Neue Datenschutz-Grundverordnung und neues Datenschutzgesetz ...

Die wichtigsten Neuerungen im Überblick!

... ab 25.05.2018 anzuwenden!

GASTROdat®
Hotel. Software & Marketing

EINLEITUNG

Der Grundsatz bleibt wie bisher bestehen: **Datenverarbeitung ist verboten!** Eine Verarbeitung ist nur rechtmäßig, wenn einer der gesetzlich vorgesehenen Ausnahmetatbestände vorliegt.

Der derzeitige **„Auftraggeber“** heißt in der neuen DSGVO **„Verantwortlicher“**. Damit gemeint ist eine *„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“.*

Mit anderen Worten ist derjenige Verantwortlicher – und damit Haftender nach dem Datenschutzgesetz –, der die Daten eingibt, speichert, abändert, löscht und auch sonst entscheidet, was mit ihnen geschieht. Das bedeutet, dass **„Sie als Hotelbetreiber“** auf die Einhaltung der datenschutzrechtlichen Vorschriften achten müssen.

Die GASTROdat GmbH tritt hier als sogenannter „Auftragsverarbeiter“ (derzeit sogenannter „Dienstleister“) auf. Daher ist die GASTROdat GmbH nur für die Programmierung der Software zuständig, um Ihnen eine datenschutzrechlich konforme Verwaltung zu ermöglichen, nicht aber für den Umgang mit den Daten und die Einhaltung der Bestimmungen des Datenschutzgesetzes selbst.

Um Ihnen einen Überblick über Ihre Verantwortungen und die Neuerungen im Mai 2018 zu geben, haben wir im Folgenden die wichtigsten Themen zusammengefasst:

1. Sind die Strafen in der DSGVO wirklich so hoch?

Mit einem Wort: **JA! Der Strafrahmen wird drastisch erhöht**.
Waren im bisherigen Datenschutzgesetz Verwaltungsstrafen in der Höhe von EUR 10.000,-- bis 25.000,-- vorgesehen, beträgt die neue Strafdrohung **bis zu EUR 20 Millionen oder 4 %** des weltweit erzielten Jahresumsatzes Ihres Unternehmens, je nachdem, welcher Betrag höher ist! Zusätzlich birgt ein datenschutzrechtlicher Verstoß immer ein hohes (unternehmerisches) Risiko im Hinblick auf einen **Vertrauensverlust, Imageschaden** und **drohende Klagen** von Mitbewerbern und Betroffenen. Auch strafrechtliche Sanktionen sind möglich.

Konkret drohen Geldbußen für die folgenden Tatbestände:
bis zu **EUR 20 Mio / 4 % des weltweit erzielten Jahresumsatzes** zB bei:

- Zweckü̈berschreitung;
- Verstoß gegen Prinzip der Datenminimierung;
- Verstoß gegen Löschungsverpflichtung;
- unrechtmäßiger Verarbeitung
  (zB ohne Zustimmung der Betroffenen);
- unrechtmäßige Übermittlung von Daten (insb in ein Drittland);
- Nichtbefolgung einer Anweisung der Aufsichtsbehörde.

bis zu **EUR 10 Mio / 2 % des weltweit erzielten Jahresumsatzes** zB bei:

- Fehlen der elterlichen Zustimmung für die Nutzung von Diensten der Informationsgesellschaft durch Kinder unter 16 Jahren (DSG 2018: 14 Jahre);
- Verstoß gegen die Handlungspflichten bei Data Breaches;
- Verstöße gegen die Datenschutz-Folgenabschätzung;
- Verstoß gegen privacy by design und privacy by default;
- Verstöße des Auftragsverarbeiters bei der Datenverarbeitung;
- Verstöße gegen die Pflicht zur Führung von Verarbeitungsverzeichnissen;
- Verstöße gegen die Benennung eines Datenschutzbeauftragten.

2. Was können Sie tun, damit solche Strafen Ihr Hotel nicht in den Ruin treiben?

Für eine datenschutzrechtlich konforme Umsetzung aller rechtlichen Vorgaben werden Sie in vielen Fällen nicht umhin kommen, die Beratung eines Datenschutzexperten einzuholen.

Es gibt jedoch allgemeine Vorgaben bei der Datenverarbeitung, die man mit dem Hausverstand problemlos beachten kann.

- Geben Sie in Ihrem Unternehmen das Credo aus: **„Datenschutz ist in unserem Hotel wichtig!** Die Daten unserer Gäste sind ein wertvolles Gut und wir gehen mit ihnen dementsprechend um!“ Machen Sie auf das Thema aufmerksam, schulen Sie Ihre Mitarbeiter, seien Sie Vorbild und Vorreiter in Ihrer Gemeinde!
- Halten Sie sich immer von Augen, warum Ihnen ein Gast seine Daten gibt. **Genau dafür dürfen Sie sie verwenden!** Wenn Sie beispielsweise seine E-Mail-Adresse speichern möchten, um ihm Angebote für die nächste Saison zuzuschicken, fragen Sie den Gast um sein **Einverständnis**! So vermeiden Sie auch ungehaltene Gäste oder erboste Kritiken.
- Speichern Sie **so wenig Information wie möglich**, dann kommen Sie nicht in Erklärungsnot gegenüber einem Gast oder der Behörde. Und achten Sie darauf, dass die Daten, die Sie nach sorgfältiger Prüfung verarbeiten, korrekt sind.
- Durchforsten Sie Ihr System regelmäßig auf sogenannte digitale „Karteileichen“, nämlich Daten, die Sie seit langer Zeit nicht mehr verwendet haben und voraussichtlich auch nicht mehr benötigen werden. **Löschen Sie diese**! Im Idealfall etablieren Sie Löschungsroutinen, dann macht das ein Programm automatisch für Sie.

Sollte es doch hart auf hart kommen und die Datenschutzbehörde steht vor Ihrem Hoteleingang, sollten Sie im Sinne einer Schadensbegrenzung über folgende Punkte Bescheid wissen, die von der Behörde bei der Bemessung der Strafhöhe berücksichtigt werden. Die Höhe der Geldstrafe wird nämlich nach den Umständen des Einzelfalls festgelegt und soll **wirksam, verhältnismäßig** und **abschreckend** sein.

- Art, Schwere und Dauer des Verstoßes (unter Berücksichtigung von Art, Umfang und Zweck der Verarbeitung sowie Zahl der betroffenen Personen und Schadensausmaß);
- **Vorsätzlichkeit oder Fahrlässigkeit**;
- Maßnahmen zur Minderung des entstandenen Schadens;
- **Grad der Verantwortung** unter Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen;
- **einschlägige frühere Verstöße**;
- Umfang der Zusammenarbeit mit der Aufsichtsbehörde bei Aufklärung und Schadensbegrenzung;
- **Kategorien** der vom Verstoß betroffenen personenbezogenen Daten;

- Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde (insbesondere „Selbstanzeige“);
- Einhaltung früher angeordneter ähnlicher Maßnahmen zum selben Gegenstand;
- Einhaltung genehmigter Verhaltensregeln (von zB Verbänden oder Kammern) oder Zertifizierungsverfahren;
- alle weiteren erschwerenden oder mildernden Umstände (zB unmittelbar oder mittelbar durch den Verstoß erlangten finanzielle Vorteile oder vermiedene Verluste).

Ganz allgemein: Sie können sich sicher vorstellen, dass die Etablierung eines routinemäßigen Standards in Ihrem Hotel einen anderen (positiven) Eindruck macht, als wenn für die Behörde ersichtlich wird, dass Sie das Thema Datenschutz nicht kümmert.

3. Was ist eine Datenschutz-Folgeabschätzung und wofür brauchen Sie diese?

Wie der Name bereits sagt, soll eine Datenschutz-Folgeabschätzung **vor Beginn einer Datenverarbeitung** beurteilen, wie stark diese in Rechte anderer eingreift. Die Pflicht zur Durchführung einer Datenschutz-Folgeabschätzung trifft Sie als datenschutzrechtlichen Verantwortlichen persönlich.

Rechtlich gesprochen ist eine solche zwingend vorab durchzuführen, wenn eine Datenverarbeitungsform **aufgrund der Art, des Umfangs, der Umstände und der Verarbeitungszwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten von Personen** zur Folge hat. Beispielhaft kann dies der Fall sein, wenn vertrauliche oder höchstpersönliche Daten (zB gesundheitsbezogene Daten) verarbeitet werden, oder wenn Datenverarbeitung in sehr großem Umfang vorgenommen wird.

WICHTIG: Für bestimmte Datenverarbeitungen ist nach derzeitiger Rechtslage eine Vorabgenehmigung der Datenschutzbehörde notwendig. Konkret ist diese für Datenanwendungen vorgeschrieben, die (i) sensible Daten (zB Daten über rassische oder ethnische Herkunft, die Religion oder sexuelle Orientierung einer Person) enthalten, (ii) strafrechtlich relevante Daten enthalten, (iii) die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben oder (iv) in Form eines Informationsverbundsystems durchgeführt werden sollen.

Laut derzeitigem Informationsstand soll für Datenverarbeitungen, die nach der jetzigen Rechtslage von der Datenschutzbehörde vorabgenehmigt wurden, keine Datenschutz-Folgeabschätzung notwendig sein – natürlich nur solange sich bei der jeweiligen Datenverarbeitung nichts ändert.

Relevanter Anwendungsbereich für Ihr Hotel sind zum Beispiel **Videoüberwachungsanlagen**, die nach derzeitiger Rechtslage vorabgenehmigungspflichtig sind. Es kann also – abgesehen davon, dass Sie diese nach den derzeit bestehenden rechtlichen Vorgaben vorab genehmigen lassen müssen – durchaus Sinn machen, **geplante Videoüberwachungen noch vor Mai von der Behörde genehmigen zu lassen, um eine Datenschutz-Folgeabschätzung vorerst nicht durchführen zu müssen**.

Die Beurteilung, ob ansonsten eine Datenschutz-Folgeabschätzung in Ihrem Fall durchzuführen ist, kann nur individuell anhand der Datenstrukturen Ihres Hotels geprüft werden. Auch wenn Sie zu dem Schluss kommen, keine Datenschutz-Folgeabschätzung vornehmen zu müssen, müssen Sie das als Verantwortlicher begründen und dokumentieren. Bitte wenden Sie sich hierfür an einen Datenschutzexperten!

4. Brauchen Sie verpflichtend einen Datenschutzbeauftragten?

Rechtlich gesprochen benötigen Sie einen Datenschutzbeauftragen, wenn Ihre „**Kerntätigkeit** in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer **Art**, ihres **Umfangs** und/oder ihrer **Zwecke** eine **umfangreiche regelmäßige und systematische Überwachung** von betroffenen Personen erforderlich machen.“

Diese unklare Formulierung wird derzeit von Datenschutzexperten viel diskutiert. Es scheint sich jedoch abzuzeichnen, dass die Bestimmung von den Behörde eher weit ausgelegt werden wird und der Einsatz eines Datenschutzbeauftragten daher für viele Unternehmen zwingend sein wird. Sie sollten als Verantwortlicher für Ihr Hotel individuell prüfen (lassen), ob Sie einen Datenschutzbeauftragten zwingend benötigen.

Klar ist, dass kein Unternehmen – egal wie nebensächlich die Datenverarbeitung im Geschäftsbetrieb sein mag – umhin kommen wird, sich mit den (neuen) datenschutzrechtlichen Vorgaben zu beschäftigen. **Jeder Mitarbeiter sollte in seinem Bereich die Datenschutz-Grundsätze kennen und anwenden**.

Es besteht auch die Möglichkeit, in Ihrem **Hotel auf freiwilliger Basis einen Datenschutzbeauftragten (auch extern möglich)** zu beschäftigen. Die Vorteile liegen darin, dass sämtliche datenschutzrechtlichen Anfragen bei einer Person gebündelt bearbeitet werden. Auch macht es effizienztechnisch Sinn, wenn immer dieselbe Person solche Anfragen bearbeitet. Zudem gibt es eine zuständige Ansprechperson, die – wenn wirklich einmal die Behörde vor der Tür steht – weiß, wo die benötigten Informationen zu finden sind. Doch Ihnen muss bewusst sein, dass der Datenschutzbeauftragte seine Aufgaben in völliger Unabhängigkeit ausüben können muss und keine Anweisungen bei der Erfüllung seiner Aufgaben erhalten darf. Er darf zudem wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Es liegt wieder in der Verantwortung von Ihnen als Verantwortlichem, dass der Datenschutzbeauftragte ausreichend Einblick in die Betriebsabläufe erhält und frühzeitig in alle den Datenschutz betreffende Fragen eingebunden ist.

5. Was ist ein Verzeichnis von Verarbeitungstätigkeiten? Müssen Sie ein solches führen?

Dabei handelt es sich um ein in Ihrem Betrieb geführtes Verzeichnis, das im Wesentlichen die Informationen enthält, die derzeit im Rahmen einer Meldung an die Datenschutzbehörde anzugeben sind. Zum Beispiel Kategorien von Personen und deren verarbeitete Daten, Zweck der Datenverarbeitung oder Fristen für die Löschung.

Eine **Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten** trifft Sie dann, wenn Ihr Unternehmen mehr als 250 Mitarbeiter – egal ob Vollzeit, Teilzeit oder geringfügig – beschäftigt oder wenn die Verarbeitung

- ein Risiko für die Rechte und Freiheiten der Betroffenen birgt; oder
- nicht nur gelegentlich erfolgt; oder
- besondere Datenkategorien (bisher: „sensible Daten“) betrifft.

Gerade standardmäßig vorgenommene Datenverarbeitungen sollten im Zweifel in einem entsprechenden Verzeichnis abgebildet werden. Im Zweifel ist auf jeden Fall die Führung eines Verarbeitungsverzeichnisses anzuraten, da Sie im Fall der Nachschau der Behörde ohnehin **umfangreich und nachvollziehbar** über Ihre Datenverarbeitungen Auskunft geben müssen und ein entsprechender Überblick ohne eine gewisse Aufarbeitung und Organisation nur schwer möglich sein wird.

6. Hilfe, Sie wurden gehackt! Was tun?

Regelmäßig hört man in dem Medien von „Hackerangriffen“, bei denen unzählige Daten gestohlen werden und das betroffene Unternehmen mehr oder weniger erfolgreich Schadensbegrenzung vorzunehmen versucht. In unserer zunehmend digitalisierten Welt kann das jedem Unternehmen widerfahren – doch was kann oder muss man in einem solchen Fall tun?

Das Gesetz spricht von einer „Verletzung des Schutzes personenbezogener Daten“. Gemeint ist damit der Verlust der (vollständigen) Kontrolle über personenbezogene Daten und ihr Schicksal – was mit diesen gemacht wird, wer sie verwahrt, an wen sie weitergegeben werden, oder ob sie gar missbräuchlich verwendet werden. Das gilt zum Beispiel auch, wenn Ihnen ein USB-Stick oder einen Laptop abhanden kommt, auf dem sich personenbezogene Daten befinden. In einem solchen Fall müssen Sie

- **unverzüglich nach Bekanntwerden Meldung an die Datenschutzbehörde** erstatten. Erfolgt die Meldung nicht binnen 72 Stunden, so ist diese Verzögerung zu begründen.
- alles **dokumentieren**, insbesondere (mögliche) Auswirkungen und Abhilfemaßnahmen! Die Datenschutzbehörde wird Ihre Verantwortung höchstwahrscheinlich nachkontrollieren!
- außerdem **unverzüglich die Betroffenen** benachrichtigen, wenn die Verletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.

7. Müssen Sie etwas beachten, wenn Sie Videokameras installiert haben?

Ja, Videokameras sind ein besonders **heikles Thema**! Bei Aufzeichnungen, die über rein touristische, künstlerische oder familiäre Beweggründe und Kameraattrappen hinausgehen, gibt es besondere datenschutzrechtliche Vorschriften – grundsätzlich auch bei Echtzeit-Überwachung ohne Speicherung der Videoaufnahme!

- **Rechtmäßiger Zweck** einer Videoüberwachung kann nur der Schutz des überwachten Objekts, oder der überwachten Person, oder die Erfüllung rechtlicher Sorgfaltspflichten sein.
- **Absolut verboten** ist die Videoüberwachung im höchstpersönlichen Lebensbereich (zB Privatwohnungen, Umkleidekabinen, WC), zur Mitarbeiterkontrolle an Arbeitsplätzen oder die Aufzeichnung von Tondaten.
- **Erlaubt** ist dagegen die Überwachung von Objekten an Arbeitsstätten, wenn damit andere gerechtfertigte Interessen geschützt werden, wie die Überwachung eines Kassenraums oder die Überwachung eines besonders gefährlichen Arbeitsplatzes.
- **Kennzeichnungspflicht**: Information (zB Beschilderung), bevor der Betroffene den überwachten Bereich betritt.
- Auswertung der aufgezeichneten Daten **nur im Anlassfall** und von dazu berechtigten Personen.
- Sofern kein konkreter Anlass vorliegt, dürfen aufgezeichnete Daten **längstens 72 Stunden** gespeichert werden.

Wie bereits unter Punkt 4. hingewiesen wurde, sind **Videoüberwachungsanlagen** nach derzeitiger Rechtslage vorabgenehmigungspflichtig. Es kann also – abgesehen davon, dass Sie diese nach den derzeit bestehenden rechtlichen Vorgaben vorab genehmigen lassen müssen – durchaus Sinn machen, **geplante Videoüberwachungen noch vor Mai von der Behörde genehmigen zu lassen, um eine Datenschutz-Folgeabschätzung vorerst nicht durchführen zu müssen.**

8. Was tun Sie, wenn sich ein Gast an Sie wendet und wissen will, welche Infos über ihn in Ihrem Computersystem gespeichert sind? Müssen Sie diese auf seinen Wunsch löschen?

Bei einer solchen Anfrage sollten Sie Vorsicht walten lassen, denn jede Person hat umfangreiche Rechte im Hinblick auf seine oder ihre Daten. Unter bestimmten Umständen müssen Sie diese auch auf seinen oder ihren Wunsch löschen:

- **Auskunftsrecht**
  Der Verantwortliche hat betroffenen Personen auf Antrag binnen eines Monats Auskunft über die verarbeiteten personenbezogenen Daten und den Zweck der Verarbeitung zu erteilen.
- **Recht auf Richtigstellung**
  Bei unrichtigen bzw unvollständigen Daten kann die betroffene Person Richtigstellung verlangen.
- **Recht auf Löschung**
  Der Verantwortliche muss Daten löschen, wenn sie für die Zwecke der Verarbeitung nicht notwendig sind, die betroffene Person ihre Einwilligung widerruft (sofern kein anderer, zusätzlicher Erlaubnistatbestand für die Verarbeitung vorliegt), oder die Daten unrechtmäßig verarbeitet wurden.
- **Recht auf Widerspruch**
  Bei Verarbeitungen, die auf Basis eines öffentlichen Interesses oder einer Interessenabwägung erfolgen, kann die betroffene Person Widerspruch erheben.
- **Beschwerde an Datenschutzbehörde**

Im Wesentlichen bestehen diese Rechte auch aufgrund der derzeit gültigen Rechtslage; allerdings sind die Strafdrohungen bei Nichtbeachtung ab Mai 2018 um ein Vielfaches höher!

9. Was tun Sie, wenn die Datenschutzbehörde anklopft?

Grundsätzlich normiert das Gesetz eine Pflicht für Sie als Verantwortlichem, dass Sie der Datenschutzbehörde alle von dieser benötigten Unterlagen und Informationen bereitstellen. Dazu kann die Behörde Sie schriftlich auffordern; sie hat aber auch die
Befugnis, in Ihrem Hotel eine Überprüfung durchzuführen. In einem solchen Fall muss die Behörde Sie laut Gesetz vor Betretung verständigen.

- Bereiten Sie Ihr Personal auf so einen Fall vor! Die Geschäftsleitung ist diesfalls umgehend zu informieren.
- Sollten Sie einen Datenschutzbeauftragten haben, sollte auch dieser sofort informiert werden.
- Stellen Sie bereits im Vorfeld sicher, dass die relevanten Unterlagen geordnet, sofort auffindbar und gut organisiert sind!
- Ein gut vorbereiteter externer Rechtsbeistand kann helfen, die Kommunikation mit der Behörde zu übernehmen und kompetent abzuwickeln.

* **Empfohlener Partner in IT-Rechtsfragen:**

Warbek Rechtsanwälte
ist eine Rechtsanwaltskanzlei mit Sitz in Innsbruck,
die österreichweit Mandanten im Bereich des IP-Rechts berät.

www.warbek.at | Tel. +43 (0) 512 560 650