsrechte und Privatsphäre zu stärken.
- Von Relevanz sind personenbezogene (bestimmte oder bestimmbare) und identifizierbare Daten natürlicher Personen, die ganz oder teilweise automatisiert verarbeitet oder in Dateisystemen gespeichert werden.
- Betroffenenrechte beinhalten insbesondere das Recht auf Auskunft, Recht auf Richtigstellung und Löschung bzw. Sperrung sowie das Recht auf Widerspruch.
- Kontrollakteure sind der DB/DSK, die Datenschutzbehörde, Verbraucherverbände und ordentliche Gerichte.
- DSB kann Bußgelder bis zu 20 Mio Euro oder 4 Prozent des weltweiten Jahresumsatzes (je nachdem, was höher ist) verhängen. Hinzu kommen evtl. Schadenersatzforderungen und Imageschaden.

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

2. Umgang mit Gast- und Mitarbeiterdaten

ZIELFRAGEN:

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

2.1. Gastdaten

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

2.1.1. Anforderungen an die Hotelsoftware

Die zentrale Speicherung und Verwaltung von Gastdaten erfolgt in der Hotelsoftware. Bei der Suche nach einem guten Hotelmanagement-System sollten neben den hotelspezifischen Funktionalitäten auch immer datenschutzrechtliche Anforderungen berücksichtigt werden. Bereits bei der Auswahl des einzusetzenden Systems sind diese Funktionalitäten durch Sie zu berücksichtigen. Die Durchführung einer Datenschutz-Folgenabschätzung (siehe Kapitel 4.3) dokumentiert unter anderem auch den Entscheidungsprozess, warum Sie sich für eine Hotelsoftware entschieden haben. Folgende Funktionalitäten und gesetzlichen Anforderungen sollten Sie auf jeden Fall prüfen:

1. Kleine Hotels haben andere Anforderungen als Häuser mit 50 oder mehr Zimmern. Während kleine Häuser vielleicht eher ein einfaches, **webbasiertes Hotelverwaltungssystem** einsetzen, arbeiten größere Hotels und Hotelketten mit einem **Property Management System (PMS)**, einer Hotelsoftware für die Zimmerreservierung und Abrechnung von Leistungen und Beeinflussung von Kassensoftware und anderen Peripheriegeräten.

Zunächst ist zu klären, wo sich die Daten befinden. Ist der **Standort der Datenbank/des Systems** direkt im Hotel oder werden die Daten auf Servern von Dienstleistern gehostet? Befinden sich die Daten auf eigenen Servern im Hotel, muss sichergestellt sein, dass sich kein Unbefugter Zutritt und Zugang zu den Servern verschaffen kann. Es sind strenge Anforderungen an die Einrichtung eines Serverraums umzusetzen, um die Vertraulichkeit und Integrität (siehe 1.2.) zu gewährleisten.

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 kann. Ist dennoch eine Datenübermittlung bzw. Datenspeicherung in ein Drittland geplant, so sind die Anforderungen gemäß Art. 46, 47 DSGVO umzusetzen.

2. Eng verbunden mit der Auswahl des Dienstleisters ist auch die Regelung für eine nachfolgende **Betreuung des Hotelmanagement-Systems**, den 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). Nur wenn ausgeschlossen werden kann, dass der Dienstleister keine Möglichkeit hat, die Daten einzusehen (z.B. Verschlüsselung), kann auf eine Datenschutzvereinbarung verzichtet werden.

   HINWEIS | Fragen Sie Ihren Systemanbieter bzw. Hoster nach einer Datenschutzvereinbarung. Sollte er Ihnen keine bereitstellen können, sind das schon die ersten Hinweise darauf, dass der Datenschutz keinen hohen Stellenwert hat. Allerdings ist der Auftragsverarbeiter auch nicht verpflichtet, Ihnen eine entsprechende Vereinbarung zur Verfügung zu stellen. Als Auftraggeber sind Sie dafür verantwortlich, eine Vereinbarung nach den Vorgaben der DSGVO abzuschließen und alle erforderlichen technischen und organisatorischen Maßnahmen, insbesondere bei Wartungsarbeiten, der Vertraulichkeit (Verschlüsselung), der Speicherfristen und ggf. der Datensicherung, festzulegen. Weitere Infos dazu finden Sie im Kapitel 6.

3. **Personenbezogene Daten** sind zu **löschen**, wenn der Zweck der Verarbeitung weggefallen ist. Dem gegenüber stehen oft gesetzliche Aufbewahrungsfristen, die einzuhalten sind. In diesem Fall schreibt der Gesetzgeber vor, dass die Daten zu sperren sind. D.h.

den Zugriff auf Gastdaten spätestens ein Monat nach Abreise (wenn es keine Forderungen mehr seitens des Hotels gibt) auf begrenzte Benutzergruppen (z.B. Reservierung, Buchhaltung, Sales) Systems einzuschränken. Mit einer wiederholten Buchung werden so die Gastdaten wieder aktiviert und eine Gästehistorie aufgebaut, bis dahin haben aber das Front Office, Housekeeping etc. keine Möglichkeit, die Gastdaten abzurufen.

HINWEIS | 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.

Gastdaten sind auch dann regelmäßig zu löschen, wenn Gäste z.B. nicht angereist sind und es keine Verpflichtung gibt, diese aufzubewahren (z.B. weil es keinen steuerrechtlichen Vorgang gab). Sind steuerrechtliche Aufbewahrungsfristen zu berücksichtigen, sind die Gastdaten spätestens nach 7 Jahren zu löschen.

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

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

   Eine **gemeinsame Nutzung von personenbezogenen Daten** setzt voraus, dass eine Vereinbarung auf Grundlage von Art. 26 DSGVO zwischen den Verantwortlichen getroffen wird, da sie gemeinsam für die Verarbeitung verantwortlich sind. Es gibt kein Konzernprivileg!

   HINWEIS | Der Gast ist bei der ersten Buchung darüber zu informieren, dass mehrere Hotels auf seine Daten zugreifen können. Er ist auf sein Widerspruchsrecht hinzuweisen. In Fall eines Widerspruchs ist maßgeblich, 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 den Positionen und Abteilungen 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.

HINWEIS | Für jeden Mitarbeiter ist ein eigener Zugang mit entsprechenden Zugriffsrechten einzurichten. Die Vergabe, Änderung und Deaktivierung der Benutzerrechte sowie die Löschung nach 7 Jahren ist für jeden Benutzer in der Hotelsoftware zu dokumentieren.

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.

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

PRAXISTIPP | Es ist davon auszugehen, dass Sie als Hotelier bereits über ein Hotelmanagement-System verfügen. Auch in diesem Fall sollten Sie mindestens die 6 genannten Punkte prüfen und umsetzen. Setzen Sie sich mit Ihrem Systemanbieter in Verbindung und klären Sie die Punkte gemeinsam mit ihm. Auch er ist dazu verpflichtet, gemäß Art. 25 DSGVO eine datenschutzfreundliche Anwendung bereitzustellen.

2.1.2. Reservierung

Bereits bei der Reservierung erhält das Hotel umfangreiche Daten über den Gast. Die Daten, die über die unterschiedlichsten Kommunikationskanäle zum Hotel gelangen, sind zumeist Namen, Anschrift, Kontaktdaten, Kreditkartennummern und Wünsche. Alle Informationen werden in die Hotelsoftware übernommen, zum Vorgang erhaltene oder ausgedruckte Unterlagen werden zusätzlich in Reservierungsordnern abgelegt. Anfragen über E-Mail werden 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 (Aus-

kunft, Berichtigung, Löschung, Widerspruch, Datenübertragbarkeit sowie Beschwerderecht bei der Datenschutzbehörde) 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) zu integrieren. Nähere Information zur Datenschutzerklärung finden Sie im Anhang.

TEXTBEISPIEL

Informationen zur Erhebung und Verarbeitung meiner personenbezogenen Daten habe ich der Datenschutzerklärung entnommen.

HINWEIS | Wenn das Onlinereservierungssystem von einem Dienstleister integriert und betrieben wird, ist eine Datenschutzvereinbarung zwischen Hotel und Dienstleister abzuschließen. Reservierungsdaten im Onlinereservierungssystem sollten zeitnah gelöscht werden.

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

2. Für Reservierungen über **Hotelreservierungsportale (OTAs)** gilt: Auch wenn der Betreiber des jeweiligen Systems selber für die Umsetzung der datenschutz- und datensicherheitstechnischen Anforderungen verantwortlich ist, muss das Hotel 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.

   HINWEIS | 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.

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

4. Zu beachten sind die **Informationspflichten nach Art. 14 DSGVO**, wenn der Buchende nicht direkt bei der Erhebung seiner Daten informiert werden konnte. Das ist dann der Fall, wenn die Buchung über ein Hotelreservierungsportal, über ein Reisebüro, per E- Mail, Fax, Telefon etc. erfolgte. Sofern die Buchungsdaten in das Hotelmanagementsystem

übernommen werden, ist der Buchende über die Datenspeicherung und -nutzung (siehe dazu Kapitel 1) 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), ist der Gast über seine Datenspeicherung z.B. im Rahmen einer Pre Stay E-Mail zu informieren. Bei Kenntnis von Adressdaten kann der Gast auch per Post angeschrieben und informiert werden.

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

2.1.3. Check-In und Gästeverzeichnisblatt

Mit dem Einchecken werden alle offenen Fomalitäten erledigt. Der Gast füllt sein Gästeverzeichnisblatt aus und bezahlt eventuell schon vorab sein Zimmer bzw. werden Zahlungsdaten, wie seine Kreditkartennummer aufgenommen. Überlegen Sie sich rechtzeitig, welche Gastdaten Sie über die Erfüllung des Beherbergungsvertrages hinaus verarbeiten möchten und daher eine Einwilligung durch den Betroffenen benötigen. Im zweiten Schritt prüfen Sie, zu welchem Zeitpunkt die Einwilligung eingeholt werden kann (z.B. bei der Reservierung oder bei Check-In) und ob mehrere Verarbeitungszwecke auf einem Einwilligungsblatt eingeholt werden können (z.B. Newsletter, aber auch die Speicherung von sensiblen Daten). Soweit dieses auf dem Meldeschein vorgesehen ist, sind diese separat und unabhängig von den Meldedaten einzuholen.

TEXTBEISPIEL für eine Einwilligungserklärung für einen Newsletterversand

☐ Ich bin an Angeboten und Neuigkeiten vom Hotel xxx interessiert und erkläre mich damit einverstanden, Informationen und Werbung für Angebote, Produkte und Dienstleistungen per E-Mail zu erhalten. Ich stimme zu, dass die dafür erforderlichen Daten, nämlich mein Name und meine E-Mail-Adresse zu diesem Zweck verarbeitet werden.

Meine Einwilligung kann ich jederzeit und ohne Angabe von Gründen per E-Mail an xxx (und/oder über einen in den elektronischen Zusendungen enthaltenen Link und/oder telefonisch unter +xxx widerrufen. Meine Daten werden über Anforderung oder nach Einstellung des Newsletter Services für diesen Verwendungszweck gelöscht.

Das Front Office hat darauf zu achten, dass die Unterlagen nach ihrer Bestimmung getrennt und sicher aufbewahrt werden. Insbesondere ist auf eine Trennung nach Gästeverzeichnisblatt, Reservierungsunterlagen und Abrechnungsunterlagen (Rechnung inkl. Händler-

beleg) zu achten. Wenn die **Händlerbelege** Angaben zu den Kontodaten des Gastes (z.B. Kreditkartennummer) enthalten, sind diese verschlossen aufzubewahren. Es empfiehlt sich die Anonymisierung der Kreditkartendaten auch auf dem Händlerbeleg.

Der Hotelier ist weder berechtigt noch verpflichtet, die Angaben des Gastes zu kontrollieren. **Es gibt daher keine gesetzliche Grundlage, die dem Hotel gestattet Kopien von Personalausweisen** der Gäste anzufertigen und einzubehalten.

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

Es besteht die Möglichkeit, das Gästeverzeichnisblatt auch in elektronischer Form zu führen. Die Gästedaten können in ein elektronisches Gästeverzeichnis durch einscannen, durch elektronisches Erfassen der Meldedaten und Übernahme der elektronisch erfassten Unterschrift (Unterschriftspad) oder durch elektronische Einbringung mit qualifizierter elektronischer Signatur eingebracht werden. Der Hotelier hat organisatorisch sicherzustellen, dass auch bei einem elektronischen Gästeverzeichnis die erforderlichen Daten von ausländischen Gästen vollständig erfasst werden (insbesondere Nummer, Ausstellungsbehörde, Ausstellungsdatum sowie Staat der Ausstellung des Reisedokumentes).

HINWEIS | Wird ein Gästeverzeichnis automationsunterstützt geführt, hat der Hotelier sicherzustellen, dass geeignete, dem jeweiligen Stand der Technik entsprechende Vorkehrungen getroffen werden, um einen Zugriff von Unberechtigten zu verhindern. Das Gästverzeichnisblatt bzw. automationsunterstützt verarbeitete Daten sind 7 Jahre aufzubewahren bzw. zu speichern und dürfen darüber hinaus solange aufbewahrt werden, als dies zur Erfüllung gesetzlicher Verpflichtungen notwendig ist. Danach sind sie zu löschen bzw. datenschutzkonform zu vernichten.

PRAXISTIPP | Möchten Sie gleich am selben Blatt und im Zusammenhang mit der Datenerhebung für das Gästeverzeichnisblatt über die Pflichtangaben weitere personenbezogene Daten der Gäste erheben (z.B. E-Mail-Adresse, KFZ-Kennzeichen für Garage), so sind diese Felder klar vom Gästeverzeichnisblatt abzugrenzen. Es muss für den Gast erkennbar sein, dass es sich um eine „freiwillige“ Angabe handelt.

2.1.4. Kreditkartendaten

Kreditkartendaten sind vom Gesetzgeber (Erwägungsgrund 75 DSVGO) als besonders vertrauenswürdig eingestuft worden. Von daher empfiehlt es sich, feste Vorgaben im Umgang mit den Kreditkartendaten festzulegen und die Mitarbeiter regelmäßig zum Umgang zu belehren. Insbesondere ist darauf zu achten, dass:

- Kreditkartendaten nach Abreise des Gastes gelöscht werden. (spätestens nach 30 Tagen, im Onlinereservierungssystem 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, …)

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

2.1.5. Aufenthalt

Das Hotel erfährt 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 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 erfolgte. (Siehe dazu untenstehend „Aufnahme von Gastwünschen und Informationen in die Hotelsoftware“.)

Videoüberwachung

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

HINWEIS | Mehr zur Videoüberwachung finden Sie im Kapitel 7.

Elektronische Türschließsysteme

Das elektronische Türschließsystem dient in erster Linie als „Schlüsselersatz“ zum Betreten von Hotelzimmern und anderen nichtöffentlichen Bereichen im Hotel. Die Programmie-

rung 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 nicht 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.

Internetnutzung

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

Der Geschäftsführer haftet allerdings für eigenes Fehlverhalten und für das seiner Mitarbeiter.

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 bestimmte Zeitung am Frühstückstisch bis hin zu sensiblen Daten, wie z.B. Allergien. Um den Beherbergungsvertrag erfüllen zu können, können diese Daten verarbeitet werden. Wenn sensible Daten allerdings in der Hotelsoftware über den Aufenthalt hinaus gespeichert werden sollen dann ist hierfür eine ausdrückliche Zustimmung vom Gast einzuholen. Dies kann bereits im Rahmen der Reservierung über Ihr Buchungsportal geschehen, per E-Mail bei der Übermittlung der Reservierungsbestätigung oder dann direkt vor Ort beim Check-In.

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

2.1.6. 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 der Hotelier die E-Mail-Adresse für eine Online-Befragung einholen. Die Befragung sollte zeitnah erfolgen, also innerhalb von 14 Tagen nach Abreise.

Der Hotelier hat eine ordnungsgemäße Aufbewahrung von Gästeverzeichnisblattsammlung und Reservierungsunterlagen in dafür geeigneten Archivräumen sicherzustellen. Gerade in den Reservierungsunterlagen sind oft sensible Daten wie Kreditkartennummern abgelegt. Ein vertraulicher Umgang muss gewährleistet werden, Aufbewahrungsfristen sind zu berücksichtigen. Alle Unterlagen sind nach Ablauf der Aufbewahrungsfristen datenschutzgerecht zu vernichten.

HINWEIS | Sofern die Reservierungsunterlagen elektronisch abgelegt werden, gelten dieselben Anforderungen wie bei der Reservierungsakte, insbesondere stark eingeschränkte Zugriffsrechte auf die Unterlagen und Archivierung (weitere Einschränkung der Zugriffsrechte = Sperrung) nach Abreise.

- Die Hotelsoftware ist der zentrale Speicherort für Gastdaten. Mit der DSGVO werden zahlreiche datenschutzrelevante Forderungen (datenschutzfreundliche Software) an die eingesetzte Software gestellt, die umzusetzen sind.
- Kreditkartendaten gelten als streng vertraulich, entsprechend ist mit ihnen umzugehen.
- Die Meldepflicht ist gesetzlich geregelt und für den Hotelier daher verpflichtend durchzuführen.
- Es gibt keine gesetzliche Erlaubnis, Personaldokumente zu kopieren.
- Es erfolgt keine Haftung für die Internetnutzung durch den Gast, jedoch bei den Mitarbeitern.

- *Überprüfung der Hotelsoftware. Werden alle datenschutzrechtliche Belange umgesetzt?*
- *Wie sicher sind die Kreditkartendaten?*
- *Überprüfung der Umsetzung der Meldepflicht im Hotel. Gibt es einen Standard?*
- *Wie informiere ich den Gast formgerecht über die Speicherung und Verarbeitung seiner Daten?*

2.2. Mitarbeiterdaten

ZIELFRAGEN:

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

Unter dem Stichwort Beschäftigten- oder Arbeitnehmerdatenschutz werden Regelungen zusammengefasst, die sich speziell mit der Erhebung, Verarbeitung und Nutzung von Arbeitnehmerdaten bzw. Daten im Zusammenhang mit einem Beschäftigungsverhältnis befassen.

Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verwendet 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.

Jeder Arbeitnehmer hat einen **Anspruch auf den Schutz seines Persönlichkeitsrechts**.

Durchführung des Beschäftigungsverhältnisses

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

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

Der Hotelier darf aber auch Mitarbeiterdaten erheben, speichern und nutzen, um seine Rechte im Zusammenhang mit dem Beschäftigungsverhältnis wahrnehmen zu können. Dazu gehören **Kontrollen zu Leistung und Verhalten des Beschäftigten** ebenso wie In-

formationen 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 Hotelier darf alle zur Beendigung erforderlichen bzw. damit im Zusammenhang stehenden Mitarbeiterdaten erheben und speichern. Dazu gehören auch alle Daten im Zusammenhang mit einer Kündigung wie Abmahnungen oder Beweismittel zur Begründung einer Kündigung und im Falle eines Rechtsstreites auch alle im Zusammenhang mit der Durchführung des Rechtsstreits anfallenden Daten und Unterlagen.

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

Grundsatz der Erforderlichkeit

Mitarbeiterdaten dürfen verwendet werden, wenn dies erforderlich ist. Grundsätzlich dürfen nicht mehr Daten verarbeitet werden, als zur Erfüllung der jeweiligen Aufgabe benötigt werden. Dieses Gebot ergibt sich aus dem **Grundsatz der Datenvermeidung und Datensparsamkeit**. Es dürfen auch keine Daten auf Vorrat erhoben werden.

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

Informationspflichten bei der Datenerhebung

Mit der Datenerhebung und -speicherung ist der Mitarbeiter gemäß Art. 13 DSGVO über die Identität der verantwortlichen Stelle (i.d.R. das Hotel als Arbeitgeber), die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung, die Löschfristen und bei Datenübermittlungen auch über die Kategorien von Empfängern (z.B. Krankenkasse, Bankinstitut, Lohnverrechnung wenn extern durchgeführt wird) 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 beim Bewerbungsprozess in verkürzter Form und dann bei der Einstellung des Mitarbeiters nachkommen.

Arbeitnehmerdaten in nichtautomatisierten Verfahren und Dateien (Akten)

Das Datenschutzgesetz ist auch anzuwenden, wenn im Rahmen eines Beschäftigungsverhältnisses personenbezogene Daten aus einer nicht automatisierten Datei erhoben, verarbeitet oder genutzt werden. Damit ist klargestellt, dass die **Personalakten**, unabhängig von der technisch-organisatorischen Form und dem Aufbau der Personalakten immer den Vorschriften des Datenschutzgesetzes unterliegen. Werden im Rahmen eines **Bewerbungsverfahrens** vom Bewerber Informationen erfragt und manuell festgehalten oder bei der Einstellung ein Personalfragebogen ausgefüllt, fallen diese Unterlagen ebenfalls unter den Schutzbereich des Datenschutzgesetzes.

2.2.1. Bewerbung

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

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

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

Die Zulässigkeit der **Web-Recherche** wird unterschiedlich beurteilt. Einerseits wird argumentiert, dass diese Daten allgemein zugänglich zur Verfügung stehen, in aller Regel sogar von den Betroffenen selbst eingestellt worden sind und deshalb vom Arbeitgeber unter Beachtung des Erforderlichkeitsprinzips auch abgefragt werden dürfen.

Wir empfehlen, eine Web-Recherche zur Beschaffung von Zusatzinformationen über den Bewerber nicht durchzuführen. Der Bewerber soll, wenn er sich in ein Anbahnungsverhältnis begibt, soll sich 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 zurückzugeben oder datenschutzgerecht zu vernichten. Soweit Bewerbungen elektronisch gespeichert sind, ergibt sich eine Löschungsverpflichtung aus dem Datenschutzgesetz.

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

Auch bei **Initiativbewerbungen** erscheint eine Speicherfrist von bis zu sechs Monaten als sachgerecht. Anders wäre es, wenn der Bewerber erklärt hat, mit einer längeren Speicherung einverstanden zu sein, bis das Unternehmen für ihn eine geeignete Stelle gefunden hat.

Eine Weiterleitung von Bewerbungen (z.B. innerhalb von konzernangehörigen Unternehmen) an eine Schwestergesellschaft oder an die Muttergesellschaft ist nur mit Einwilligung des Bewerbers zulässig. Sollte eine derartige Weiterleitung oder eine gewünschte längere Aufrechterhaltung der Bewerbung für zukünftige Stellen in Frage kommen, kann die Einholung der Einwilligung mit dem Ablehnungsschreiben verbunden werden. Ansonsten wird je nach Speicherungsform seine Bewerbung nach Ablauf der nach dem GlBG angemessenen Frist gelöscht, vernichtet oder zurückgegeben.

TEXTBEISPIEL

„Ihr Einverständnis vorausgesetzt würden wir gerne Ihre Bewerbungsunterlagen für weitere Stellenausschreibungen in Evidenz halten. 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.“

2.2.2. Personalakte

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

Die Führung der Personalakten wird von folgenden Grundprinzipien bestimmt:

- Vertraulichkeit der Personalunterlagen
- Richtigkeit und Vollständigkeit
- Zulässigkeit und Zweckbindung der Informationen
- Transparenzgrundsatz

Personalakte 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**.

Wenn Sie **sensible Daten** (Gesundheitsdaten, Gewerkschaftszugehörigkeit, Religionsbekenntnis) von Arbeitnehmern erfassen, beachten Sie, dass der Zugriff nur besonders befugten Personen erlaubt ist. Keinesfalls dürfen ärztliche Zeugnisse oder sonstige Unterlagen mit Informationen über die gesundheitlichen Verhältnisse des Mitarbeiters ungeschützt in der Personalakte abgelegt werden.

Richtigkeit und Vollständigkeit der Personalakten

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

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

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

Inhalt und Aufbewahrungsdauer

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.

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 **Aufbewahrungsfristen von 7 Jahren**. Für die sonstigen Unterlagen richtet sich die Dauer der Aufbewahrung sowohl bei elektronisch gespeicherten Daten als auch bei manuell geführten Daten nach den Vorschriften der DSGVO.

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.

Für die **Zeit nach dem Ausscheiden eines Beschäftigten** existiert ebenfalls keine Aufbewahrungsvorschrift. In Verbindung mit dem Austritt 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, sind ebenfalls bis zum Ablauf von etwaigen Fristen (z.B. § 1478 ABGB Anspruch auf Ausstellung eines Dienstzeugnisses 30 Jahre mit Fristbeginn bei Beendigung des Dienstverhältnisses) aufzubewahren. 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 7 Jahren gilt i.d.R. als ausreichend, kann aber z.B. auch abhängig vom Alter der Betroffenen länger gestaltet werden.

Recht auf Einsichtnahme

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

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

2.2.3. Elektronisches Personalaktenarchiv

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

Zugriffsschutz

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

- uneingeschränkter Zugriff auf alle Unterlagen, z.B. für die Betroffenen
- eingeschränkter Zugriff auf ausgewählte Unterlagen, z.B. für die Fachvorgesetzten
- u.U. Differenzierung der Zugriffsberechtigungen auf Teile der Personalakte, z.B. für Personalsachbearbeiter mit bestimmten Teilzuständigkeiten (Lohnabrechnung, disziplinar- oder arbeitsrechtliche Angelegenheiten etc.)
- sensiblen Daten müssen zusätzlich geschützt werden können

Verknüpfung von Dokumenten

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

Löschung oder Sperrung von Dokumenten

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

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

Protokollierung von Zugriffen

Aufgrund der besonderen Vertraulichkeit von Personalunterlagen sollten die Zugriffe auf die Unterlagen vom System protokolliert werden. Das Datenschutzgesetz verlangt hierzu, dass nachträglich festgestellt werden kann, von wem welche Daten in das System eingegeben, verändert oder entfernt worden sind. Die Dokumentation des Systems sollte deshalb ein Konzept enthalten, das die Protokollierungen nachprüfbar beschreibt.

Weitergabekontrolle

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

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

Zugriffsmöglichkeiten durch Administratoren

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

Information der Betroffenen

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

Mitbestimmung Betriebsrat

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 Einzelvereinbarung abzuschließen.

2.2.4. Arbeitsvertrag

Mit Abschluss des Arbeitsvertrages ist der Mitarbeiter über die Dauer des Arbeitsverhältnisses hinaus auf das **Datengeheimnis** zu verpflichten (Art. 32 Abs. 4 DSGVO, § 6 DSG). Neben dem Verantwortlichen und einem Auftragsverarbeiter haben auch Mitarbeiter personenbezogene Daten, die ihnen auf Grund ihrer beruflichen Tätigkeit anvertraut worden sind, geheim zu halten. Es empfiehlt sich, diese Verpflichtung im Arbeitsvertrag anzuführen. Aus der Verpflichtung zum Datengeheimnis ergibt sich die **Pflicht zu Schulungen** (Art. 39 DSVGO).

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

2.2.5. Lohnabrechnung

Beauftragt der Hotelier eine externe Lohnverrechnung, so unterliegt die Beauftragung des Dienstleisters der Datenverarbeitung im Auftrag (siehe Kapitel 6). Entsprechend ist der Dienstleister zu prüfen und es ist eine Datenschutzvereinbarung abzuschließen. In der Datenschutzvereinbarung sind technische und organisatorische Maßnahmen festzulegen, die den Schutz der Mitarbeiterdaten betreffen. Insbesondere sind Maßnahmen für eine sichere Datenübermittlung, z.B. per E-Mail (Verschlüsselung) zu treffen.

2.2.6. Zustimmungspflichtige Maßnahmen

Durch den Arbeitsvertrag ergibt sich das Recht des Dienstgebers auf Kontrolle der Einhaltung der arbeitsrechtlichen Pflichten des Arbeitnehmers. Das Recht der Kontrolle ist nicht uneingeschränkt. Gemäß § 96 ArbVG unterliegen Verfahren, die zu einer Leistungs- und Verhaltenskontrolle von Mitarbeitern geeignet sind sowie deren Persönlichkeitsrechte einschränken können, dem Mitbestimmungsrecht, also der Zustimmung durch den Betriebsrat. Die Regelungen werden in Betriebsvereinbarungen festgelegt, der Betriebsrat gibt seine Zustimmung im Namen aller Mitarbeiter.

Ist in einem Hotel kein Betriebsrat vorhanden, so ist vor der Implementierung von Kontrollmaßnahmen (Videoüberwachung, Zutrittskontrollsystem) die Zustimmung der betroffenen Arbeitnehmer einzuholen (§ 10 AVRAG). Die Zustimmung sollte schriftlich und befristet, mit Hilfe von Einverständniserklärungen und Nutzungsvereinbarungen, für einen bestimmten Zeitraum eingeholt werden.

2.2.7. E-Mail und Internetnutzung am Arbeitsplatz

Wenn keine Nutzungsregelung in einer Betriebsvereinbarung, einem Arbeitsvertrag oder durch Anweisung des Arbeitgebers vorhanden ist, so ist von einer erlaubten, auf das für den Arbeitgeber zumutbare Ausmaß reduzierten Nutzung auszugehen. Darunter ist zu ver-

stehen, dass die Arbeit nicht beeinträchtigt werden darf, die technischen Ressourcen dürfen nicht belastet werden, es darf kein zusätzliches Sicherheitsrisiko geschaffen werden und es dürfen keine widerrechtlichen Handlungen (z.B. Kinderporno) unterstützt werden.

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

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

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

- Alle Informationen, die einem einzelnen Arbeitnehmer zugeordnet werden können, sind personenbezogene Daten.
- Bezüglich des Inhalts von Personalakten sind alle Mitarbeiter nach einheitlichen Grundsätzen zu behandeln. Die in der Personalakte gesammelten Daten müssen objektiv, richtig und vollständig sein.
- Inhalte, die den Betroffenen belasten, müssen aus der Personalakte entfernt werden, sobald der Grund für die Aufnahme entfallen ist und diese für die Zukunft nicht mehr erforderlich sind (z.B. Abmahnungen).
- Es ist unzulässig, neben den als offizielle Personalakte definierten Unterlagen weitere Personalakten zu führen, die dem betroffenen Mitarbeiter nicht zugänglich sind.
- Bei komplexen Personalaktenstrukturen, die für den Betroffenen nicht erkennbar sind (z.B. bei mehreren Teil- oder Nebenakten, Verteilung auf verschiedene Standorte oder Vorgesetzte), sollte ein Personalaktenverzeichnis angelegt und dem Beschäftigten bei der Einsichtnahme zugänglich gemacht werden.
- Im Bewerbungsverfahren dürfen nur Fragen gestellt werden, die nach objektiven Maßstäben zur konkreten Entscheidung über die Bewerbung erforderlich sind. Fragen, die erst zum Vertragsabschluss relevant werden, sind unzulässig (z.B. Fragen zur Religionszugehörigkeit).

- Kommt es nicht zur Einstellung, können die erhobenen Bewerbungsdaten bis zu sechs Monate nach Ablehnung der Bewerbung vorgehalten werden.
- Bei Anwendungen, die eine Leistungs- und Verhaltenskontrolle des Mitarbeiters ermöglichen, sind Informationspflichten und Mitbestimmungsrechte zu beachten.
- Die Nutzung von Kommunikationsmedien durch Mitarbeiter im Hotel ist zu regeln, anderenfalls ist alles erlaubt. Das kann zum Nachteil des Hoteliers in seinen Kontrollrechten führen.

- *Ist der Arbeitnehmerdatenschutz ein fester Bestandteil unserer Datenschutzorganisation?*
- *Haben wir Regelungen im Umgang mit Personaldaten, insbesondere der Datenspeicherung und -nutzung sowie im Umgang mit der Personalakte?*
- *Haben wir mit unserer externen Lohnverrechnung eine Datenschutzvereinbarung abgeschlossen? Die Tätigkeiten unterliegen nicht der Verschwiegenheitspflicht eines Steuerberatungsbüros.*
- *Werden Mitarbeiter bei der Ausübung ihrer Tätigkeit in ihren Persönlichkeitsrechten eingeschränkt?*
- *Sind Regelungen zur privaten Nutzung von E-Mail und Internet vorhanden?*

3. 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.

ZIELFRAGEN:

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

3.1. Gast

Wird eine Auskunftsanfrage an eine Abteilung im Hotel gestellt, so ist innerhalb von einem Monat bzw. innerhalb von weiteren zwei Monaten bei komplexeren Angaben Auskunft zu erteilen. Dabei ist auf dem Umfang entsprechend Art. 15 DSGVO (siehe hierzu auch Kapitel 1.7.1 Recht auf Auskunft) Bezug zu nehmen. Die Auskunft ist schriftlich (in Briefform oder in Ausnahmefällen per E-Mail, nicht per Fax) und unentgeltlich zu erteilen. Sie ist direkt an den Betroffenen zu richten.

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

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

3.2. Behörde

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.

Die Weitergabe von Informationen über den Betroffenen **ohne** Rechtsgrundlage erfordert das **Einverständnis des Betroffenen** oder eine **gerichtliche Anordnung** und ist anlassbezogen direkt beim Betroffenen schriftlich einzuholen.

HINWEIS | Der Meldebehörde und den Organen des öffentlichen Sicherheitsdienstes muss auf Verlangen jederzeit in das Gästeverzeichnis Einsicht gewährt werden. Bei automationsunterstützter Verarbeitung sind auf deren Verlangen schriftliche Ausfertigungen aus dem Gästeverzeichnis zu übergeben oder die Daten elektronisch zu übermitteln.

3.3. Sonstige Dritte

Für alle anderen Unternehmen aus dem nichtöffentlichen Bereich (wie Verbände, Versicherungen, Anwälte…) oder Personen (Dritte), die Auskünfte über Informationen eines Betroffenen (insbesondere Gast oder Mitarbeiter) erhalten wollen, gibt es grundsätzlich keine Rechtsgrundlage zur Weitergabe von personenbezogenen Daten. Für die Weitergabe von Informationen über Betroffene bedarf es des Einverständnisses des Betroffenen. Diese ist anlassbezogen (Einverständniserklärung oder Schweigepflichtentbindungserklärung) direkt beim Betroffenen schriftlich einzuholen. Die Privatsphäre ist zu wahren!

Beispiele hierfür können sein:

- Ein Gast erkundigt sich über 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.

HINWEIS | Erhält die Rezeption eine telefonische oder persönliche 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:

„Entschuldigen Sie bitte, aber aus datenschutzrechtlichen Gründen darf ich Ihnen keine Auskünfte über unsere Gäste erteilen. Sie haben doch sicherlich eine Handynummer, über die Sie die Person erreichen können.“

- Bei der Auskunftspflicht zu Gastdaten ist zwischen den in der Hotelsoftware gespeicherten Daten, wie Adress- und Kontaktdaten, Gästehistorie oder Rechnungen zu unterscheiden. Meldedaten sind der Meldebehörde und den Organen des öffentlichen Sicherheitsdienstes über das Gästeverzeichnis jederzeit zugänglich zu machen. Die Herausgabe von Gästelisten, in der Hotelsoftware gespeicherte Daten bis hin zur Videoüberwachung im Rahmen der Aufklärung von Straftaten bedürfen i.d.R. einer richterlichen Anordnung.
- Der Meldeschein ist auf Verlangen den zuständigen Behörden vorzulegen.
- Geben Sie keine telefonische Auskunft über Gäste.

- *Überprüfung des Umgangs der Auskunftspflicht im Hotel. Werden alle rechtlichen Belange erfasst? Gibt es dafür einen Standard?*
- *Wie gehen wir mit Auskunftsanfragen um?*

4. Verzeichnis von Verarbeitungstätigkeiten

ZIELFRAGEN:

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

Durch die DSGVO ist eine Registrierung von meldepflichtigen Datenverarbeitungen beim Datenverarbeitungsregister (DVR) nicht mehr erforderlich. Das DVR, welches zur Datenschutzbehörde (DSB) gehörte, ist nicht mehr existent.

Aus dem DVR wurde das Verzeichnis von Verarbeitungstätigkeiten (VVT) gemäß Art. 30 DSGVO. Das VVT ist ein eigenes Verzeichnis, in welchem die Datenanwendungen, die im Unternehmen anfallen, aufgelistet und erläutert sind. Die DSB kann die Vorlage des VVT jederzeit verlangen.

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

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

Die DSGVO sieht zwar eine Ausnahme für Unternehmen mit weniger als 250 Mitarbeiter vor, allerdings geht diese Ausnahmeregelung ins Leere. Spätestens bei Zugrundelegung einer regelmäßigen Verarbeitung, der Verarbeitung von Beschäftigtendaten, Videoüberwachung bzw. Kreditkartendaten ist der Hotelier unabhängig von seiner Mitarbeiterstärke betroffen und hat demnach ein VVT zu führen.

Das Verzeichnis ist zentraler Bestandteil der Datenschutzdokumentation.

Das VVT kann auch als Grundlage für Risikobewertungen durch den DB/ DSK und unterstützt den DB/DSK bei seinen Beratungs- und Kontrollpflichten.

4.1. 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 des Verantwortlichen 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
- ggf 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 Unterabs. 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

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

4.2. Muster

Hotels, die ihre Datenverarbeitung beim DVR gemeldet haben, wie es im DSG 2000 gesetzlich verankert war, wird die Erstellung des VVT leichter fallen. Es sollte daher zuerst geprüft werden, inwieweit die bisher geführten Verarbeitungen gemeldet sind. Die daraus gewonnenen Informationen sind dann mit den Anforderungen des Art. 30 DSGVO abzugleichen und entsprechend zu ergänzen.

Im Falle von fehlender Datenschutzdokumentation muss zunächst ermittelt werden, in welchen Fällen personenbezogene Daten von z.B. Gast- und Interessentendaten, Lieferanten

oder Beschäftigten erhoben und verarbeitet werden. Hierzu bietet es sich als ersten Anhaltspunkt an, alle innerhalb des Hotels bestehenden Anwendungen 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. Hotelbuchung, Gastronomie, Wellness, Rechnungswesen, etc., …) bestehen.

HINWEIS | Jedes Verfahren muss separat aufgeführt werden. Hierzu können im **Muster zum Verzeichnis von Verarbeitungstätigkeiten (siehe Anhang)** die Anlagen in fortlaufender Nummerierung genutzt werden.

4.3. Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung (DSFA) wird in Art. 35 DSGVO geregelt. Eine DSFA ist immer dann durchzuführen, wenn besonders sensible Daten verarbeitet werden oder die Datenverarbeitung dazu bestimmt ist, die Persönlichkeit des Betroffenen, einschließlich seiner Fähigkeiten, Leistungen oder seines Verhaltens zu bewerten und dient also der Bewertung von Risiken und deren mögliche Folgen für die persönlichen Rechte und Freiheiten der Betroffenen.

Nach Art. 35 Abs. 1 DSGVO ist eine DSFA 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 Abs. 1 oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10
- systematische weiträumige Überwachung öffentlich zugänglicher Bereiche

Von der DSB wurde eine Liste von Verarbeitungstätigkeiten erstellt, für die eine Erstellung einer DSFA gesetzlich nicht erforderlich ist. Details finden Sie dazu in der DSFA-Ausnahmeverordnung (DSFA-AV). Auch wurde von der DSB eine Liste mit Verarbeitungsvorgänge erstellt, für die auf alle Fälle eine DSFA erforderlich ist. Mehr dazu finden Sie unter der DSFA-V.

Die DSFA-AV und DSFA-V sind keine abschließenden Aufzählungen, sondern diese führen nur Verarbeitungsvorgänge an, die jedenfalls einer oder keiner DSFA unterliegen. Sollte ein Verarbeitungsvorgang nicht durch einen der beiden Verordnungen gedeckt sein, so hat der Verantwortliche zu prüfen, ob eine DSFA erforderlich ist oder nicht.

Der DB/DSK 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 DSGVO bestimmt folgende Mindestanforderungen bezüglich des Inhalts einer DSFA:

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

- Das VVT ersetzt die Meldung an das DVR.
- Das VVT verfolgt einen prozessorientierten Ansatz. Es beschreibt das Verfahren der Datenverarbeitung, bei welchem auch mehrere Datenanwendungen beteiligt sein können.
- Das VVT ist zentraler Bestandteil Ihres Datenschutzmanagements.
- Jedes Hotel ist dazu verpflichtet ein VVT zu erstellen und aktuell zu halten.
- Datenschutz-Folgenabschätzung und das VVT sind getrennt zu betrachten d.h. es sind zwei unterschiedliche Dokumentationen, wobei auf Grund der Risikobewertung ein Bezug im VVT hergestellt werden kann.

- *Haben wir unsere Anwendungen beim DVR gemeldet?*
- *Wenn ja, was kann daraus für die Erstellung des VVT herangezogen werden?*
- *Wenn nein, welche Verarbeitungen kommen bei uns vor und wie kann somit das VVT aussehen?*
- *Führt jede Abteilung eigenverantwortlich das VVT oder delegieren wir die Tätigkeiten zentral an den DB/DSK? Wie bzw. wer unterstützt bei der Erstellung?*

5. Sales & Marketing

ZIELFRAGEN:

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

5.1. Der Internetauftritt

Nutzer von Firmenwebseiten und firmeneigener Social Media Dienste sind rechtzeitig und in geeigneter Form auf die Speicherung, Nutzung und Übermittlung von personenbezogenen Daten an Dritte hinzuweisen. Ein **Impressum** gemäß § 5 ECG sowie eine **Datenschutzerklärung** nach § 96 TKG sind so einzubinden, dass sie **von jeder Seite aus abrufbar** sind.

5.1.1. Informationspflichten

Wenn das Hotel eine oder mehrere Webseiten anbietet, tritt es als Dienstanbieter gemäß ECG auf. Entsprechend kommt auf das Hotel zunächst **„Allgemeine Informationspflichten“ (Impressum)** mit folgenden Angaben zu:

- Firma (Firmenwortlaut gemäß Firmenbucheintrag)
- Firmenbuchnummer
- Firmenbuchgericht
- Firmensitz
- Rechtsform
- Befindet sich das Unternehmen in Liquidation, ist dies anzuführen
- Angaben auf Grund derer der Nutzer rasch und unmittelbar mit dem Anbieter in Kontakt treten kann und elektronische Postadresse
- zuständige Aufsichtsbehörde, soweit die Tätigkeit einer behördlichen Aufsicht unterliegt
- Kammerzugehörigkeit
- UID

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

Der Hotelier hat nach § 96 Abs. 3 TKG somit die Nutzer seiner Webseite „darüber zu informieren, welche personenbezogenen Daten er ermittelt, verarbeitet und übermitteln wird, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt und für wie lange die Daten gespeichert werden."

HINWEIS | Die Datenschutzerklärung ist individuell auf Ihr Hotel abzustimmen. Finden Sie im **Anhang eine Checkliste und einen Link zu einer Musterdatenschutzerklärung**. Beides unterstützt Sie bei der Erstellung.

WICHTIG: Art. 7, 13 DSGVO fordern vor der direkten Erhebung von personenbezogenen Daten beim Nutzer eine formgerechte Einwilligung sowie die Benachrichtigung über den Umfang, die Nutzung, … (siehe Kapitel 1.6.1) der erhobenen Daten. Als Webseitenbetreiber müssen Sie nachweislich sicherstellen, dass der Gast, der reserviert, die Möglichkeit hat auf die Datenschutzerklärung zuzugreifen und zu lesen. Entsprechend empfiehlt es sich vor Buchungsabschluss, Newsletteranmeldung etc. einen Hinweis auf die allgemeinen Datenschutzbestimmungen inkl. Link auf die Datenschutzerklärung zu geben, bevor eine Datenübermittlung durch den Nutzer erfolgen kann.

HINWEIS | Wird die Webseite in mehreren Sprachen angeboten, so sollte die Datenschutzerklärung auch in diesen Sprachen verfügbar sein.

5.1.2. Social Plugins und Cookies

Social Plugins sind kleine Buttons von Social Media Kanälen, welche in Ihrer Webseite eingebaut werden können. Der Besucher Ihrer Webseite kann dann diese Buttons betätigen, um somit den Artikel zu teilen, zu öffnen oder sich auch ein Video ansehen, ohne dabei die geöffnete Webseite verlassen zu müssen. Bei diesem Vorgang übermittelt der Browser automatisch aktuelle IP Adressen und Cookies an den Social Media Kanal. Loggt sich der Nutzer dann in den Social Media Kanal ein, dann ist dieser in der Lage, die erhobenen Daten rückwirkend dem Nutzer zuzuordnen und somit das Profil für Werbeschaltungen zu schärfen.

Verwenden Sie Social Plugins auf Ihrer Webseite? Wenn ja, dann ist hier Handlungsbedarf gegeben. Wir empfehlen Ihnen folgende Vorgehensweise:

1. Prüfen Sie zuerst die Erfordernis des Plugins mit Ihrem Webseitenbetreuer/Marketingverantwortlichen.
2. Social Plugins sind auch einwilligungspflichtig – implementieren Sie hier eine Einwilligung – falls diese noch nicht vorhanden ist. Lassen Sie sich von Ihrem Webseitenbetreuer informieren, welche Variante (z.B. Zwei Klick Lösung) für Sie die passende ist.
3. Auch über die Einbindung ist zu informieren. Prüfen Sie Ihre Datenschutzerklärung auf Inhalte diesbezüglich und adaptieren Sie gegebenenfalls.

Cookies sind Textdaten, die der Browser (z.B. Firefox, etc.) auf dem Computer des Webseitenbesuchers speichert. Wenn Sie eine Webseite zum ersten Mal aufrufen, werden Cookies angelegt. Der Webseitenbetreiber hat die Möglichkeit, Kopien dieser Cookies zu erhalten, wenn die Cookies dann vom Browser zurückgesendet werden. Generell ist zu unterscheiden, dass Cookies verschiedene Funktionen erfüllen können. Im Groben ist zu unterscheiden zwischen funktionalen Cookies, welche z.B. zum Betreiben der Buchungsplattform auf Ihrer Webseite benötigt werden, und Cookies, mit deren Hilfe man Statistiken ableiten, Schlüsse auf das Surfverhalten des Besuchers ziehen oder auch Nutzerprofile anlegen kann. Ein Beispiel für Cookies, welche wir für unsere Statistiken oft verwenden, ist z.B. Google Analytics.

Der Besucher Ihrer Webseite hat aktiv einzuwilligen, sobald auf der Webseite personenbezogene Cookies verarbetet werden. Eine Formulierung in einem Banner wie z.B. „Mit dem Fortsetzen des Besuches stimmen Sie der Verwendung von Cookies zu“ oder auch ein vorangehaktes Kontrollkästchen in einem Banner sind nicht mehr ausreichend. D.h. wenn Sie Cookies verwenden, welche über die Funktionserhaltung (Nutzung) für die Webseite hinausgehen, dann erfordert das Setzen dieser Cookies eine aktive und informierte Einwilligung des Besuchers.

Cookies für eine Webseite gelten dann als unbedingt erforderlich und einwilligungsfrei, „wenn der alleinige Zweck die Durchführung oder Erleichterung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder, soweit dies unbedingt erforderlich ist, um einen vom Teilnehmer oder Nutzer ausdrücklich gewünschten Dienst der Informationsgesellschaft zur Verfügung zu stellen“ (Art. 5 Abs 3 ePrivacy-RL). Leider gibt es keine Auflistung, welche Cookies genau darunter zu verstehen sind. Es ist aber davon auszugehen, dass darunter Cookies fallen, welche für Ihre Buchungsmöglichkeit auf Ihrer Webseite benötigt werden, für die Login Möglichkeit bei Gästeprogrammen, für die Sprachauswahl sowie Cookies, die eine Cookie Einwilligung speichern.

Unter informiert ist zu verstehen, dass der Besucher vor Einwilligung erfährt, welche Cookies eingesetzt werden, die Art, die Funktion und die Funktionsdauer der Cookies, der Zugriffs-

möglichkeiten durch Dritte und der Möglichkeit des Widerrufs. Besucher Ihrer Webseite sollten auf die Datenschutzerklärung und das Impressum zugreifen können, ohne dass hierfür Cookies verwendet werden. Verlinken Sie am besten im Cookie Banner auf die Datenschutzerklärung – in welcher Sie der Informationspflicht nachkommen und weisen Sie hier auch auf die Opt Out Möglichkeit (wie kann ich meine Cookie Einwilligung widerrufen) hin.

Verwenden Sie Cookies auf Ihrer Webseite? Was ist nun zu tun?

1. Prüfen Sie mit Ihrem Webseitenbetreuer, ob Sie Cookies einsetzen.
2. Wenn ja – bringen Sie in Erfahrung, welche Art von Cookies verwendet werden.
3. Sind die Cookies lediglich technisch erforderlich für den Betrieb der Webseite, so sind keine weiteren Maßnahmen durchzuführen. (Lassen Sie sich diese Info am Besten schriftlich von Ihrem Webseitenbetreuer geben).
4. Werden „Marketing Cookies“ verwendet? Wenn ja
   a. Prüfen Sie, wann das Cookie gesetzt wird. Dieses sollte nicht schon dann gesetzt werden, wenn der Besucher noch nicht die Möglichkeit hatte zuzustimmen bzw. abzulehnen. Wenn dies der Fall sein sollte, so ist dies zu ändern.
   b. Bietet Ihre Webseite die Möglichkeit, das Setzen der Marketing Cookies aktiv und informiert abzulehnen? Wenn dies nicht der Fall ist, dann ist dies zu adaptieren.
   c. Ist die Information (Datenschutzerklärung) zu den Cookies genügend?

PRAXISTIPP | Machen Sie keine „Schnellschüsse“, sondern erarbeiten Sie konzentriert mit Ihrem Webseitenbetreuer/Marketingverantwortlichen die erforderlichen Schritte und Maßnahmen, um sicherzustellen, dass Sie einerseits weiterhin die Daten erhalten, die Sie für Ihre Marketingaktivitäten benötigen aber andererseits Ihre Webseite auch die datenschutzrechtlichen Aspekte erfüllt.

5.1.3. Urheberrechtsschutz

Beachten Sie, dass eine unerlaubte Veröffentlichung und Nutzung von Fotos und Grafiken auf der Webseite oder auch in Ihren Flyern Ansprüche auf Unterlassung, Beseitigung, Zahlung eines (verschuldensunabhängigen) angemessenen Lizenzentgeltes und Schadenersatzanspruches auslöst (§§ 81 ff UrhG). Die Verwendung von Musik, z.B. als Hintergrundmusik auf der Webseite, unterliegt ebenfalls dem Urheberrechtsschutz und ist entsprechend zu melden.

Sollten Sie Fotos oder Filme mit Personen anfertigen lassen oder selbst anfertigen, um diese auf der Webseite oder in sozialen Netzwerken, aber auch in Printmedien zu veröffentlichen bzw. zu posten, beachten Sie das Recht des Gastes oder auch Mitarbeiters am eigenen Bild gem. § 78 UrhG. Für diese Fälle benötigen Sie immer eine individuelle Einwilligungserklärung vom Abgebildeten. Wenn mehrere Personen auf einem Bild abgebildet

werden, ist von jeder einzelnen Person das Einverständnis einzuholen. Ein Gruppenrecht gibt es nicht, Ausnahmen bestehen nur bei Personen aus dem öffentlichen Leben.

PRAXISTIPP | 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 den entsprechenden Informationen (Verantwortlicher, Zweck der Aufnahmen und Hinweis auf Widerspruch) im Eingangsbereich der Veranstaltung sollte die Informationspflichten abrunden, um einer individuellen Einwilligung zu entgehen.

5.2. Social Media (Web 2.0)

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

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

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

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

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

5.3. Werbemaßnahmen

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

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

Es ist zu empfehlen, dass Adress- und Kontaktdaten von Geschäftskunden spätestens nach 3 Jahren nach dem letzten Kontakt gelöscht werden.

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

5.3.1. E-Mail-Werbung (Newsletter)

Eine besondere Form von E-Mail-Werbung sind **Newsletter**. Die gesetzliche Regelung findet sich dafür im Mediengesetz. Es handelt sich dann um einen Newsletter, wenn er **mindestens vier Mal im Kalenderjahr** in vergleichbarer Gestaltung versandt wird.

Die Nutzung der E-Mail-Adresse für einen **Newsletterservice** bedarf grundsätzlich der schriftlichen Einverständniserklärung des Gastes und dem Hinweis auf sein Recht auf Widerruf, eine Ausnahme gilt bei bestehender Geschäftsbeziehung (siehe 5.3.3.).

Der Gast muss mit dem aktiven Setzen eines Hakens oder Kreuzes und/oder seiner Unterschrift einwilligen. Die elektronische Einwilligung muss vom angegebenen Empfänger stammen. Als einzige anerkannte Verfahrensweise gilt das „Double-Opt-in“ Verfahren. Der Versender des Newsletters sendet dem neuen Empfänger eine Authentifizierungs-E-Mail mit einem Aktivierungslink zu. Der Empfänger bestätigt den Erhalt durch Anklicken des Links.

Versender und Empfänger schützen sich so vor dem Missbrauch von E-Mail-Adressen durch Dritte.

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

HINWEIS | 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.

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

HINWEIS | 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.

Für die Einhaltung der Offenlegungspflicht, welche mindestens über einen Link zu erfolgen hat, ist wie folgt anzuführen:

- Name/Firma des Medieninhabers
- Unternehmensgegenstand des Medieninhabers
- Wohnsitz/Sitz des Medieninhabers

5.3.2. Weitere Anforderungen an E-Mail-Werbungen

Bei der Versendung von E-Mail-Werbung gilt es auch folgendes zu beachten:

- Nennung der Identität des Absenders und authentische E-Mail-Adresse (§ 107 Abs. 2TKG)
- Kennzeichnung als Werbung (§ 6 ECG)
- Klarstellung des Absenders (§ 6 ECG)
- Erkennbarkeit von Angeboten zur Absatzförderung wie Zugaben und Geschenke (§ 6 ECG)
- Erkennbarkeit von Preisausschreiben und Gewinnspielen (§ 6 ECG)

5.3.3. 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 frühere und bestehende Geschäftsbeziehungen (§ 107 Abs. 3 TKG). 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.*“

Die verantwortliche Stelle kann für den Absatz **eigener, ähnlicher Waren und Dienstleistungen** per E-Mail werben, ohne die ausdrückliche Einwilligung des Gastes einzuholen bis die weitere Nutzung untersagt wird. **Auf die Widerspruchsmöglichkeit** muss der Gast 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. Die Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) führt eine Liste, in die sich diejenigen Personen und Unternehmen kostenlos eintragen können, die für sich die Zusendung kommerzieller Kommunikation im Weg der elektronischen Post ausgeschlossen haben. Diese Liste ist vor Versand zu beachten (§ 107 Abs. 3 Nr. 4 TKG).

5.3.4. 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.

TEXTBEISPIEL für den Widerspruch bei Werbung

Wenn Sie zukünftig keine Information von uns erhalten möchten, teilen Sie uns dies bitte unter Tel.: … oder per E-Mail an … inklusive Angabe Ihres Vor- und Nachnamens und Anschrift mit. Ihnen entstehen dadurch keine Kosten.

5.4. Gästebewertung

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

5.4.1. Gästefragebogen

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

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

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

5.4.2. Online-Bewertungen

Zunehmend wird den Gästen angeboten, ihre Hotelbewertung online abzugeben. Diese wird dann auf der Hotelwebseite veröffentlicht. Viele Hotels 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.

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.

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

5.5. Kundenbindungsprogramme

Kundenbindungsprogramme richten Leistungs- und Kommunikationsangebote an bestimmte Kundensegmente – und zwar über den eigentlichen Kaufprozess hinaus. Ein Kundenbindungsprogramm kann bspw. 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 bspw. wesentlich den Check-In der Stammgäste in 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.

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 Einwilligung 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 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 zu informieren. In der Hotelsoftware ist der Datensatz zum Gast für die Datenfreigabe gegenüber verbundener Unternehmen zu kennzeichnen.

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 Kundenbindungsprogrammen. 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 für andere Zwecke 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 sechs 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 Internettauftritt sind gesetzliche Informationspflichten zu beachten. Die gesetzlichen Erfordernisse lt. TKG und ECG sind bei Webseite und E-Mail-Werbung einzuhalten.
- 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.
- Werden Reservierungen über Ihre Webseite getätigt, so sollte die Anwendung der AGB's 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.
- Einhaltung des Urheberrechtsgesetzes in allen Ihrer Medien, sowie die Beachtung bei musikalischer Wiedergabe.
- Differenzierung zwischen Newsletter und E-Mail-Werbung.
- Bei Verwendung von personenbezogenen Cookies ist dies zumindest auf der Webseite anzuführen, zu bevorzugen ist eine Zustimmung durch den Webseiten-User.
- Einwilligungserklärungen können zusammen mit Informationspflichten zur Nutzung von Adress- und Kontaktdaten zu Werbezwecke beim Antrag einer Kundenkarte berücksichtigt werden.

- *Überprüfung der gesetzlichen Informationspflichten auf der Webseite.*
- *Hinweispflicht bei Verwendung von personenbezogenen Cookies bzw. Zustimmung durch den User implementieren.*
- *Kontrolle, ob bei allen Medien das Urhebergesetz eingehalten wird.*
- *Überprüfung des Newsletterversandes.*
- *Gibt es eine Dokumentation aller Vertriebs- und Marketingaktivitäten?*
- *Wo werden Adress- und Kontaktlisten noch gespeichert (Excel- Dateien)?*
- *Wird ein Datenexport dokumentiert? Wer kann Gastdaten exportieren?*

6. Datenverarbeitung im Auftrag

ZIELFRAGEN:

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

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

Die DSGVO regelt die Auftragsverarbeitung in Art. 28 ff. **Als Auftraggeber sind Sie dazu verpflichtet, die Anforderungen umzusetzen**. Prüfen Sie also alle **Auftragsverhältnisse und Verträge**, es müssen **Datenschutzvereinbarungen** abgeschlossen werden, wenn es sich um eine Datenverarbeitung im Auftrag handelt. Sollen also personenbezogene Daten im Auftrag verarbeitet werden (z.B. Fernwartung Hotelsoftware, Online-Reservierungs-

system, 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.

Der Hotelier bleibt als Auftraggeber auch für die Dienstleister verantwortlich.

EMPFEHLUNG | Führen Sie über die bestehenden Verträge über Auftragsverarbeitung ein Vertragsverzeichnis damit Sie jederzeit den Überblick behalten.

WICHTIG: 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 bestrafen.

6.1. Abgrenzung von Datenverarbeitung im Auftrag

Datenschutzrechtlich zu unterscheiden sind beim Outsourcing die Auftragsverarbeitung und die Funktionsübertragung. Die Frage wie ein Outsourcing 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 **Funktionsübertragung** wird dagegen auch die der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zu Grunde liegende Aufgabe ganz oder teilweise abgegeben. Die in Anspruch genommene Serviceeinrichtung erbringt – über die technische Durchführung des Umgangs mit personenbezogenen Daten hinaus – materielle Leistungen mit Hilfe der überlassenen Daten. Sie handelt hierbei **eigenverantwortlich**, auch **im Sinne des Datenschutzrechts**, tritt selbst als verantwortliche Stelle auf.

Erkennungsmerkmale für Funktionsübertragung

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

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

Sonderfall Wartung und Pflege

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

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

6.2. Auswahl des Dienstleisters

6.2.1. Prüfung des Leistungsumfangs

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

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

HINWEIS | 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.

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

6.2.2. Besondere Prüfungspflichten im Rahmen der Datenschutz-Folgenabschätzung

Wenn eine Form der Verarbeitung von personenbezogenen Daten, insbesondere bei Verwendung neuer Technologien oder aufgrund des Umfangs, der Umstände und Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, muss der Verantwortliche gemäß Art. 35 DSGVO vorab eine Abschätzung der Folgen für den Schutz der personenbezogenen Daten der Betroffenen 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 DSFA unterliegen. Vergleichen Sie hierzu Kapitel 4.3.

6.2.3. Berücksichtigung der Eignung

Es darf **nur ein Auftragsverarbeiter beauftragt** werden, wenn dieser **ausreichende und hinreichende Garantien** erbracht hat und die notwendigen technischen und organisatorischen Maßnahmen im Einklang mit den Anforderungen der DSGVO stehen. Als Beleg sol-

cher 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 DB/DSK führt eine entsprechende Prüfung durch.

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

6.3. Vertragsgestaltung und Vertragsabschluss

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

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

Dazu sollten insbesondere konkret geregelt sein:

- Weisungsbefugnis des Auftraggebers/Verantwortlichen,
- Verpflichtung des Auftragnehmers, nur solche Personen bei der Verarbeitung und Nutzung personenbezogener Daten einzusetzen, die mit den Vorschriften des Datenschutzgesetzes vertraut gemacht und auf das Datengeheimnis verpflichtet worden sind,
- Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO zum Schutz der zur Verarbeitung übergebenen Daten vor einer unbefugten Verwertung, insbesondere zur Verhinderung des Missbrauchs von Daten durch unbefugten Zugriff, Verfälschung, Zerstörung, Verlust oder Preisgabe an Unbefugte.
- Verpflichtung des Auftragnehmers, Subunternehmen nur nach vorheriger Abstimmung mit dem Hotel einzusetzen,
- Verpflichtung zur Unterstützung der Umsetzung von Betroffenenrechten 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.

HINWEIS | Unter diesem Link, finden Sie ein Vertragsmuster der Wirtschaftskammer. Beachten Sie, dass dieses je nach Einzelfall anzupassen ist.

6.3.1. Abgrenzung der Leistung

Im ersten Schritt ist entsprechend den Merkmalen aus Kapitel 6.1 abzugrenzen, ob es sich bei der Dienstleistung um eine Auftragsverarbeitung oder eine Funktionsübertragung handelt.

6.3.2. Auswahl der Vertragsform

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

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

PRAXISTIPP | Prüfen Sie ob und wenn ja welche Art des Vertrages mit Ihrem Auftragnehmer vorhanden ist. Dementsprechend ist dann zu berücksichtigen, ob lediglich eine Verpflichtung auf das Datengeheimnis, eine Vertraulichkeitsvereinbarung, eine Datenschutzvereinbarung oder sogar eine EU-Standarddatenschutzklausel (Vorlage, die von der Europäischen Kommission erlassen oder genehmigt worden ist), abzuschließen ist. Die nachfolgende Aufstellung hilft Ihnen bei der Entscheidungsfindung.

Vertragsarten	Vertragsformen zur Zusatzvereinbarung
Dienstleistungs- und Servicevertrag	Auftrag gemäß Art. 28 DSGVO Verpflichtung von Dritten – Vertrags-partnern – auf das Datengeheimnis Vertraulichkeitsvereinbarung
Fremdpersonal	Verpflichtung von Dritten – Fremdpersonal – auf das Datengeheimnis
Rahmenvereinbarungen	Datenschutzvereinbarung / Zusatzverein-barung
Datenübermittlung in Drittstaaten ohne angemessenen Datenschutzniveau (Drittländer außerhalb der EU/EWR)	EU-Standarddatenschutzklausel gemäß Art.46 Abs. 2 lit. c DSGVO
Datenübermittlung in Drittstaaten mit angemessenen Datenschutzniveau (auch Privacy Shield)	Datenschutzvereinbarung (DEU/ENG)

Bestehende Verträge

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

6.3.3. 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

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

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

7. Videoüberwachung

ZIELFRAGEN:

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

7.1. Was ist eine Videoüberwachung?

Videoüberwachung ist die systematische, insbesondere fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt oder eine bestimmte Person betreffen, mittels technischer Bildaufnahme oder Bildübertragungsgerät. Eine Regelung in der DSGVO ist nicht vorhanden. Im DSG fällt die Videoüberwachung unter dem Abschnitt 3, der „Bildverarbeitung". Unter einer Bildaufnahme wird die Verwendung technischer Einrichtungen zur Bildverarbeitung von Ereignissen im öffentlichen oder nicht öffentlichen Raum zu privaten Zwecken verstanden. Zur Bildaufnahme gehören auch die mitverarbeiteten akustischen Informationen.

Bevor eine Videoanlage in Betrieb genommen werden kann, ist durch den DB/DSK zu prüfen, um auszuschließen, dass Persönlichkeitsrechte durch die Aufzeichnungen verletzt werden. Der DB/DSVK muss nur dann keine DSFA durchführen, wenn die Ausnahmebestimmungen der DSFA-AV für die Verarbeitung (DSFA-AA09) bei der Implementierung/Installation zutreffen und eingehalten werden. Die Verarbeitung Videoüberwachung ist in das VVT 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 Implementierung sollten alle Kameras, egal welchen o.g. Typs, einzeln aufgeführt und beschrieben werden. Es ist eine Übersicht zu führen, wo sich die jeweiligen Kameras befinden (ein Lageplan ist hier hilfreich). Zusätzlich sind zu jeder Kamera nachfolgende Kriterien aufzuführen:

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

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

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

7.2. Zulässige und unzulässige Videoüberwachungen

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

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

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 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 DSB/DSK vor Installation zwischen den Interessen der Betroffenen und des Hotels abwägen.

HINWEIS | Eine Videoüberwachung kann nicht damit gerechtfertigt werden, dass das **Eigentum der Gäste zu schützen** ist.

Eine **verdeckte Videoüberwachung** von Beschäftigten ist nur zulässig, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass Beschäftigte im Beschäftigungsverhältnis eine Straftat begangen haben, die Erhebung zur Aufdeckung erforderlich ist und Art und Ausmaß der Erhebung im Hinblick auf den Zweck nicht unverhältnismäßig sind. Im Vorfeld ist die vermutete Straftat bei den Strafverfolgungsbehörden anzuzeigen.

7.3. Kennzeichnungspflicht

Die **Videoüberwachung** und die dafür **verantwortliche Stelle** (Name und Kontaktdaten) ist gemäß § 13 Abs. 5 DSG (**Kennzeichnungspflicht**) durch geeignete Maßnahmen erkennbar zu machen. Der Hinweis ist deutlich sichtbar anzubringen, er muss vor Betreten des überwachten Bereiches problemlos wahrnehmbar sein. Zu kennzeichnen sind insbesondere die Eingangsbereiche, auch beim Einsatz von **Kamera-Dummys**. Die Betroffenen müssen die Kennzeichnung frühzeitig erkennen. Dementsprechend ist auch eine angemessene Größe zu beachten.

7.4. Protokollierungs- und Löschungspflicht

In § 13 Abs. 3 DSG definiert der Gesetzgeber, dass die Daten **unverzüglich zu löschen** sind, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder wenn keine anderen gesetzlichen Aufbewahrungsfristen mehr bestehen. Eine längere Speicherung als 72 Stunden ist in der DSFA-VA nur in Ausnahmefällen (gesetzlich, behördlich oder durch eine Betriebsvereinbarung geregelt) zulässig. Daten welche ggf. für Schutz- oder Beweissicherungszwecke länger benötigt werden, können länger aufbewahrt werden. Bei Anfrage seitens der Polizei sind diese zu sichern, eine Herausgabe kann i.d.R. nur auf Grundlage einer richterlichen Anordnung erfolgen.

Bei Durchführung von Bildaufnahmen ist zu beachten, dass der Verantwortliche geeignete Datensicherheitsmaßnahmen zu ergreifen und Sorge zu tragen hat, dass der Zugang zur Bildaufnahme und eine nachträgliche Veränderung durch Unbefugte ausgeschlossen ist. Jeder Verarbeitungsvorgang/Zugriff auf Videoaufzeichnungen ist durch den Verantwortlichen lückenlos zu dokumentieren.

7.5. Auskunftsrecht

Betroffene haben das Recht, die Übermittlung einer Kopie der von ihnen gefertigten Aufnahmen anzufordern. Des Weiteren kann der Betroffene auch die Einsichtnahme auf die Lesegeräte des Hotels verlangen. Zusätzlich 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. Ein möglichst genauer Zeitraum und der Ort der Überwachung ist dem Hotelier mitzuteilen.

7.6. Zufällige Aufzeichnungen von strafbaren Handlungen

Sollten bei Aufnahmen zufällig Ereignisse aufgenommen werden, die nicht vom 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 auf Grundlage einer richterlichen Anordnung an die zuständige Behörde oder das Gericht übermittelt werden.

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

Verfüge ich über eine Videoüberwachung? Wenn ja, erfülle ich alle gesetzlichen Anforderungen?

- Bei Implementierung, Prüfung an Hand der Checkliste zur Videoüberwachung.
- Kennzeichnung der überwachten Bereiche.
- Erstellung von Vorlagen zur Protokollierung und Einführung von Standards zum Umgang mit der Videoüberwachungsanlage.

8. Datenschutz und Sicherheit – Regelungen im Hotel

ZIELFRAGEN:

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

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

8.1. Angemessene Sicherheitsmaßnahmen

Als Verantwortlicher hat der Hotelier unter Beachtung des Verhältnismäßigkeitsgrundsatzes geeignete technische und organisatorische Maßnahmen zu treffen um sicherzustellen, dass die Verarbeitungen rechtmäßig verlaufen. Er hat solche Verarbeitungstechniken zu wählen, die den Datenschutzgrundsätzen der Datenminimierung und den Grundsätzen des Datenschutzes durch Technikgestaltung (data protection by design) 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.

8.2. Datenschutzrichtlinien

Datenschutzrichtlinien regeln die rechtlichen und die grundsätzlichen technischen und organisatorischen Maßnahmen zum Datenschutz. Im Anhang ist eine Struktur einer Datenschutzrichtlinie angeführt von der Sie mögliche Inhalte entnehmen können. Die Regeln zum Datenschutz sollten regelmäßig in einem internen Datenschutzaudit auf Einhaltung und Aktualität geprüft werden.

Weil ein wirksamer Datenschutz nicht alleine durch Regelungen und Bestimmungen erreicht werden kann, sondern von einem ausgeprägten Datenschutz- und Sicherheitsbewusstsein der 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 Richtlinien erlassen werden, insbesondere zu Verfahren, bei denen die Persönlichkeitsrechte von Betroffenen eingeschränkt werden können. Hierzu zählen auch Verfahren, die eine Leistungs- und Verhaltenskontrolle von Mitarbeitern bzw. das Profiling von Kunden zulassen. Zusätzliche Richtlinien können sein:

- Nutzung von E-Mail und Internetdiensten im Hotel
- Nutzung von Telefondiensten
- Einsatz von Videoüberwachungssystemen
- Einsatz von Zeiterfassungssystemen
- Einsatz von elektronischen Türschließsystemen
- wie z.B. Social Media Guidlines

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

8.3. IT-Sicherheitsrichtlinien

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

Sie können aus der im **Anhang** aufgeführten **Struktur einer IT-Sicherheitsrichtlinie** mögliche Inhalte entnehmen. Die Regelungen sollten regelmäßig in einem internen IT-Sicherheitsaudit auf Einhaltung und Aktualität geprüft werden.

8.4. Phasen der Implementierung

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

Abbildung 3 | Phasen der Implementierung einer IT- und Datenschutzrichtlinie
Quelle: in Anlehnung an R. Knyrim/M. Oman, IT und Datenschutz-Policies in der Praxis

- Eine IT- und Datenschutzrichtlinie klärt in Ihrem Hotel datenschutzrechtliche Sicherheitsaspekte und dient dazu Ihre Mitarbeiter entsprechend zu unterweisen.
- Die Regeln zu Datenschutz und Datensicherheit sollten regelmäßig in einem internen Audit auf Einhaltung und Aktualität geprüft werden.

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

Anhang

Linkliste

www.oehv.at/datenschutzgrundverordnung

Gesetzestexte:

Datenschutz-Anpassungsgesetz 2018)
https://www.ris.bka.gv.at/eli/bgbl/I/2017/120

Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV)
https://www.ris.bka.gv.at/eli/bgbl/II/2018/108/20180525

Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V)
https://www.ris.bka.gv.at/eli/bgbl/II/2018/278/20181109

E-Commerce-Gesetz:
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001703

EU-Datenschutz-Grundverordnung:
https://www.jusline.at/gesetz/dsgvo

Telekommunikationsgesetz 2003:
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20002849

Vorlagen:

Musterdokumente zur EU-Datenschutz-Grundverordnung:

https://www.wko.at/branchen/noe/tourismus-freizeitwirtschaft/hotellerie/datenschutz-grundverordnung-in-der-hotellerie.html

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Informationen-zur-EU-Datenschutz-Grundverordnung.html

Muster Verzeichnis von Verarbeitungstätigkeiten

Verzeichnis von Verarbeitungstätigkeiten nach DSGVO

Name des Verantwortlichen
Kontaktdaten des Verantwortlichen
Name des Datenschutzbeauftragten/Datenschutzkoordinators
Kontaktdaten des Datenschutzbeauftragten/Datenschutzkoordinators

Nr. der Verarbeitung	Bezeichnung der Verarbeitungstätigkeit	Zweck der Verarbeitung	Betroffenen-kreise	Daten-kategorien	sensible Daten	Speicherdauer der Datenkategorie	Empfängerkreise – Namen der Gesellschaften außerhalb der eigenen Gesellschaft, aber innerhalb des Konzerns oder fremde Dritte	Transfers in Drittländer außerhalb der EU (Name des Empfängers, Land)	Beschreibung der Datensicherheitsmaßnahmen (Art. 30), um Verlust, Zerstörung, Veränderung, unauthorisierten Zugang oder Veröffentlichung zu verhindern durch technische und organisa-torische Maßnahmen

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

Checkliste zur Prüfung der Inhalte der Datenschutzerklärung

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

Allgemeine Angaben

1. Wer betreibt die Internetseite?
   Name und Kontaktdaten des Verantwortlichen, ggf. Datenschutzbeauftragten

Erhebung und Verarbeitung personenbezogener Daten

1. Werden personenbezogene Daten über die Webseite erhoben und verarbeitet?
   Erläutern Sie in diesem Zusammenhang die Kategorien der zu erhebenden Daten (Vor- und Nachname, Adress-, und Kontaktdaten, Zahlungsdaten, Buchungsdaten)
2. Erheben Sie oder Ihr Webspace Provider Zugriffs- und Protokolldaten?
   Wenn ja, so ist anzuführen, wer und welche Daten erhoben werden und was mit den Daten geschieht.
3. Bieten Sie Kontaktmöglichkeiten an (z.B. Kontaktanfrage, Blog)?
   Wenn ja, dann ist anzuführen, welche Daten genutzt werden, was mit den Daten geschieht (Zweck, Rechtsgrundlage, Löschfrist). Es ist zusätzlich darauf zu verweisen, dass für die Bearbeitung der Anfrage die Daten gespeichert werden.
4. Bieten Sie die Möglichkeit, über ein Online-Reservierungssystem zu buchen?
   Wenn ja, dann ist anzuführen, welche Daten genutzt werden, was mit den Daten geschieht (Zweck, Rechtsgrundlage, Löschfrist). Sollte der Service über einen Drittanbieter angeboten werden, so ist dieser ebenfalls anzuführen.
5. Bieten Sie die Möglichkeit, einen Newsletter zu abonnieren an?
   Wenn ja, dann ist anzuführen, welche Daten erhoben werden, was mit den Daten geschieht (Zweck) und dem Hinweis auf Widerruf bei Einwilligung. Sollte der Service über einen Drittanbieter angeboten werden, so ist dieser ebenfalls anzuführen.
6. Möchten Sie die E-Mail-Adresse zur Kontaktaufnahme für eine Online-Bewertung nutzen?
   Wenn ja, dann ist anzuführen, welche Daten genutzt werden, was mit den Daten geschieht (Zweck, ggf. Zweckerweiterung wie anonymisierte Auswertung, Rechtsgrundlage, Löschfrist) und dem Hinweis auf Widerruf. Sollte der Service über einen Drittanbieter angeboten werden, so ist dieser ebenfalls anzuführen.
7. Bieten Sie den Nutzern Ihrer Webseite ein Gutscheinsystem an?
   Wenn ja, dann ist anzuführen, welche Daten genutzt werden, was mit den Daten geschieht (Zweck, Rechtsgrundlage, Löschfrist). Sollte der Service über einen Drittanbieter angeboten werden, so ist dieser ebenfalls anzuführen.

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

9. Bieten Sie eine Registrierfunktion an (z.B. für Stammgäste)?
Wenn ja, führen Sie an, was der Zweck der Registrierung ist. Welche Daten aufgenommen werden und was genau mit diesen Daten geschieht.

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

Weitergabe von personenbezogenen Daten an Dritte

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

12. Beabsichtigen Sie, Gastdaten an ein Franchise-Unternehmen weiterzugeben?
Wenn ja, dann ist anzuführen, welche Daten dem Franchiser übermittelt werden. Der Nutzer ist über den Zweck, die Rechtsgrundlage und sein Widerspruchsrecht gegen die Datenübermittlung zu informieren.

13. Beauftragen Sie Dritte um Dienstleistungen für den Gast zu erfüllen (z.B. Buchung von Stadtrundfahrten, Abholung vom Flughafen)?
Wenn ja, informieren Sie den Nutzer, dass Sie Daten nur dann an Dritte weitergeben werden, sofern dies zur Erbringung von Dienstleistungen erforderlich ist, und dass die Partner die Daten lediglich für die Erfüllung des Auftrages nutzen.

14. Beabsichtigen Sie, personenbezogene Daten an weitere Dritte weiterzugeben?
Wenn ja, dann ist anzuführen, welche Daten an welchen Dritten (z.B. Bonusprogramm, Tischreservierung, …) übermittelt werden. Der Nutzer ist über den Zweck, die Rechtsgrundlage und sein Widerspruchsrecht gegen die Datenübermittlung zu informieren.

Instrumente zur Webseitenoptimierung und Analyse des Nutzungsverhaltens

15. Binden Sie fremde Inhalte, wie z.B. Google Maps, RSS Feeds oder Grafiken auf Ihrer Webseite ein?
Wenn ja, führen Sie den Hinweis an, dass diese die IP Adresse des Nutzers speichern. Dass kein Einfluss darauf besteht, ob diese Drittanbieter die IP Adresse z.B. für statistische Zwecke speichern, dass jedoch falls dies bekannt ist, der Nutzer darauf hingewiesen wird.

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

17. Verwenden Sie Google Analytics oder andere Analyse- und Trackingtools?
Wenn ja, so sind diese entsprechend anzuführen. Hierzu finden Sie standardisierte Texte im Internet, z.B. https://www.cookiechoices.org

18. Haben Sie Social Plugins (z.B. Facebook) integriert?
Wenn ja, so ist eine Formulierung betreffend der Datenverarbeitung in Bezug auf das Plugin anzuführen (Funktion, was macht es und wozu ist es vorhanden).

Rechte der Betroffenen

19. Informieren Sie den Nutzer der Webseite, welche Rechte er bezüglich der Verarbeitung seiner Daten wie wahrnehmen kann.
- Auskunft
- Löschung
- Berichtigung
- Widerspruch

20. Informieren Sie den Nutzer der Webseite über sein Beschwerderecht bei der Datenschutzbehörde.

Datensicherheit

21. Informieren Sie den Nutzer der Webseite über getroffene technische und organisatorische Sicherheitsvorkehrungen.
- Verschlüsselung
- Zusammenarbeit mit Zahlungsdienstleistern
- Datenschutzvereinbarungen mit Dienstleistern

Checkliste Datenverarbeitung im Auftrag (mgl. Dienstleister)

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

Checkliste Einsatz und Nutzung von Videokontrollsystemen

1. Welche Räumlichkeiten/Objekte sollen videoüberwacht werden?

2. Was ist der Zweck der Datenspeicherung?

3. Wie erfolgt die Speicherung der Daten?

☐ analog ☐ digital

Bemerkungen: .....

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

☐ ja ☐ nein

Bemerkungen: .....

5. Werden auch Tondaten erfasst?

☐ ja ☐ nein

Bemerkungen: .....

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

.....

7. In welchen Zeiträumen wird videoüberwacht?

☐ rund um die Uhr ☐ Bewegungsmelder ☐ vorgegebene Zeiten .....
☐ außerhalb der Geschäftszeiten ☐ nur nachts

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

.....

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

.....

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

☐ Benutzer ☐ Passwort ☐ keine Zugriffsregelung

Bemerkungen: .....

11. Werden **Mitarbeiterdaten** erfasst?

☐ ja ☐ nein
☐ regelmäßig ☐ unregelmäßig

Bemerkungen: .....

12. Sind die Kamerapositionen **schwenkbar**?

☐ ja ☐ nein

Bemerkungen: .....

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

☐ ja ☐ nein

Bemerkungen: .....

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

☐ Einsatz von Sicherheitspersonal ☐ Alarmanlage
☐ Zugangskontrollsystem ☐ Echtzeitkamera

Bemerkungen: .....

Ist eine DSFA erforderlich?

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

....

Ort, Datum Unterschrift, Stempel

Muster zum Inhalt einer Datenschutzrichtlinie

Muster zum Inhalt einer IT-Sicherheitsrichtlinie

Österreichische Hoteliervereinigung
Hofburg, A-1010 Wien

T: +43 (0)1 533 09 52-0 I F: +43 (0)1 405 25 84 I office@oehv.at I www.oehv.at

Für eine STARKE Hotellerie.