HotellerieSuisse

Neue europäische Datenschutzgrundverordnung (DSGVO) – Anwendbarkeit und Auswirkungen auf Schweizer Beherbergungsbetriebe (Stand: Dezember 2017)

1. Anwendbarkeit der DSGVO auf Schweizer Unternehmen

Die neue europäische Datenschutzgrundverordnung (DSGVO) tritt am 25. Mai 2018 in Kraft. Sie gilt nicht nur für in der EU niedergelassene Unternehmen, sondern unter gewissen Voraussetzungen unmittelbar auch für schweizerische Unternehmen, beispielsweise wenn diese Unternehmen Kunden aus der EU haben und ihnen dort Waren oder Dienstleistungen anbieten und in dem Zusammenhang auch Personendaten (Name, Adresse, E-Mail, Geburtsdatum, Bankdaten etc.) verarbeiten.

Schweizer Beherbergungsbetriebe haben somit die Regeln der neuen DSGVO zu beachten, wenn sie ihre Dienstleistungen (Beherbergung) EU-Bürgern innerhalb der EU anbieten. Dies kann insbesondere über die eigene Webseite erfolgen, mit welcher auch EU-Bürger Reservationen tätigen können. Nicht erfasst werden Unternehmungen, die ihre Dienstleistungen ausschliesslich in der Schweiz anbieten.

Aufgrund dieser Ausgangslage ist davon auszugehen, dass die Mehrheit der Hotelbetriebe auch der DSGVO unterstellt sein wird, soweit diese Personendaten von EU-Bürgern verarbeiten.

Der Begriff «Verarbeiten» umfasst das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von personenbezogenen Daten.

2. Die Grundprinzipien der DSGVO

- **Rechtmässigkeit, Verarbeitung nach Treu und Glauben, Transparenz**
  Personenbezogene Daten müssen auf rechtmässige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

- **Zweckbindung**
  Die Verarbeitung der Daten muss einem eindeutigen, festgelegten Zweck dienen, und die Daten dürfen nur für diesen konkreten Zweck verwendet werden.

- **Datenminimierung**
  Es dürfen nur diejenigen Daten verarbeitet werden, die für den (definierten) Zweck notwendig sind.

- **Richtigkeit**
  Die personenbezogenen Daten müssen sachlich richtig sein. Es sind alle angemessenen Massnahmen zu treffen, damit unrichtige Daten unverzüglich gelöscht oder berichtigt werden.

- **Speicherbegrenzung**
  Die Speicherfristen für personenbezogene Daten sind auf das erforderliche Mindestmass zu beschränken.

- **Integrität & Vertraulichkeit**
  Der Schutz personenbezogener Daten muss durch geeignete technische und organisatorische Massnahmen gewährleistet sein, einschliesslich Schutz vor unbefugter oder unrechtmässiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

- **Rechenschaftspflicht**
  Der Verantwortliche ist für die Einhaltung der genannten Grundsätze verantwortlich und muss deren Einhaltung nachweisen können. Verantwortlicher im Sinne der DSGVO ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

3. Die wichtigsten Regelungen in der DSGVO (Auswahl)

3.1 Rechtmässigkeit der Verarbeitung von Daten

Die Datenverarbeitung (bspw. die erstmalige Erhebung von Gästedaten) ist erlaubt, wenn unter anderem mindestens eine der folgenden Voraussetzungen erfüllt ist:

- Die Datenverarbeitung ist für die **Erfüllung eines Vertrags** erforderlich, dessen Vertragspartei die betroffene Person ist oder für **vorvertragliche Massnahmen** auf deren Anfrage hin (bspw. im Zusammenhang mit dem Abschluss eines Gästeaufnahmevertrages oder einer Reservation).

- Die Datenverarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung** des Verantwortlichen nötig (bspw. gesetzliche Pflicht, die Gäste einen Hotel-Meldeschein ausfüllen zu lassen).

- Die Verarbeitung ist zur **Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich** (bspw. Direktwerbung an ehemalige Gäste), solange die Interessen oder die elementaren Rechte der betroffenen Person nicht überwiegen.

- Es liegt die ausdrückliche **Einwilligung** der betroffenen Person vor.

Die **Einwilligung** muss durch eine eindeutige, bestätigende Handlung erfolgen (bspw. aktives Häkchen-Setzen). Eine stillschweigende Zustimmung oder eine bereits mit einem Häkchen versehene Checkbox bzw. eine Checkbox, die aktiv angeklickt werden muss (sog. Opt-OutOptionen) genügen den Anforderungen nicht.

Bei der Verarbeitung **sensibler Daten**, also beispielsweise solcher betreffend Religion, Gesundheit oder biometrischer Daten (z.B. Foto, Fingerabdruck) bedarf es immer einer ausdrücklichen Einwilligung der betroffenen Person.

Bei mehreren verschiedenen Datenverarbeitungen muss die Zustimmung für jede einzelne Verarbeitungstätigkeit vorliegen.

Die betroffene Person kann ihre Einwilligung jederzeit widerrufen. Es muss sichergestellt werden, dass dieser Widerruf genauso einfach erfolgen kann, wie die Einwilligung selbst (bspw. mit einem „Unsubscribe“-Link im Newsletter).

Wichtig: die betroffene Person muss vor Abgabe der Einwilligung über das Recht zum Widerruf der Einwilligung in Kenntnis gesetzt werden.

Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so sollte die betroffene Person jederzeit unentgeltlich Widerspruch gegen eine solche Verarbeitung einlegen können. Die betroffene Person ist ausdrücklich auf dieses Recht hinzuweisen; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

Beispiel einer Formulierung:

„Der Vertragspartner stimmt zu, dass seine persönlichen Daten (z.B. Name, E-Mail-Adresse) zum Zweck der … (z.B. zur Zusendung von Newslettern oder Werbematerial über die Dienstleistungen des Hotels xx) beim Hotel xx gespeichert werden. Diese Einwilligung kann jederzeit bei … (Kontaktdaten, E-Mail-Adresse) widerrufen werden.“

3.2 Rechte der betroffenen Person bzw. Pflichten der Datenverarbeitenden

- **Informationspflichten**

Werden Daten erhoben, muss die betroffene Person gleichzeitig über diesen Umstand informiert werden; dies gilt auch für den Fall, dass die Datenerhebung nicht direkt bei der betroffenen Person erfolgt. Die Informationen müssen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt werden. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch.

Bei einer Reservation beispielsweise via Webseite des Hotels sollten die Informationen direkt zur Verfügung stehen. Allenfalls können die Informationen via Link auf das entsprechende Dokument/die Webseite bei der Reservationsbestätigung übermittelt werden.

Die Informationen haben zwingend das Folgende zu beinhalten:

- Name und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten (falls vorhanden)
- Zweck und Rechtsgrundlage der Verarbeitung
- Berechtigte Interessen (sofern diese als Bearbeitungsgrund angeführt werden)
- Empfänger bzw. Kategorien von Empfängern
- Absicht der Datenübermittlung in Drittland oder an internationale Organisation (sofern vorgesehen)
- Dauer der Speicherung
- Hinweis auf das Bestehen eines Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch und auf Datenübertragbarkeit
- Hinweis auf das Bestehen eines Rechts auf jederzeitigen Widerruf der Einwilligung
- Hinweis auf das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- Information, ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist und mögliche Folgen der Nichtbereitstellung
- Allenfalls: Bestehen einer automatisierten Entscheidungsfindung inkl. Profiling (bspw. automatisierte Bonitätsprüfung)
- Sofern Daten nicht bei der betroffenen Person erhoben wurden: Hinweis auf Quelle, ggf. ob aus öffentlich zugänglicher Quelle
- Information über eine mögliche Zweckänderung der Datenverarbeitung

- **Auskunftsrecht**

Die betroffene Person hat das Recht zu erfahren, ob und welche personenbezogenen Daten vom Betrieb verarbeitet werden, inkl. des Rechts auf Information über Verarbeitungszwecke, Datenkategorien, Empfänger(-kategorien), Speicherdauer, Recht der betroffenen Person auf Berichtigung, Löschung, Einschränkung der Daten, Widerspruchsrecht, Beschwerderecht, Herkunft der Daten und, sofern es stattfindet, das Bestehen einer automatisierten Entscheidungsfindung.

- **Recht auf Berichtigung bzw. Löschung**

Die betroffene Person hat das Recht, falsche Daten berichtigen zu lassen. Personenbezogene Daten sind unter anderem unverzüglich zu löschen, wenn:

- diese für den Zweck, für den sie erhoben wurden, nicht mehr benötigt werden;
- die betroffene Person ihre Einwilligung widerruft und es keine andere Rechtgrundlage zur Erhaltung der Daten gibt (bspw. gesetzliche Pflicht);
- die betroffene Person Widerspruch gegen die Verarbeitung einlegt.

- **Recht auf Datenübertragbarkeit**

Die betroffene Person kann verlangen, dass ihr der Verantwortliche (z.B. Hotelbetrieb) jene Daten, die sie ihm bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format überlässt. Voraussetzung für das Recht auf Datenübertragbarkeit ist, dass die ursprüngliche Verarbeitung auf Grundlage einer Einwilligung oder eines Vertrags und mithilfe automatisierter Verfahren erfolgte.

- **Widerspruchsrecht**

Die betroffene Person kann gegen die Verarbeitung ihrer Daten Widerspruch erheben. Widerspricht die betroffene Person beispielsweise der Verarbeitung für Zwecke der Direktwerbung, so dürfen die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet werden.

3.3 Weitere Pflichten der Datenverarbeitenden (Auswahl)

- **Pflicht zur Datenschutz-Folgeabschätzung**

Bei der Datenschutz-Folgenabschätzung handelt es um eine Risikoanalyse im Vorfeld der Verarbeitung personenbezogener Daten. Sie umfasst unter anderem eine Beschreibung der geplanten Datenbearbeitung, die Risiken, die für die betroffenen Personen entstehen und die Massnahmen, mit denen diese Risiken eingeschränkt oder verringert werden. Die DatenschutzFolgeabschätzung betrifft jedoch nur Datenverarbeitungen, die ein hohes Risiko für Freiheitsrechte von Personen (z.B. Kunden, Nutzer, Mitarbeiter etc.) zur Folge haben (bspw. Gesundheitsdaten, die von Krankenkassen bearbeitet werden). Die übliche Datenverarbeitung durch Hotelbetriebe sollte grundsätzlich kein solch hohes Risiko mit sich bringen.

- **Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen**

Es müssen Massnahmen getroffen werden, die dem Grundsatz des Datenschutzes durch Technik (Data Protection by Design) und durch datenschutzfreundliche Voreinstellungen (Data Protection by Default) gerecht werden. Es ist also sicherzustellen, dass durch entsprechende Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

- **Dokumentationspflichten**

Datenverarbeitende haben ein Verzeichnis (schriftlich oder elektronisch) über ihre Verarbeitungstätigkeiten zu führen, welches unter anderem folgende Punkte zu enthalten hat:

- Namen und die Kontaktdaten des bzw. der Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- Zweck der Verarbeitung;

- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (z.B. Kunden und Lieferanten; Rechnungsdaten, Adressdaten);
- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden (z.B. Polizei, Sozialversicherung), einschliesslich Empfänger in Drittländern oder internationalen Organisationen (Konzernmutter in USA);
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Massnahmen zum Schutz der Daten

4. Mögliche Folgen bei Pflichtverletzungen: hohe Bussen

Die EU droht hohe Bussen an. Für einfachere Verletzungen, wie der Verstoss gegen Pflichten des Verarbeiters, gelten Bussen bis zu EUR 10 Mio. oder 2% des weltweiten Umsatzes des vorangegangenen Jahres. Bei schwerwiegenden Verletzungen drohen Bussen bis zu EUR 20 Mio. oder 4% des weltweiten Jahresumsatzes des vorangegangenen Jahres.

5. Datenschutz in der Schweiz

In der Schweiz wird das Datenschutzgesetz zurzeit ebenfalls revidiert. Viele Regelungen der DSGVO werden gleich oder ähnlich übernommen. Der neue Gesetzesentwurf muss nun vom Parlament beraten werden. Das revidierte DSG wird voraussichtlich anfangs 2019 in Kraft treten. Auch aus diesem Grunde empfiehlt es sich, den neuen Datenschutzregeln bereits Beachtung zu schenken.

6. Vorgehensempfehlungen

- Klären Sie, wer in Ihrem Betrieb für den Datenschutz zuständig ist/sein soll.
- Überprüfen Sie, welche Daten von Personen (Gäste, Mitarbeitende, Lieferanten, WebBesucher etc.) Sie genau bearbeiten, insbesondere solche von in der EU ansässigen Bürgern.
- Handelt es sich um sensible Daten (z.B. Daten zur Gesundheit, Religion)?
- Überprüfen Sie die Rechtsgrundlage für die Verarbeitung der Daten (z.B. gesetzliche Pflicht, Vertrag, berechtigte Interessen, Einwilligung)
- Überprüfen Sie, ob Sie die Daten überhaupt benötigen. Falls nicht, löschen Sie diese.
- Überprüfen Sie Ihre Verträge, AGB, Datenschutzerklärungen bezüglich Vereinbarkeit mit der DSGVO.
- Überprüfen/Erstellen Sie Prozesse/Dokumente, um Ihren Pflichten bezüglich Information, Auskunft, Dokumentation, Datenübertragbarkeit etc. nachkommen zu können.
- Überprüfen Sie den Stand der technischen Datensicherheit.

Weitere Hilfsmittel:

- HOTREC guidelines on the General Data Protection Regulation
- Hilfreiche Checkliste auf der Internetseite der Wirtschaftskammer Österreich

Wichtiger Hinweis:

Dieses Merkblatt enthält eine Zusammenstellung von Informationen bezüglich den neuen EU-Datenschutzbestimmungen. Es soll einen ersten Überblick über die wichtigsten Regelungen vermitteln und als unverbindliche Orientierungshilfe dienen. Die Informationen wurden mit grösstmöglicher Sorgfalt erstellt, es besteht jedoch kein Anspruch auf Vollständigkeit, Richtigkeit und/oder Aktualität.