Datenschutz Beiblatt

Im Mai 2018 tritt die neue Datenschutz-Grundverordnung (DSGVO) in Kraft. Hoteliers müssen künftig detailliert darlegen, welche Daten ihrer Gäste von ihnen verarbeitet werden, wo diese liegen und wohin sie weitergeben werden. Generell sollten sich Unternehmen gut auf den Einführungstermin der Datenschutzverordnung vorbereiten, denn bei Verstößen drohen Strafen von bis zu 20 Millionen Euro (!) oder vier Prozent des Umsatzes.

Die wichtigsten Punkte betreffen folgende Bereiche:

- **Aktive Einwilligung der Gäste erforderlich.** In den Hotels werden persönliche Daten verarbeitet und die Gäste müssen sich künftig damit einverstanden erklären. Bisher genügte es, dass der Gast der Nutzung nicht aktiv widersprach. Das beutet auch, dass ein Newsletter-Versand oder ein Gästemailing in der Regel nur mit ausdrücklicher Zustimmung des künftigen Empfängers möglich ist. Unter bestimmten Voraussetzungen gibt es für den Versand von Newslettern nun Erleichterungen in Form von einer Ausnahmeregel (*siehe 5.1*).
- **Dokumentationspflicht.** Zu mehr bürokratischem Aufwand für die Hoteliers dürfte die Neureglung der Nachweis- und Rechenschaftspflichten führen. So müssen Hoteliers dokumentieren, dass sie alle geeigneten Maßnahmen ergreifen, um personenbezogene Daten rechtskonform zu bearbeiten. Das Hotel muss also beweisen, dass es alles richtiggemacht hat.

1. Personenbezogene Daten

Personenbezogene Daten sind Informationen über natürliche oder juristische Personen, deren Identität eindeutig bestimmt oder bestimmbar ist, z.B. Adresse/Name.

Beispiele für personenbezogene Daten:

Name	Gewicht	Zuverlässigkeit	Persönliche Interessen
Geburtsdatum	Haar- und Augenfarbe	Karriereplanung	Freizeitverhalten
Geburtsort	Kleidergröße	Persönliche Verhältnisse	Standortdaten
Wohnanschrift	Familienverband	Unwahrheiten	Ortswechsel
Beruf	Wirtschaftliche Lage	Beschimpfungen	Lebenslauf
Staatsangehörigkeit	Kreditwürdigkeit	Verspottung	Schulbesuche
Geschlecht	Charaktereigenschaften	Verleumdungen	Kontaktdaten
Körpergröße	Arbeitseinstellung	Vorlieben	E-Mail-Adresse
Online-Kennung	Sozialversicherungsnummer	Schulden	Aufnahmen des äußeren Erscheinungsbildes (Gesicht, Statur, Haltung)
Benutzernamen	Kontoinformationen	Rechtliche Verhältnisse	Video- und Audioaufnahmen
IP Adresse	Kreditkartennummer	Melderegisternummer	….
Telefonnummer	Einkommen/Gehalt	Personenkennzeichen	

2. Sensible Daten (formunabhängig)

Sensible Daten sind eine spezielle Klasse von personenbezogenen Daten, die auf Grund ihrer Art besonders schutzwürdig sind. Dazu gehören:

- rassische und ethnische Herkunft
- politische Meinung
- Gewerkschaftszugehörigkeit
- religiöse oder philosophische Überzeugung
- Gesundheit oder medizinischer Status
    - Gesundheitszustand
    - Krankengeschichte
    - Körperliche und geistige Verfassung
    - Krankheiten
    - Behinderungen
    - Krankheitsrisiken
    - Vorerkrankungen
    - Erfolgte Behandlungen und Therapien
    - Informationen über körpereigene Substanzen
    - Genetische oder biologische Proben
    - Nummern, Symbole und Kennzeichen im Zuge einer Untersuchung oder Therapie
- Sexualleben bzw. sexuelle Orientierung
- Biometrische Informationen (Gesichtsbild, Stimmbild, Papillarlinien, Irismuster, etc.)
- Genetische Informationen

Diese Aufzählung ist abschließend, d.h. nur die hier aufgezählten Datenarten sind sensibel, weitere gibt es nicht!

Sensible Daten unterliegen damit strengeren Verarbeitungsvoraussetzungen. So ist jedenfalls eine „ausdrückliche“ Einwilligung für die Verarbeitung sensibler Daten erforderlich.

Eine Weitergabe sensibler Daten ist somit generell nur sehr eingeschränkt erlaubt, beispielsweise:

- wenn eine ausdrückliche Zustimmung des Betroffenen vorliegt;
- zur Erfüllung arbeitsrechtlicher Pflichten;
- wenn eine gesetzliche Ermächtigung vorliegt, die Weitergabe in einem angemessenen Verhältnis zum verfolgten Ziel steht und die Verarbeitung aufgrund eines erheblichen öffentlichen Interesses erforderlich ist;
- wenn lebenswichtige Interessen des Betroffenen oder eines Dritten davon abhängen.

Mitarbeiter sind zu schulen, was sensible Daten im Sinne des Datenschutzgesetzes sind und dazu zu verpflichten, im Umgang mit sensiblen Daten und einer Datenweitergabe in diesem Bereich noch sorgsamer zu sein.

3. Betroffener (Gast)

Ein sogenannter Betroffener ist jede, vom Auftraggeber verschiedene, natürliche oder juristische Person oder Personengemeinschaft, deren personenbezogene Daten verwendet oder verarbeitet werden.

4. Dienstleister (Auftragsdatenverarbeiter)

Ein sogenannter Dienstleister oder Auftragsdatenverarbeiter ist jede natürliche oder juristische Person, Personengemeinschaft oder Organ einer Gebietskörperschaft, die datenschutzrechtlich relevante Daten nur zur Herstellung eines ihnen aufgetragenen Werkes verwendet bzw. verarbeitet. Dienstleister oder Auftragsdatenverarbeiter werden dann zu Auftraggebern bzw. Verantwortlichen, wenn sie Daten zu einem anderen als dem ihnen aufgetragenen Zweck verwenden.

Mit jedem dieser Auftragsdatenverarbeiter ist ein Vertrag abzuschließen, der die genauen Rechte und Pflichten der beiden Vertragspartner regelt und dokumentiert. Ein solcher Vertrag wird Auftragsdatenverarbeitervereinbarung (ADV) genannt.

5. Zustimmungserklärung

Jeder Betroffene muss grundsätzlich der Verarbeitung und Verwendung seiner Daten zustimmen. *Ausgenommen sind nur Daten, für die eine gültige Verpflichtung durch eine Rechstnorm besteht. Ein Beispiel dafür wären Daten, deren Verwendung und Speicherung das Sozialversicherungsgesetz vorschreibt.*

Eine solche Zustimmungserklärung hat gewissen Formvorschriften zu folgen. Dazu gehört, dass sie freiwillig und in voller Kenntnis der Sachlage und aller möglichen Folgen und Risiken für den Gast gegeben wurde. Andernfalls ist eine gegebene Zustimmung nicht gültig, unabhängig davon, ob der Gast nun mit der Verarbeitung bzw. Verwendung seiner Daten einverstanden wäre oder nicht. Eine eventuelle Androhung disziplinarer oder anderer Konsequenzen durch den Auftraggeber schließt die Freiwilligkeit und damit auch die Gültigkeit einer Zustimmungserklärung aus. Eine Zustimmungserklärung hat auch zu enthalten, welche Daten des Gastes zu welchem Zweck verarbeitet und an wen sie übermittelt werden. Das Verfassen einer Zustimmungserklärung obliegt dem Auftraggeber.

Beispielhafter Formulierungsvorschlag:

„Der Vertragspartner stimmt zu, dass seine persönlichen Daten, nämlich … (die Datenarten genau aufzählen, z.B. „Name“, „Adresse“, etc) zum Zweck der … (genaue Zweckangabe, z.B. „zur Zusendung von Werbematerial über die Produkte der Firma …“) bei der Firma NN gespeichert werden. Diese Einwilligung kann jederzeit bei … (Angabe der entsprechenden Kontaktdaten) widerrufen werden.“

5.1. Ausnahmeregelung für E-Mail-Werbung

Ausnahmen für den Versand von Newslettern bestehen für den Versand an frühere und bestehende Geschäftsbeziehungen (§ 107 Abs. 3 TKG). So kann ein Hotelier auch ohne Einwilligung einen Newsletter versenden, wenn er im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung vom Gast dessen E-Mail-Adresse erhalten hat. **Auf die Widerspruchsmöglichkeit** muss der Gast jedenfalls **bereits bei der Erhebung der E-Mail-Adresse** und bei jeder unaufgeforderten Zusendung **hingewiesen werden**.

6. Rechte & Pflichten

Das österreichische Datenschutzgesetz definiert Rechte und Pflichten für Auftraggeber, Dienstleister und Betroffene (Gäste).

6.1. Auskunftsrecht

Der Auftraggeber hat jeder Person, auf schriftlichen Antrag mit Identitätsnachweis, innerhalb von 8 Wochen unentgeltlich Auskunft über die zu dieser Person verarbeiteten Daten zu geben (Löschungsverbot für 4 Monate!). Die Auskunft hat folgendes zu beinhalten:

- alle verarbeiteten Daten
- Herkunft der Daten
- allfällige Empfänger
- Zweck der Verarbeitung
- Rechtsgrundlage der Verarbeitung
- allfällige Dienstleister

6.2. Richtigstellungs- bzw. Löschungsrecht

Der Auftraggeber hat unrichtige oder entgegen den Bestimmungen des Datenschutzgesetzes verarbeitete Daten innerhalb von 8 Wochen richtigzustellen oder zu löschen, und zwar aus eigenem Antrieb, wenn der Zweck nicht mehr gegeben ist, oder auf Antrag. Es sei denn, es widerspricht anderen gesetzlichen Vorgaben (Archivierungsdauer). Der Antragsteller ist vom Auftraggeber aktiv über die durchgeführte Löschung bzw. Richtigstellung zu informieren.

6.3. Widerrufsrecht

Sofern die Verwendung von Daten nicht gesetzlich vorgesehen ist, hat jeder Betroffene das Recht, Widerruf einzulegen gegen die Verwendung seiner personenbezogenen oder sensiblen Daten (eigene bzw. freiwillige Veröffentlichung negiert nicht die Schutzwürdigkeit!!). Der Auftraggeber hat daraufhin die Daten des Betroffenen binnen 8 Wochen aus der Datenanwendung zu löschen und umgehend allfällige Übermittlungen zu unterlassen. Jeder Betroffene hat jederzeit das Recht, bereits erteilte Zustimmungen zur Verarbeitung seiner Daten ohne Angabe von Gründen zu widerrufen.

6.4. Spezialfall Videoüberwachung

Der Betrieb einer Hotel-Videoüberwachungsanlage unterliegt speziellen Regelungen. Zwar sind die dabei verarbeiteten Daten per Definition nicht sensibel, trotzdem ist die Verwendung der Anlage unter bestimmten Voraussetzungen genehmigungspflichtig. Zu diesen Voraussetzungen gehört, dass Videodaten tatsächlich abgespeichert werden. Eine reine Live Übertragung ist (meist) nicht genehmigungspflichtig.

Die maximale Aufbewahrungsdauer von Videodaten beträgt 72 Stunden. Danach sind diese Daten in jedem Fall zu löschen bzw. ist die Videoüberwachungsanlage so zu konfigurieren, dass Videodaten, die älter als 72 Stunden sind, automatisch gelöscht oder überschrieben werden. Die einzige Ausnahme von dieser Regel ist ein Auskunftsbegehren. In diesem Fall müssen die Daten 4 Monate lang aufbewahrt werden.

6.5. Data Breach Notification Duty

Die Data Breach Notification Duty beschreibt die Verpflichtung, sämtliche Verstöße gegen die Datenschutzregeln der entsprechenden Aufsichtsbehörde zu melden.

Österreichische Datenschutzbehörde
Hohenstaufengasse 3, 1010 Wien
E-Mail: dsb@dsb.gv.at

Diese Verpflichtung impliziert natürlich die Fähigkeit und die Pflicht von Unternehmen, in der Lage zu sein, eventuelle Verstöße überhaupt feststellen zu können. Weiters geht damit auch eine sorgfältige und umfangreiche Dokumentationspflicht einher.

Zusammengefasst macht diese Verpflichtung eine gründliche und umfassende Überwachung notwendig, die natürlich den Anforderungen des Datenschutzes zu entsprechen hat.

7. Datenschutz Folgeabschätzung

Die **Datenschutz Risiko- und Folgeabschätzung** gehört zu den erweiterten Dokumentationspflichten.

In einem ersten Schritt soll eine Risikobewertung für die identifizierten Risiken der Verarbeitungstätigkeiten durchgeführt werden (Abschätzung Eintrittswahrscheinlichkeiten und Auswirkungen). Wenn aus Sicht der betroffenen Personen voraussichtlich ein hohes Risiko besteht, ist eine Datenschutz-Folgenabschätzung durchzuführen. Diese muss für Datenverarbeitungen mit erkennbarem Risiko (z.B. Big Data, Profiling, Verwendung sensibler Daten) durchgeführt und dokumentiert werden.

Bestandteile dieser Datenschutz Folgeabschätzung sind zumindest:

- Dokumentation des Anwendungsdesigns
- Anwendungsbeschreibung
- mögliche Risiken und deren Eintrittswahrscheinlichkeit
- Restrisiken
- Kontrollmaßnahmen

8. Verfahrensverzeichnis

Die Melde- und Genehmigungspflicht im DVR entfällt. Als Ersatz dient das sogenannte **Verfahrensverzeichnis**, das im Grunde dieselben Informationen enthält wie das DVR, aber nun von den Unternehmen selbst zu erstellen ist.

Für alle Datenanwendungen ist ein solches Verfahrensverzeichnis mit diversen Detailangaben anzulegen. Dieses Verfahrensverzeichnis hat mindestens folgende Informationen zu enthalten:

- Kontaktdaten der Beteiligten
- den Zweck der Verarbeitung
- die Rechtsgrundlage der Verarbeitung
- verwendete Daten(kategorien)
- beteiligte Empfänger(kategorien)
- die Speicherdauer
- getroffene Datensicherheitsmaßnahmen
- durchgeführte Datentransfers

Nach der DSGVO sind die Löschfristen bzw. Aufbewahrungsfristen nach Möglichkeit ins Verfahrensverzeichnis aufzunehmen. Beispielsweise kann bei unbefristeten Verträgen keine konkrete Löschfrist angegeben werden, da der konkrete Vertragsablauf unbestimmt ist. Es empfiehlt sich hier allerdings eine abstrakte Frist anzugeben (z.B. „nach Ablauf des Vertrages“).

9. Weitere Dokumentationspflichten

Weitere Dokumentationspflichten sind u.a.:

- Sicherstellung und Dokumentation der Einhaltung datenschutzrechtlicher Bestimmungen für interne Prozesse
- Datenschutzkonzept inkl. entsprechender Regelungen und Richtlinien
- Mitarbeitersensibilisierung
- Auftragsverarbeitungsverträge
- Sicherstellung der Einhaltung und Dokumentation der Datenschutzprozesse (Auskunft, Löschung, Richtigstellung, Widerruf, Portabilität, Data Breach Notification Duty, etc.)
- Datenschutzerklärungen
- Zustimmungserklärungen und deren Einholung
- Berechtigungs- und Rollenkonzepte
- Standardvertragsklauseln

Rückfragen & Kontakt:

PRODINGER TOURISMUSBERATUNG
Thomas Reisenzahn, t.reisenzahn@prodinger.at
Marco Riederer, m.riederer@prodinger.at

ATRICON GROUP
Christian Steinocher
christian.steinocher@atricongroup.com

ATRICON GROUP

ATRICON positioniert sich als IT- und Unternehmensberatung, die den Business Value seiner Kunden in den Mittelpunkt stellt. Unser Leitsatz „**inspired – designed – realized**“ betont die ganzheitliche Sichtweise, die uns leitet. Wir greifen auf jahrelange Praxis in großen, internationalen Unternehmen zurück. **ATRICON** analysiert die Situation, erarbeitet gemeinsam mit seinen Kunden Lösungen und begleitet die Umsetzung.

PRODINGER BERATUNGSGRUPPE

Als führende Wirtschaftsberatung unterstützt die **PRODINGER BERATUNGSGRUPPE** ihre Kunden in den Geschäftsfeldern **Steuerberatung, Unternehmensberatung, Tourismusmarketing und Tourismusberatung**. Die Firmengruppe hat Spezialisten in den Branchen Tourismus, Bau- und Baunebengewerbe, Immobilienwirtschaft, freiberufliche Tätigkeiten, Handel, Gewerbe und Dienstleistung. Die Beratungsgruppe hat Standorte in Bad Hofgastein, Bozen, Innsbruck, Lech am Arlberg, Linz, Mittersill, München, Saalfelden, Salzburg, St. Johann im Pongau, Velden, Wien und Zell am See.

Die Netzwerkgruppe betreut aktuell mehr als 6.000 Kunden, davon über 500 Hotelbetriebe, 30 Destinationen und 40 Bergbahnen. Derzeit sind 250 Mitarbeiterinnen und Mitarbeiter an 13 Standorten tätig.

Die PRODINGER BERATUNGSGRUPPE ist Mitglied in mehreren Netzwerken. Die Prodinger Steuerberatung ist unabhängiges Mitglied der GGI Geneva Group International. Die Prodinger Tourismusmarketing ist integriert in der Serviceplan Gruppe bei Saint Elmo´s Travel mit 26 Standorten weltweit.