

H3

HOTELTRAINING
UND BERATUNG



DSGVO im Hotelalltag

Datenschutz praktisch im Hotel
integrieren und organisieren



ÖSTERREICHISCHE
HOTELVEREINIGUNG

Ein ÖHV Online Talk



- 1 DSGVO Grundprinzipien
- 2 To-dos im Hotelalltag
- 3 Marketing und Gästedaten
- 4 Videoüberwachung
- 5 Datenverlust und Reaktion





Kurz zu mir

Mag. (FH) Annemarie Maurer
Gründerin von H3 Hotel Training & Beratung



Seit 2016 Beratung und Training
ausschließlich für Hotelbetriebe

Schwerpunkte:

Datenschutz

Qualitätsmanagement

Trainings on the job

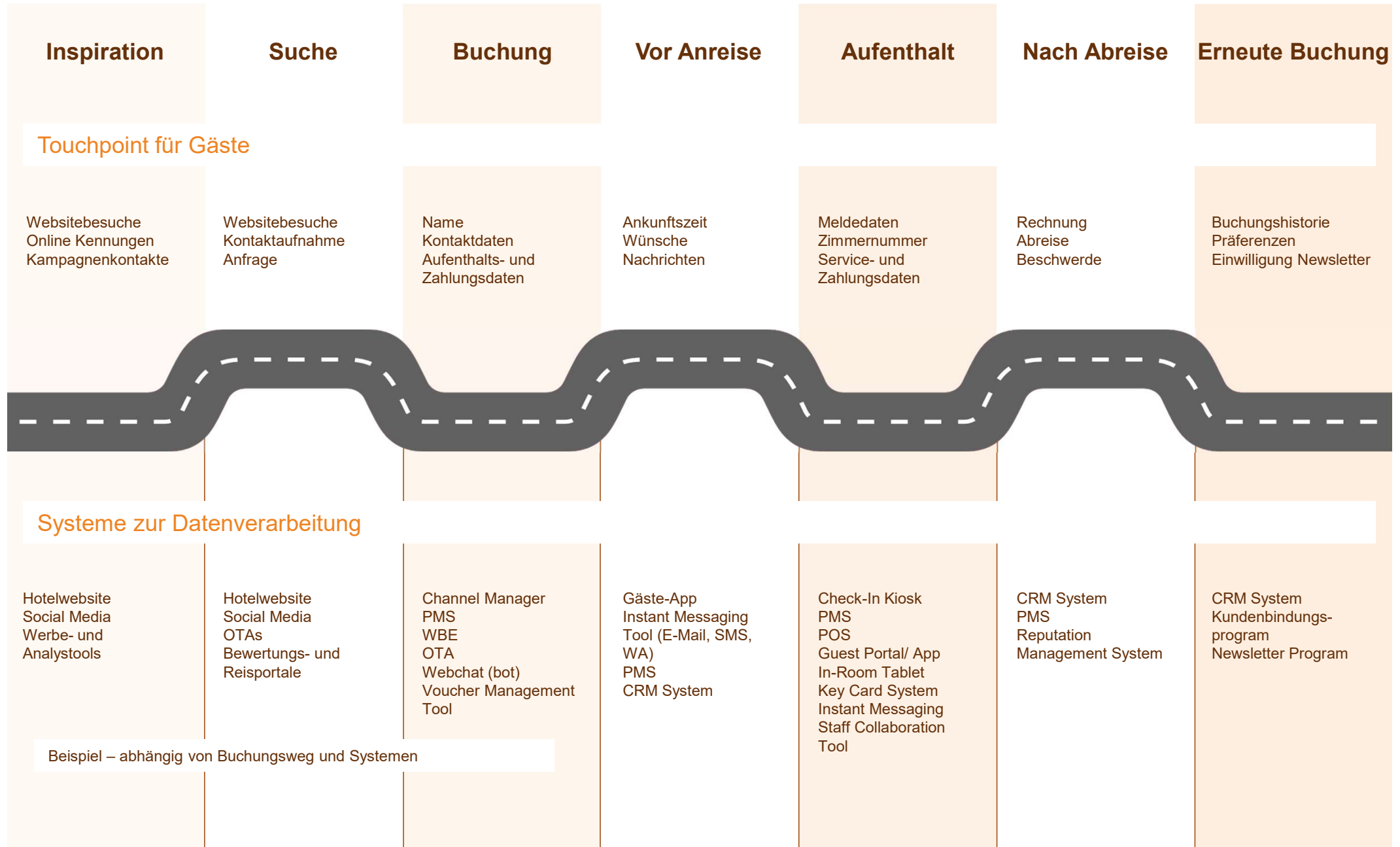


Geprüfte Datenschutzexpertin und
Trainerin in der Hotellerie

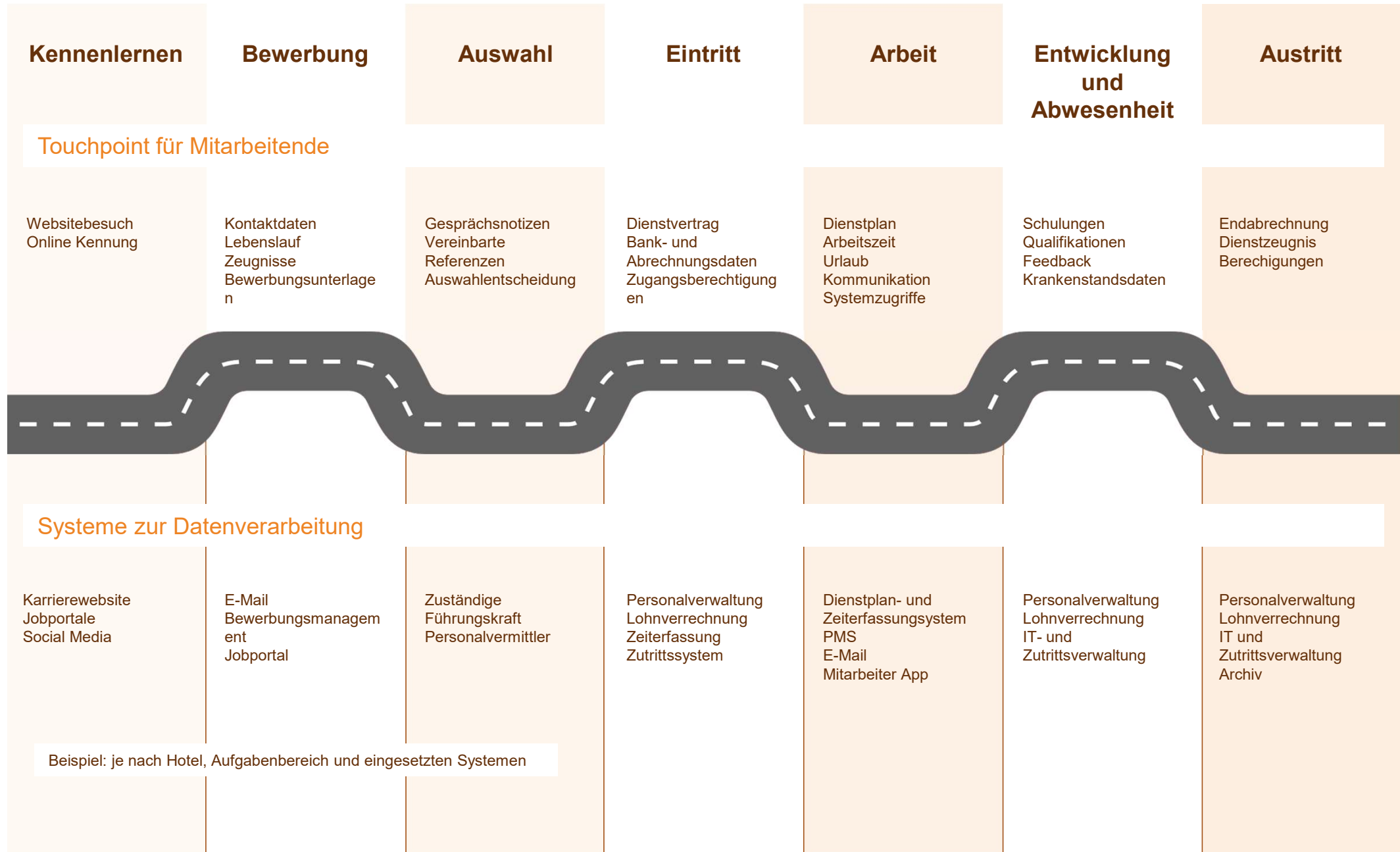
Co-Autorin des ÖHV-Leitfadens „Datenschutz in der
Hotellerie“ und regelmäßig mit Fachartikeln vertreten



Gastdaten entlang der Gästereise



Mitarbeiterdaten





DSGVO Grundprinzipien



Der rote Faden – die sieben Grundprinzipien

1. **Rechtmäßigkeit:** Verarbeiten nach Treu und Glauben, Transparenz
2. **Zweckbindung:** Daten nur für vorher festgelegte Zwecke
3. **Datenminimierung:** nur erheben und nutzen, was nötig ist
4. **Richtigkeit:** sachlich falsche oder veraltete Daten korrigieren
5. **Speicherbegrenzung:** löschen sobald der Zweck und Aufbewahrungspflicht enden
6. **Integrität und Vertraulichkeit:** angemessen schützen
7. **Rechenschaftspflicht:** die Einhaltung nachweisen können



Für jeden Zweck eine Rechtsgrundlage

- **Vertrag:** Reservierung bearbeiten, Aufenthalt durchführen, Rechnung erstellen
- **Gesetzliche Pflicht:** Melde- und Aufbewahrungspflichten
- **Berechtigte Interesse:** nur nach dokumentierter Interessensabwägung
- **Einwilligung:** freiwillig, informiert, konkret und widerrufbar
- (Lebenswichtige Interessen oder öffentliche Aufgabe)



Transparenz:

Datenumgang verständlich erklären

- **Wer** ist verantwortlich und wie kann man den Betrieb erreichen?
- **Welche Daten** werden für welchen Zweck verarbeitet und auf welcher Grundlage?
- **Welche Dienstleister** oder Empfänger erhalten Daten?
- **Von Wem** erhalten wir Daten?
- **Wie lange** werden die Daten gespeichert oder wann und nach welchen Kriterien werden sie gelöscht?
- **Welche Rechte** haben Gäste und Mitarbeiter und an wen können sie sich wenden?



Rechenschaftspflicht: zur Übersicht und Nachweis

- Verzeichnis der Verarbeitungstätigkeiten: Zwecke, Daten, Empfänger, Fristen, Schutzmaßnahmen
- Datenschutzhinweise: Website, Buchung, Aufenthalt, Videoüberwachung, Mitarbeiter
- Auftragsverarbeitungsverträge und Dienstleisterprüfung
- Berechtigungskonzept
- Löschregeln
- Mitarbeiterschulungen
- (Datenschutz-Folgenabschätzung, Verarbeitungen mit hohem Risiko)





To-dos im Hotelalltag



Datenflüsse und Systeme kennen

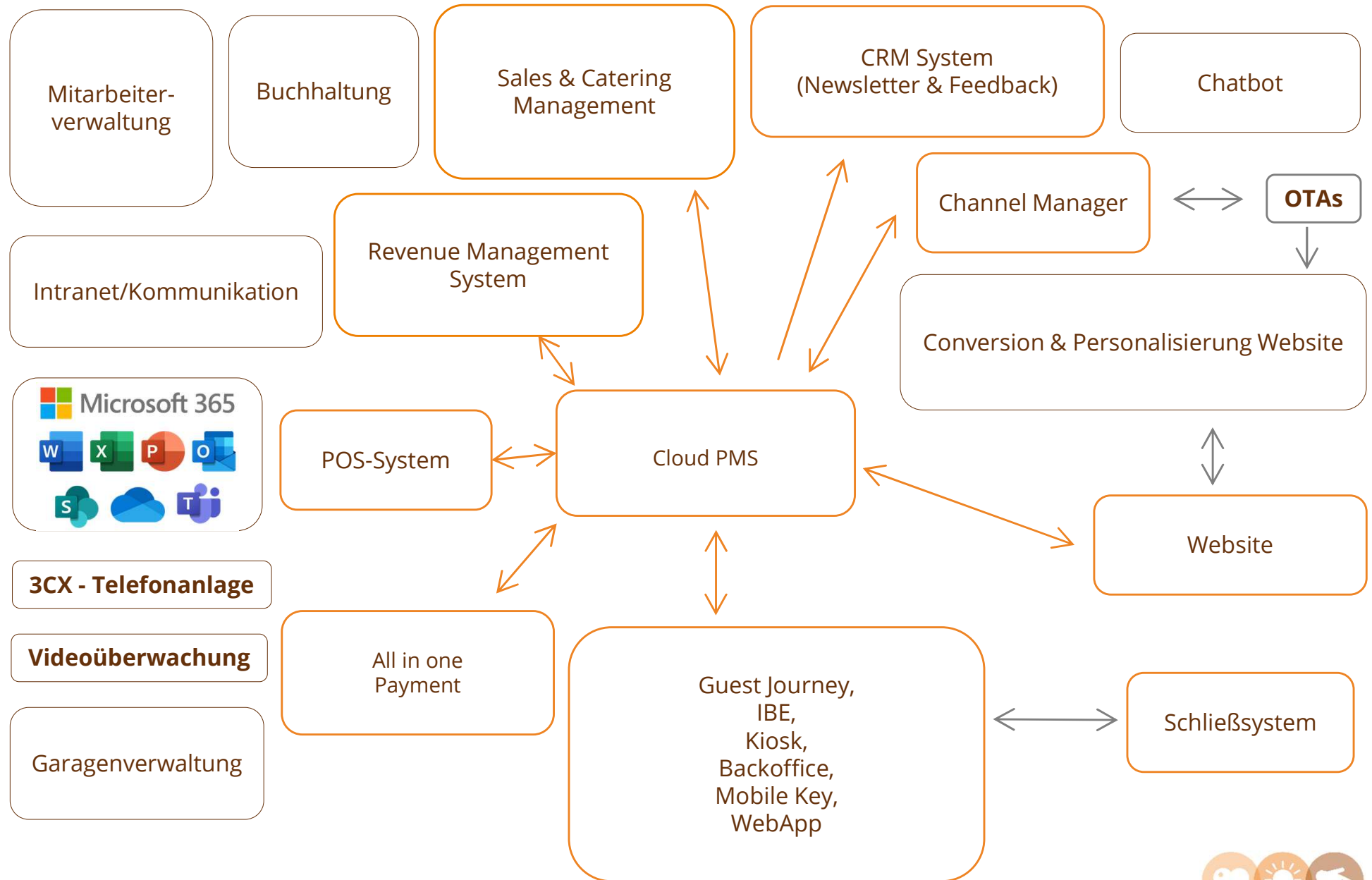
- Systemliste oder grafische Übersicht mit Datenwegen



Systemübersicht

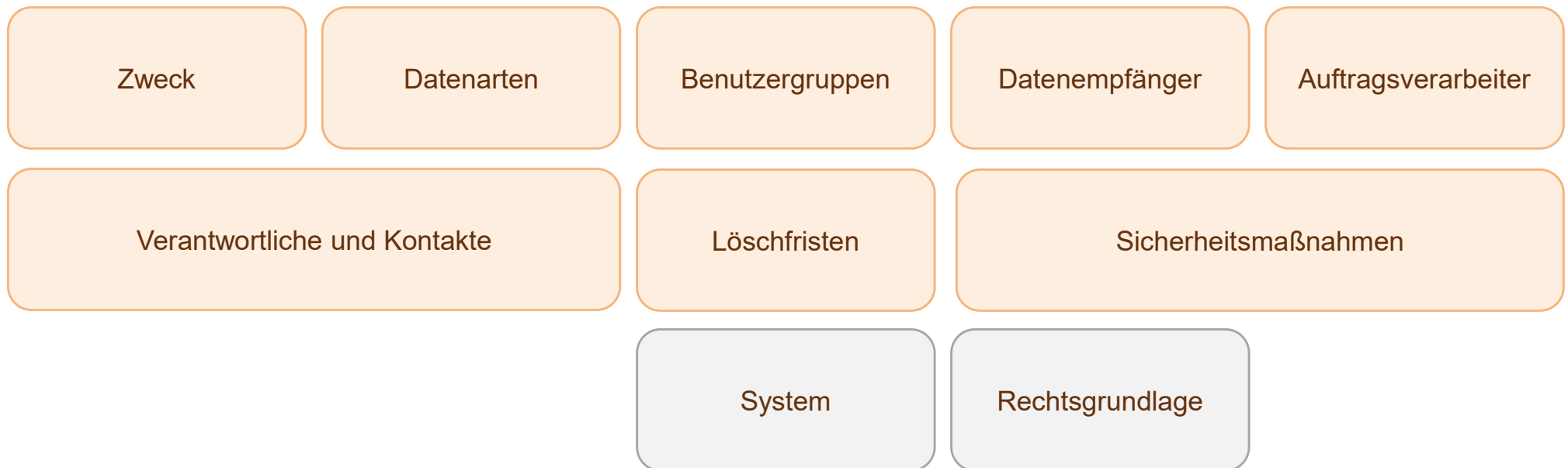
Legende

CRM = Customer Relationship Management
OTA = Online Travel Agency (Booking, Expedia)
PMS = Property Management System
POS = Point of Sale
IBE = Internet Booking Engine



Datenflüsse und Systeme kennen

- Systemliste oder grafische Übersicht mit Datenwegen
- **Verzeichnis von Verarbeitungstätigkeiten:**



Dienstleister prüfen

- Gibt es mit jedem meiner Dienstleister einen Vertrag nach Art. 28 DSGVO?
- Sind Unterauftragnehmer, Datenstandorte und mögliche Drittlandzugriffe bekannt?
- Welche Sicherheitsmaßnahmen, Kommunikationswege und Löschprozesse sind vereinbart?
- Kann und wird der Anbieter bei Auskunft, Vorfällen und Prüfung unterstützen?



Verwaltung von Bedienern

- Sind in den Systemen sinnvolle Benutzergruppen und –rechte angelegt?
- Hat jeder Nutzer einen eigenen Zugang?
- Sind in den Systemen MFA aktiviert?
- Werden Änderungen bei Rollenwechsel und Austritt zeitnah und korrekt durchgeführt?



Nur notwendige Daten zeigen



- Liegen Gästelisten offen auf?
- Werden E-Mails vor Versand geprüft auf Empfänger und Anhänge?
- Werden Listen und Ausdrücke nach Verwendung sicher archiviert oder entsorgt?



Aufbewahrungsfristen einhalten

- Werden die Daten entsprechend der gesetzlichen Aufbewahrungsfrist aufbewahrt?
- Werden Daten nach Zweckende gelöscht oder anonymisiert, sofern keine Pflicht oder Rechtsverteidigung entgegensteht?
- Werden Löschlauf und Ausnahmen dokumentiert?



Bearbeitung von Betroffenenrechten

- Leiten meine Mitarbeiter eine Anfrage sofort an die richtige Stelle weiter?
- Wie prüfe ich die Identität und wie lange habe ich Zeit, um zu antworten?
- Wie führe ich die Daten aus meinen Systemen zusammen?
- Wie verfasse ich eine Antwort oder Ablehnungen eines Betroffenenrechts?



Praxis: “Löschen Sie alle meine Daten!”

Fall: Herr Huber schreibt eine E-Mail an das Hotel H3 mit der E-Mail Adresse: office@h3hoteltraining.at und folgendem Inhalt:

*„Sehr geehrte Damen und Herren,
bezugnehmend auf Ihre E-Mail von gestern, in der Sie mich über
einen Hackerangriff informiert haben, ersuche ich Sie, meine
personenbezogenen Daten im Zusammenhang mit meinem
Aufenthalt vom 5. bis 10. Juli 2026 umgehend zu löschen.
Bitte löschen Sie auch die Daten meiner Begleitpersonen. Ich
ersuche Sie um eine Bestätigung, sobald die Löschung erfolgt ist.*

*Mit freundlichen Grüßen
Markus Huber“*





Marketing und Gästedaten



Zusammenarbeit mit Agenturen

- Social-Media- und Werbekonten sollten dem Hotel gehören.
- Agenturen erhalten eigene, auf ihre Aufgabe beschränkte Zugänge.
- Passwörter werden nicht geteilt; Zugriffe werden regelmäßig geprüft.



Website und Buchungstrecke

- Impressum und Datenschutzhinweise: leicht auffindbar und aktuell.
- Kontakt- und Buchungsformulare sollten nur jene Angaben abfragen, die für den jeweiligen Schritt benötigt werden.
- Nicht notwendige Cookies und Werbe- oder Tracking-Pixel dürfen erst nach der erforderlichen Einwilligung laden.
- Consent Banner: „Akzeptieren“ und „Ablehnen“ müssen eine echte, gleichwertige Wahl ermöglichen.
- Karten, Videos oder Social-Media-Inhalte können bereits beim Laden Daten an externe Anbieter übertragen.
- Die Web-Booking-Engine gehört in die Prüfung mit hinein.



Newsletter: Einwilligung oder Bestandskunde

SCHRITT 1 · VORRANGIG PRÜFEN



Geltungsbereich

Werbliche Newsletter per E-Mail (inkl. SMS) an Hotelgäste mit Empfänger in Österreich. Reine Buchungs- und Servicenachrichten ohne Werbecharakter sind nicht Gegenstand.



Newsletter: Einwilligung oder Bestandskunde

SCHRITT 2 · RECHTSGRUNDLAGE FÜR DEN VERSAND



2 Wirksame, nachweisbare Einwilligung vorhanden?

Ja

Nein

Weiter mit Schritt 4

Abschließende Kontrolle vor dem Versand

Weiter mit Schritt 3

Bestandskundenausnahme prüfen

Anforderungen an die Einwilligung

- Freiwillig, informiert, unmissverständlich (Art. 6 Abs. 1 lit. a DSGVO)
- Aktiv erteilt, keine vorangekreuzte Checkbox
- Kopplungsverbot
- Jederzeit widerruflich



Newsletter: Einwilligung oder Bestandskunde

SCHRITT 3 · BESTANDSKUNDENAUSNAHME (§ 174 ABS. 4 TKG 2021)



A

E-Mail-Adresse im Zusammenhang mit dem Verkauf oder einer Dienstleistung erhalten (z. B. Zimmerbuchung)

B

Werbung ausschließlich für eigene, ähnliche Produkte oder Dienstleistungen des Hotels

C

Klare, kostenfreie und problemlose Ablehnungsmöglichkeit bereits bei der Erhebung und zusätzlich bei jeder Übertragung

D

Kein vorheriger Widerspruch, insbesondere kein Eintrag in der ECG-Liste der RTR-GmbH (§ 7 Abs. 2 ECG)

3

Sind alle vier Voraussetzungen (A,B,C,D) vollständig erfüllt?

Alle vier müssen kumulativ erfüllt sein.

Ja

Weiter mit Schritt 4

Abschließende Kontrolle vor dem Versand

Nein

Einwilligung einholen

Kein Versand ohne Rechtsgrundlage.
Aktiv, getrennt von anderen Erklärungen und dokumentiert.

EuGH C-654/23 (13.11.2025)

Ist die Ausnahme vollständig erfüllt, braucht der Versand selbst keine zusätzliche Rechtsgrundlage nach Art. 6 DSGVO. Tracking und Profiling bleiben gesondert zu prüfen.



Newsletter: Einwilligung oder Bestandskunde

SCHRITT 4 · ABSCHLIEßENDE KONTROLLE VOR DEM VERSAND



Vor dem Versand prüfen:

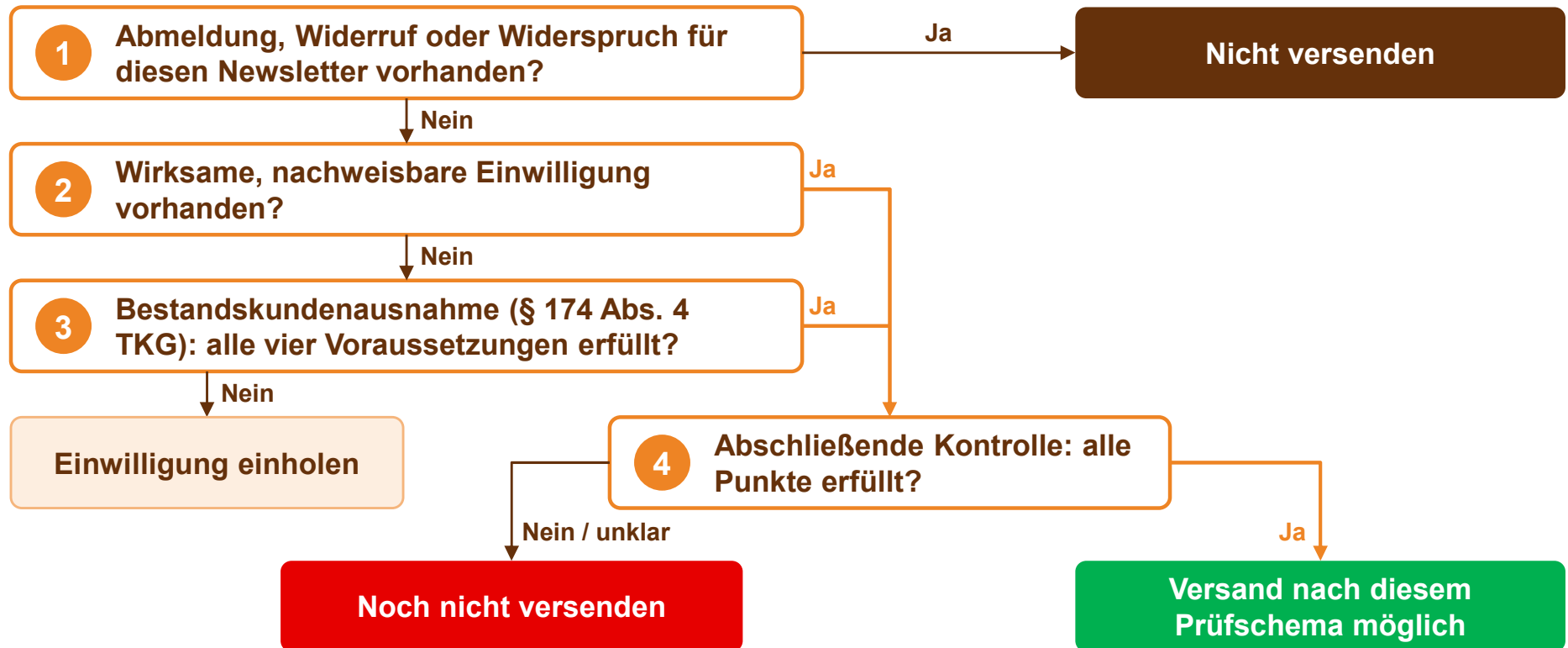
- Funktionierender Abmeldelink in jeder E-Mail
- Absenderidentität und Impressum erkennbar (§ 174 Abs. 5 TKG)
- Datenschutzinformation passend zum Zweck
- Datenminimierung: in der Regel genügt die E-Mail-Adresse (Art. 5 DSGVO)
- Externer Newsletter-Dienstleister: Auftragsverarbeitung (Art. 28 DSGVO); bei Anbietern außerhalb des EWR Drittlandtransfer prüfen
- Tracking und Erfolgsmessung als eigene Datenverarbeitung bewerten
- Rechtsgrundlage im Verarbeitungsverzeichnis dokumentieren
- ECG-Liste der RTR-GmbH bei jedem Versand mit Bestandskundenausnahme berücksichtigen



Newsletter: Einwilligung oder Bestandskunde

GESAMTÜBERSICHT · DSGVO + TKG 2021 (ÖSTERREICH)

1 2 3 4



Rechtsquellen: DSGVO Art. 5, 6, 7, 28 · TKG 2021 § 174 (RIS, geltende Fassung) · ECG § 7 Abs. 2 (ECG-Liste) · EuGH 13.11.2025, C-654/23 Inteligo Media

Praxisquellen: WKO – Einwilligungserklärung für Newsletter (TKG/DSGVO) · Datenschutzbehörde (DSB), FAQs Direktwerbung · RTR-GmbH, ECG-Liste

Stand 13. Oktober 2026 · Vereinfachte Darstellung für die Marketingpraxis; ersetzt keine Rechtsberatung im Einzelfall.



Tracking und Retargeting

- Tracking erfasst z.B. besuchte Angebotsseiten oder begonnene Buchungen.
- Retargeting spricht Website-Besucher:innen später erneut mit Werbung an.
- Vorab prüfen: Welche Tools und Daten sind auf der Website und Buchungstrecke im Einsatz?
- Werbe-Pixel erst nach der erforderlichen Einwilligung laden.
- Gästelisten aus PMS oder CRM nur nach Prüfung übermitteln.
- Gesundheitsdaten oder daraus ableitbare Interessen sind nicht in Werbezielgruppen zu verwenden.



Verwendung von KI

- Echte Namen, Buchungsdetails, Beschwerden oder besondere Wünsche gehören nicht ungeprüft in ein KI-Tool.
- Wenn Gästedaten für eine KI-Anwendung benötigt werden, müssen Tool, Datenverwendung und Schutzmaßnahmen vorher geprüft werden. Wo möglich, den Sachverhalt anonymisieren oder verallgemeinern.
- KI-generierte Inhalte vor der Veröffentlichung durch eine verantwortliche Person prüfen lassen.
- Bei Verwendung eines Chatbots ist erkennbar zu machen, dass Gäste mit einem KI-System kommunizieren.





Videoüberwachung



Erst den Anlass klären.

- Welchen konkreten Vorfall oder welches konkrete Risiko soll die Kamera abdecken?
- Ist die Kamera dafür wirklich notwendig?
- Reichen mildere Maßnahmen – etwa bessere Beleuchtung, ein Schließsystem oder ein Bewegungsmelder?
- Zweck und Entscheidung vor der Installation dokumentieren.
- Bei großflächiger oder besonders sensibler Überwachung prüfen, ob eine DSFA nötig ist.



Nur den notwendigen Bereich erfassen.

- Bildausschnitt und Betriebszeiten auf das notwendige Maß begrenzen.
- Öffentliche Flächen und Nachbargrundstücke möglichst ausblenden.
- Keine Kameras in Gästezimmern, Sanitäranlagen, Duschen oder Umkleiden.
- Mitarbeitende dürfen nicht zur Kontrolle ihrer Arbeitsleistung oder ihres Verhaltens überwacht werden.
- Küchen und Pausenräume sind während der Arbeitszeit besonders problematisch.



Vor dem Start: Informieren und Zugriffe begrenzen.

- Hinweisschilder müssen sichtbar sein, **bevor** Gäste oder Mitarbeitende den überwachten Bereich betreten.
- Mitarbeitende vor der Inbetriebnahme informieren und arbeitsrechtliche Vorgaben prüfen.
- Jede Kamera dokumentieren: Standort, Zweck, Bildausschnitt, Betriebszeit und Speicherdauer.
- Nur wenige berechtigte Personen dürfen Aufnahmen ansehen.
- Aufnahmen nur bei einem konkreten Anlass auswerten und nicht weiterveröffentlichen.



Speichern und löschen: So kurz wie möglich.

- Aufnahmen löschen, sobald sie für den festgelegten Zweck nicht mehr benötigt werden.
- Die DSB nennt 72 Stunden als grundsätzlichen Richtwert. Eine längere Speicherung braucht eine nachvollziehbare Begründung.
- Bei einem Vorfall nur die relevante Sequenz sichern und den Zugriff dokumentieren.



Praxisfall: Kamera im Küchenbereich

Ein Gastronomiebetrieb filmte dauerhaft den Küchen- und Abholbereich, in dem Mitarbeitende arbeiteten. Die Aufnahmen wurden 14 Tage gespeichert.

Die DSB verhängte 2023 eine Geldbuße von 20.000 Euro.

Ein nachvollziehbares Schutzinteresse rechtfertigt nicht automatisch jeden Kamerastandort und jede Speicherdauer.

Quelle: Österreichische DSB, Datenschutzbericht 2023, S. 54; Straferkenntnis D550.731





Datenverlust



Was ist eine Datenschutzverletzung?

- Vertraulichkeit: Unbefugte sehen Gästedaten.
- Integrität: Reservierungen werden verändert oder manipuliert.
- Verfügbarkeit: Das Hotel kann auf wichtige Daten nicht mehr zugreifen.

Beispiele:

gestohlener Laptop

Vorfall bei einem Systemanbieter

Fehlversand

kompromittiertes Konto



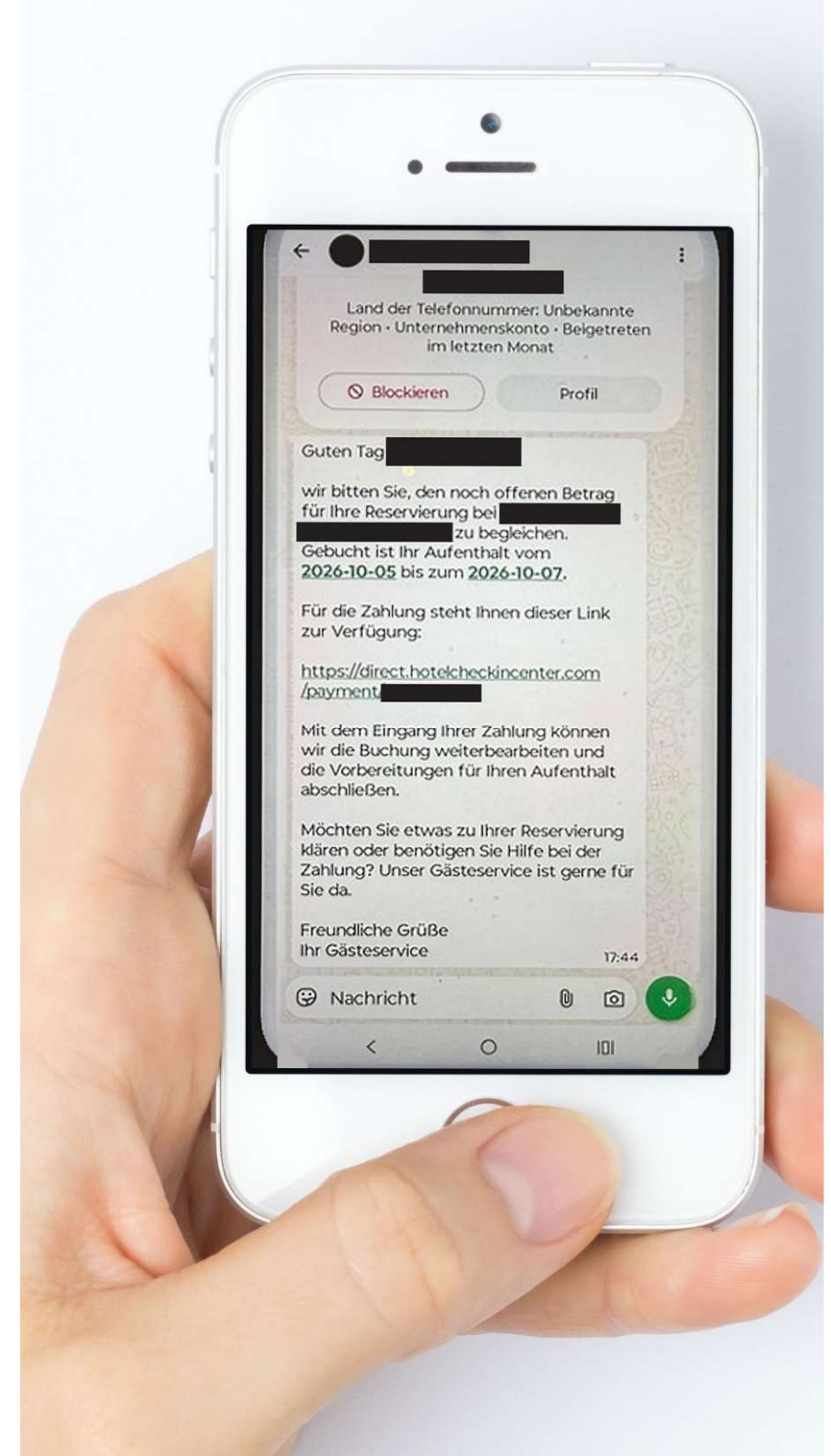
Datenverlust vermeiden und vorbereitet sein.

- **Zugänge schützen:** persönliche Benutzerkonten, starke Passwörter und Mehr-Faktor-Authentifizierung nutzen.
- **Zugriffe begrenzen:** Mitarbeitende erhalten nur jene Berechtigungen, die sie für ihre Aufgabe brauchen.
- **Systeme pflegen:** Updates zeitnah einspielen und Backups regelmäßig testen.
- **Team sensibilisieren:** verdächtige E-Mails, Links und Zahlungsaufforderungen erkennen; Gästedaten nur über sichere Wege teilen.
- **Für den Ernstfall vorsorgen:** interne Ansprechpersonen und Notfallkontakte festlegen.
- **Dienstleister einbinden:** sofortige Meldung, konkrete Informationen und Unterstützung im Vorfall vereinbaren.
- **Ablauf üben:** Team auf Gästeanfragen vorbereiten und den Vorfallsplan regelmäßig testen.



Praxis: Ein Gast meldet eine verdächtige Nachricht

Praxisfall: Ein Gast erhält eine WhatsApp mit seinem richtigen Aufenthaltsdatum und der Aufforderung, nochmals zu bezahlen.



Praxis: Ein Gast meldet eine verdächtige Nachricht

Praxisfall: Ein Gast erhält eine WhatsApp mit seinem richtigen Aufenthaltsdatum und der Aufforderung, nochmals zu bezahlen.

- Nachricht und Absender sichern lassen.
- Nicht vorschnell annehmen, woher die Daten stammen.
- Team, IT und betroffenen Systemanbieter sofort informieren.
- Prüfen, ob Hotel oder Partner tatsächlich betroffen sind.



Sofort handeln: stoppen und sichern.

- Interne Ansprechperson, Geschäftsführung und IT einbinden.
- Betroffene Zugänge sperren oder Passwörter zurücksetzen.
- Weitere Offenlegung möglichst rasch stoppen.
- Protokolle, E-Mails, Nachrichten und Zeitpunkte sichern.
- Eine Person führt die Vorfalldokumentation.



Beim Anbieter konkrete Antworten einholen.

- Welche Systeme und Daten sind betroffen?
- Seit wann besteht der Vorfall – und wann wurde er entdeckt?
- Wie viele Gäste könnten betroffen sein?
- Wurden Daten eingesehen, kopiert, verändert oder gelöscht?
- Welche Maßnahmen wurden bereits gesetzt?



Auch die eigenen Systeme prüfen: Ein Vorfall beim Anbieter schließt einen Zugriff auf Hotelkonten oder Hotelgeräte nicht aus.



Risiko bewerten und Entscheidung festhalten

- Welche Gäste oder Mitarbeitenden sind betroffen?
- Welche Daten sind betroffen – etwa Name, Kontaktdaten, Aufenthalt oder Zahlungsdaten?
- Welche Folgen sind für die Betroffenen möglich?
- Welche Maßnahmen senken das Risiko?
- Bewertung und Entscheidung dokumentieren – auch wenn keine Meldung erfolgt.



Melden und Betroffene informieren

- Datenschutzbehörde: unverzüglich und möglichst binnen 72 Stunden melden, wenn voraussichtlich ein Risiko besteht.
- Meldung gemäß Art. 33 DSGVO
- Betroffene Personen: unverzüglich informieren, wenn voraussichtlich ein hohes Risiko besteht.
 1. verständlich erklären, was passiert ist und welche Daten betroffen sein könnten
 2. bereits gesetzte Maßnahmen und eine Kontaktmöglichkeit nennen
 3. vor verdächtigen Links und Zahlungsaufforderungen warnen
 4. Gästen empfehlen, das Hotel nur über bekannte Kontaktdaten zu kontaktieren
- Die Einschätzung und die Entscheidung dokumentieren.





Datenschutz der im Hotelalltag funktioniert

“Ich unterstütze, wo Datenschutz im Hotelalltag konkret wird: bei Abläufen, Systemen und Ihren Fragen. Gemeinsam prüfen wir den aktuellen Stand, priorisieren die nächsten Schritte und entwickeln auf Ihr Hotel abgestimmte praxistaugliche Lösungen. Ich schule Ihr Team und begleite bei konkreten Themen und Herausforderungen. Der erste Schritt ist ein gutes Gespräch.“

*Ihr Hotel, unsere Mission. H3 –
Beratung mit Herz, Hirn und Hand*





Mag. (FH) Annemarie Maurer

Obere Straße 26,
3553 Schiltern bei Langenlois

Telefon: 0664 / 50 46 828

E-Mail: office@h3training.at

www.h3training.at

