Das neue Datenschutzrecht

WAS IN DER GASTRONOMIE KÜNFTIG BEACHTET WERDEN MUSS

Stand: Februar 2018

DEHOGA
BUNDESVERBAND

Impressum

Herausgeber: Deutscher Hotel- und Gaststättenverband e.V. (DEHOGA Bundesverband)
Am Weidendamm 1A · 10117 Berlin · Fon 030/72 62 52-0 · Fax 030/72 62 52-42
info@dehoga.de · www.dehoga.de

Autor: Ass. jur. Christian Reuter, reuter@dehoga.de

Verlag: INTERHOGA Gesellschaft zur Förderung des Deutschen Hotel- und Gaststättengewerbes mbH
Am Weidendamm 1A · 10117 Berlin · Fon 030/59 00 99 850 · Fax 030/59 00 99 851
sekretariat@interhoga.de · www.interhoga.de

Titelfoto: © pixabay.com

Vorwort

Liebe Kolleginen, liebe Kollegen,

ab Ende Mai 2018 werden neue Datenschutzvorschriften für alle Unternehmen in der EU gelten. Das neue Datenschutzrecht stellt insbesondere kleine und mittelständische Betriebe vor große Herausforderungen und wirft viele Fragen auf.

Eigentlich sollten die neuen Regeln vor allem auf Internetgiganten wie Facebook, Amazon und Google abzielen. Mit der DSGVO sind die EU-Instanzen jedoch weit über dieses Ziel hinausgeschossen. Deshalb können wir Ihnen auch nicht ersparen, sich mit den wesentlichen Regeln vertraut zu machen. Es versteht sich von selbst, dass wir den erheblichen organisatorischen und bürokratischen Mehraufwand der Politik aufgezeigt und Ausnahmen für den Mittelstand gefordert haben. Mit Blick auf die grundsätzliche Bedeutung des Datenschutzes und der EU-weiten Regelung waren und sind hier die Handlungsmöglichkeiten jedoch begrenzt.

Mit dieser Publikation wollen wir Sie dabei unterstützen, die neuen Vorgaben im Betrieb umzusetzen. Nach bisheriger Rechtslage muss auch heute schon ein hohes Datenschutzniveau in sämtlichen Unternehmen gewährleistet sein. In der Praxis wird das Thema Datenschutz bisher allerdings zumeist eher stiefmütterlich behandelt. Da nach neuer Rechtslage massive Bußgelder drohen und ein Unternehmen im Falle einer Kontrolle stets nachweisen muss, dass alle relevanten Prozesse datenschutzkonform ablaufen, raten wir allen gastronomischen Betrieben, sich mit diesem Thema auseinander zu setzen.

Aufgrund der Komplexität der neuen Regelungen, können wir Ihnen die etwas umfangreicheren Ausführungen in dieser Publikation leider nicht ersparen. Insbesondere fehlen bisher auch Erfahrungen zur künftigen Kontrollpraxis und möglichen Beanstandungen. Insofern wären wir Ihnen für diesbezügliche Informationen aus Ihrer alltäglichen Praxis dankbar. Wir werden diese Publikation unter Berücksichtigung der künftigen Entwicklungen in der Vollzugspraxis fortlaufend aktualisieren.

Bitte lassen Sie uns Ihre Fragen, Anregungen und Erfahrung aus Ihrer betrieblichen Praxis zukommen. Wir sind auf Ihr Feedback angewiesen.

Mit freundlichen Grüßen

Guido Zöllick
Präsident des DEHOGA Bundesverbandes

Inhaltsverzeichnis

1. Um was geht es und wer ist betroffen?

Die neue **Datenschutzgrundverordnung (DSGVO)** wird ab 25. Mai 2018 EU-weit Anwendung finden. Ziel ist die Vereinheitlichung eines hohen Datenschutzniveaus innerhalb der EU. Ebenfalls ab 25. Mai 2018 findet auch das neue **Bundesdatenschutzgesetz (BDSG-neu)** in Deutschland Anwendung. Beide Regelwerke nehmen Bezug aufeinander und ergänzen sich.

Betroffen sind grundsätzlich alle Unternehmen, die mittels Computern und Smartphones personenbezogene Daten wie Telefonnummer oder E-Mail-Adresse verarbeiten. Daneben können die neuen Regelungen auch bei der händischen Aufzeichnung solcher Daten relevant sein. Kurzum: auch Restaurants, die z. B. mit Reservierungsbüchern arbeiten, raten wir dringend dazu, sich mit dem Thema Datenschutz und den neuen Regelungen auseinanderzusetzen.

Die neuen Regelungen sind komplex und teilweise eher allgemein gehalten, so dass die Umsetzung für alle Wirtschaftsbeteiligten eine große Herausforderung darstellt und in Anbetracht der drastischen Bußgelder ernst genommen werden sollte: Es können **Geldbußen bis 20.000.000 Euro oder bis zu vier Prozent des erzielten Jahresumsatzes** des vorangegangen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist. Als Konsequenz aus den möglichen Sanktionen muss sich jedes Unternehmen mit den neuen Regeln auseinandersetzen.

Doch auch wenn die Sanktionsmöglichkeiten extrem sind, sollte bedacht werden, dass die Datenschutzbehörden primär solche Unternehmen im Blick haben dürften, deren Kerngeschäftsmodell mit dem umfänglichen Sammeln und Nutzen von personenbezogenen Daten zusammenhängt (z.B. Betreiber von Social-Media-Plattformen).

Inwieweit mit den neuen Regelungen ein strengerer Vollzug einhergeht, wird die Praxis zeigen. Es kann jedoch durchaus davon ausgegangen werden, dass die Datenschutzbehörden zunächst größtenteils eher beratend agieren und den Unternehmen Hilfestellungen anbieten werden bzw. Verwarnungen und Rügen aussprechen, ohne sofort die „Bußgeldkeule" zu schwingen. Inwieweit der aktive Kontakt zur zuständigen Datenschutzbehörde gesucht werden sollte, muss jedoch jedes Unternehmen selbst abwägen.

Neben dem Risiko einer behördlichen Kontrolle besteht insbesondere auch das **Risiko einer anwaltlichen Abmahnung**, beispielsweise aufgrund einer unvollständigen Datenschutzerklärung auf der Webseite (siehe hierzu Punkt 8 dieser Publikation).

Die zu ergreifenden Maßnahmen im Unternehmen hängen wesentlich von der Art und dem Umfang der Datenverarbeitung ab. Mit dieser Publikation wollen wir insbesondere auch kleineren und mittelständischen gastgewerblichen Unternehmen Informationen und Empfehlungen an die Hand geben und diese für das Thema Datenschutz sensibilisieren. Im Zweifel und je nach Umfang der Datenverarbeitungsprozesse kann die Bestellung eines Datenschutzbeauftragten (sofern dies nicht ohnehin gesetzlich vorgeschrieben ist, siehe Punkt 11 dieser Publikation) und/oder die Zusammenarbeit mit spezialisierten Dienstleistern sinnvoll sein.

Bitte beachten Sie, dass Sie im Falle einer behördlichen **Kontrolle** den Nachweis erbringen müssen, dass Sie sich mit dem Thema Datenschutz auseinandergesetzt haben und die entsprechenden Prozesse im Unternehmen datenschutzkonform ablaufen. Nutzen Sie dazu unser beigefügtes Muster eines sog. Verzeichnisses aller Verarbeitungstätigkeiten (VVT). Mehr Informationen zu diesem Aspekt finden Sie unter Punkt 7 dieser Publikation. Wir raten jedem Gastronomen dazu, den Status quo des Datenschutzes im Unternehmen zu analysieren und das beigefügte VVT gründlich durchzuarbeiten und aufzubewahren, um dieses im Falle einer Kontrolle vorzeigen zu können.

Um insbesondere kleine und mittlere Unternehmen besser zu informieren, hat die EU-Kommission eine anschauliche Infografik zur neuen DSGVO ins Netz gestellt, welche Sie hier abrufen können: http://ec.europa.eu/justice/smedataprotect/index_de.htm

2. Anwendungsbereich – in welchen Situationen müssen die neuen Vorschriften beachtet werden?

Grundsätzlich gilt: Sofern personenbezogene Daten (wie etwa Name, Telefonnummer, IP-Adresse oder E-Mail-Adresse) mittels Computern oder Smartphones verarbeitet werden, müssen die Regelungen der DSGVO und des BDSG-neu beachtet werden. Aber auch bei der händischen Aufzeichnung von Daten können die Regelungen einschlägig sein. Unter dem Begriff „Verarbeitung" ist unter anderem das Erheben, das Erfassen und das Speichern von personenbezogenen Daten zu verstehen. Im Detail ist bezüglich des Anwendungsbereichs Folgendes zu beachten:

Die Regelungen der DSGVO und des BDSG-neu gelten für die ganz oder teilweise

automatisierte Verarbeitung personenbezogener Daten,

sowie für die

manuelle Verarbeitung solcher Daten, sofern diese in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Beispiele für personenbezogene Daten sind: **Name, Anschrift, Telefonnummer, Kreditkartennummer, Kontodaten, Kundennummern, IP-Adressen, E-Mail-Adresse.**

Beispiel: *Reserviert ein Gast beispielsweise über Ihre Website einen Tisch in Ihrem Restaurant und hinterlässt zwecks Tischreservierung seinen Namen und seine Telefonnummer, so handelt es sich bei der Telefonnummer und dem Namen um personenbezogene Daten, denn diese Informationen können einer bestimmten natürlichen Person zugeordnet werden.*

- Eine **automatisierte Verarbeitung** von personenbezogenen Daten liegt immer dann vor, wenn personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen (also beispielsweise Computern oder Smartphones) verarbeitet werden. **Jede Benutzung von Computer, Internet oder E-Mail kann also zur Anwendbarkeit der neuen datenschutzrechtlichen Vorschriften führen, sofern personenbezogene Daten betroffen sind.**

Im obigen Beispiel erfolgt die Reservierung unter dem Einsatz von Computern. Somit liegt eine automatisierte Verarbeitung der personenbezogenen Daten vor. Die Regelungen zum Datenschutz wären also zu beachten.

- Eine **manuelle (nichtautomatisierte) Verarbeitung von personenbezogenen Daten, sofern diese in einem Dateisystem gespeichert sind oder gespeichert werden**, liegt immer dann vor, wenn personenbezogene Daten ohne Datenverarbeitungsanlagen, also mittels handschriftlichen Aufzeichnungen, verarbeitet werden. Unter einem Dateisystem versteht die DSGVO jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind.

Beispiel: *Ein Gast ruft Ihr Restaurant an oder erscheint vor Ort um einen Tisch zu reservieren. Name und Telefonnummer werden nicht in einem softwarebasierten System, sondern z. B. in einem* ***Terminkalender bzw. Reservierungsbuch*** *händisch festgehalten. Das Reservierungsbuch gilt als Dateisystem, da diese Art der Erfassung eine strukturierte Sammlung personenbezogener Daten darstellt und die eingetragenen Informationen nach bestimmten Kriterien zugänglich sind: Dem Gastwirt wäre es ohne weiteres möglich herauszufinden, an welchem Datum ein bestimmter Gast einen Tisch in der Vergangenheit oder Zukunft reserviert hat. Die Regelungen zum Datenschutz wären also zu beachten.*

Neben personenbezogenen Gästedaten gelten alle in dieser Publikation enthaltenen Ausführungen auch bezüglich personenbezogenen Mitarbeiter- und Lieferantendaten!

3. Wer ist für die Umsetzung der neuen Vorgaben verantwortlich?

Als **Verantwortlicher** im Sinne der DSGVO ist in der Regel das Unternehmen selbst anzusehen: Unter dem Verantwortlichen ist laut DSGVO die natürliche oder juristische Person zu verstehen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Die Haftung betrifft bei Verstößen gegen die neuen Vorschriften immer diejenigen Personen, die geschäftsführende Tätigkeiten wahrnehmen.

Der Verantwortliche (also das Unternehmen) muss **geeignete technische und organisatorische Maßnahmen** umsetzen, um sicherzustellen und den **Nachweis** dafür erbringen zu können, dass die Verarbeitung personenbezogener Daten gemäß den Anforderungen der DSGVO und des BDSG-neu erfolgt. Insbesondere ist der Verantwortliche für die Einhaltung der unter dem nachfolgenden Punkt aufgezeigten Grundsätze verantwortlich und muss die Einhaltung dieser Grundsätze nachweisen können.

Um im Falle einer Kontrolle den Nachweis über die rechtskonforme Verarbeitung von personenbezogenen Daten erbringen zu können, empfehlen wir ein sogenanntes **Verzeichnis von Verarbeitungstätigkeiten (VVT)** zu führen (Detaillierte Informationen zu diesem Verzeichnis finden Sie unter Punkt 7 dieser Publikation).

4. Grundsätze für die Verarbeitung personenbezogener Daten

Folgende Grundsätze müssen bei der Verarbeitung von personenbezogenen Daten beachtet werden:

- **„Rechtmäßigkeit, Treu und Glauben und Transparenz"**: Die Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

- **„Zweckbindung"**: Die Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

- **„Datenminimierung"**: Die Daten müssen auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Hinweis: *Es müssen insbesondere Speicherfristen für personenbezogene Daten festgelegt werden. Diese Speicherfristen müssen auf das unbedingt notwendige Maß beschränkt sein und es sollten regelmäßige Überprüfungen stattfinden.*

➔ Wenn sich die Fristen aus dem Gesetz ergeben (6 bzw. 10 Jahre für geschäftsrelevante Unterlagen gemäß Handelsgesetzbuch und Abgabenordnung), können Sie sich einfach an diesen Fristen orientieren. **Sobald die Daten für den jeweiligen Zweck nicht mehr benötigt werden, sollten diese in der Regel gelöscht werden.**

- **„Richtigkeit"**: Die Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein.

- **„Speicherbegrenzung"**: Die Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

- **„Integrität und Vertraulichkeit"**: Die Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, Schutz vor unbeabsichtigtem Verlust, Schutz vor unbeabsichtigter Zerstörung und Schutz vor unbeabsichtigter Schädigung. Dies ist durch **geeignete technische und organisatorische Maßnahmen** sicherzustellen (Ausführliche Informationen zu den zu ergreifenden Maßnahmen finden Sie unter Punkt 6 dieser Publikation).

5. Was sind die Voraussetzungen für eine rechtmäßige Verarbeitung von personenbezogenen Daten?

Damit eine Verarbeitung personenbezogener Daten gemäß der neuen Vorschriften rechtmäßig erfolgt, müssen bestimmte Bedingungen erfüllt sein. Für die Gastronomie sind dabei insbesondere folgende Voraussetzungen relevant:

- Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben. Zu beachten ist hierbei, dass die Einwilligung jederzeit widerrufen werden kann und die betroffene Person vor Abgabe der Einwilligung auf dieses Widerrufsrecht hingewiesen werden muss.

Hinweis: *Die Einwilligung muss durch eine eindeutige bestätigende Handlung erfolgen. Wird auf Ihrer Unternehmenswebseite beispielsweise ein* ***Kontaktformular*** *angeboten,* ***könnte die eindeutige Handlung etwa durch aktives Anklicken eines Kästchens auf der Webseite erfolgen****. Durch diese Handlung muss die betroffene Person eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung signalisieren. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der Betroffenen stellen keine DSGVO-konforme Einwilligung dar.*

oder

- Die Verarbeitung ist **zur Erfüllung des entsprechenden Vertrages** oder **zur Durchführung vorvertraglicher Maßnahmen** erforderlich, die auf Anfrage der betroffenen Person erfolgen.

Beispiel: *Wird eine* ***Restaurantreservierung*** *seitens des Gastes gewünscht, so dürfte beispielsweise die Verarbeitung von Name und Telefonnummer für die Durchführung der Reservierung (vorvertragliche Maßnahme) erforderlich sein. Eine Einwilligung ist in diesem Fall nicht erforderlich.*

oder

- Die Verarbeitung ist **zur Wahrung der berechtigten Interessen** des Unternehmens erforderlich, sofern die Interessen der betroffenen Person nicht überwiegen. Bei der Abwägung sind die vernünftigen Erwartungen der betroffenen Person zu berücksichtigen.

Beispiel: *Ein berechtigtes Interesse kann beispielsweise vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht. Dies dürfte bei dauerhaften* ***Geschäftsbeziehungen zu Lieferanten*** *regelmäßig der Fall sein. Sofern ein Unternehmen als* ***Teil einer Unternehmensgruppe*** *anzusehen ist, kann grundsätzlich ein berechtigtes Interesse an der Übermittlung von personenbezogenen Daten angenommen werden, sofern die Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke verwendet werden.*

oder

- Die Verarbeitung ist **zur Erfüllung einer rechtlichen Verpflichtung** erforderlich.

Beispiel: *Da eine rechtliche Verpflichtung zur Aufbewahrung von steuerlichen und geschäftsrelevanten Unterlagen gemäß Abgabenordnung und Handelsgesetzbuch besteht, ist insbesondere die fristgerechte Aufbewahrung dieser Unterlagen, aus denen sich in der Regel personenbezogene Daten ergeben, ohne Einwilligung möglich.*

6. Welche technischen und organisatorischen Maßnahmen müssen umgesetzt werden?

Die Beantwortung dieser Frage hängt maßgeblich vom Status quo des Datenschutzes ab. Außerdem spielen insbesondere **die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung personenbezogener Daten** eine entscheidende Rolle bei der Beantwortung der Frage nach den zu ergreifenden Maßnahmen.

Jeder betroffene Betrieb muss anhand eines **risikobasierten Ansatzes** selbst beurteilen, inwieweit **technische und organisatorische Maßnahmen** getroffen werden müssen, um die neuen datenschutzrechtlichen Vorgaben einzuhalten. Die DSGVO gibt diesbezüglich folgende Erwägungen und Anhaltspunkte vor:

- Die zu ergreifenden Maßnahmen sind unter Berücksichtigung der unterschiedlichen Eintrittswahrscheinlichkeit und **Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen** im Unternehmen umzusetzen

- Um **ein dem Risiko angemessenes Schutzniveau** zu gewährleisten sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung der personenbezogenen Daten

- Das Risiko sollte anhand einer **objektiven Bewertung** beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung im Betrieb ein Risiko oder ein hohes Risiko birgt

- **Bei der Verarbeitung von personenbezogenen Daten in der Gastronomie dürfte regelmäßig kein hohes Risiko für die Rechte und Freiheiten der Gäste bestehen (Personenbezogene Daten der Gäste, die typischerweise anfallen sind: Name, Telefonnummer, E-Mail-Adresse).** Dementsprechend dürften auch die Anforderungen an die technischen und organisatorischen Maßnahmen grundsätzlich geringer ausfallen als beispielsweise bei der Verarbeitung von personenbezogenen Daten seitens Unternehmen, deren Kerngeschäft und Haupttätigkeit die Verarbeitung einer Vielzahl (sensibler) Daten betrifft (z.B. Google, Facebook, Onlinehändler oder Krankenhäuser)

Die technischen und organisatorischen Maßnahmen können – je nach Art, Umfang und Zweck der Verarbeitung – unter anderem Folgendes einschließen:

- Die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- Implementierung eines Verfahrens zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Folgende **Standardmaßnahmen** sollten zumindest eingehalten werden:

- Stellen Sie sicher, dass die unter Punkt 8 erläuterten Pflichten des Unternehmens eingehalten werden und die Rechte der Gäste beachtet werden
- Regelmäßige Updates des verwendeten Computersystems und des Anti-Virenprogramms
- Aktenschränke, welche Dokumentenordner mit personenbezogenen Daten enthalten, stets verschlossen halten
- Stellen Sie sicher, dass ein eventuell vorhandenes Reservierungsbuch nicht durch Unbefugte eingesehen werden kann
- Sofern Sie Informationen über Allergien notieren, vermeiden Sie es, die Namen der betroffenen Personen niederzuschreiben
- Sofern Sie Kreditkartendaten telefonisch abfragen, stellen Sie sicher, dass Sie diese vernichten, sobald Sie diese nicht mehr benötigen und dass keine unbefugten Personen darauf Zugriff erhalten
- Regelmäßige Back-Ups
- Sicherstellung, dass Mitarbeiter nur auf Dateien zugreifen können, die für die jeweils entsprechende Tätigkeit nötig sind

- Alle Mitarbeiter hinsichtlich der neuen Regelungen sensibilisieren/schulen und Schulungen regelmäßig (z.B. einmal jährlich) wiederholen

- In regelmäßigen Abständen (z.B. alle 6 Monate) sollte überprüft werden, ob die Maßnahmen wirksam sind oder Anpassungen erforderlich sind

Unter Zugrundelegung dieser Grundsätze wird eine **Restaurantkette mit mehreren Filialen** einen höheren Aufwand betreiben müssen, um ihre Datenverarbeitungsprozesse zu analysieren und gegebenenfalls an die neuen Vorschriften anzupassen als ein **einzelnes Restaurant**.

Eine **kleine Imbissbude**, die überhaupt keine **Gästedaten** verarbeitet, muss diesbezüglich jedenfalls keine Maßnahmen treffen, da hier schon der Anwendungsbereich nicht eröffnet ist. Dennoch müssten derartige Betriebe die neuen Regelungen beachten, sofern personenbezogene Lieferantendaten im Sinne der DSGVO verarbeitet werden. Wenn Ihr Betrieb Arbeitnehmer beschäftigt, müssen außerdem in jedem Fall auch die neuen datenschutzrechtlichen Regelungen zum Arbeitnehmerdatenschutz beachtet werden, die ebenfalls in der DSGVO und dem BDSG-neu geregelt sind (siehe Punkt 10 dieser Publikation).

Im Falle einer eventuellen Kontrolle sollte das betroffene Unternehmen zumindest in der Lage sein, eine gewisse Mindestdokumentation über die Verarbeitungstätigkeiten von personenbezogenen Daten vorweisen zu können. Sie können dazu das in der Anlage beigefügte Muster-Verfahrensverzeichnis aller Verarbeitungstätigkeiten verwenden (siehe nächster Punkt). Zusätzlich zum VVT sollten Sie noch eine Beschreibung der getroffenen technischen und organisatorischen Maßnahmen (sogenannte „TOM-Beschreibung“) erstellen. Hier sollten sie zumindest die unter diesem Punkt genannten Standardmaßnahmen niederschreiben und zusätzlich weitere Maßnahmen vermerken, die nach der Analyse Ihrer Datenverarbeitungsprozesse eventuell getroffen werden müssen.

7. Verzeichnis der Verarbeitungstätigkeiten

Grundsätzlich ist jedes Unternehmen dazu verpflichtet, ein Verzeichnis aller Verarbeitungstätigkeiten (VVT) zu führen. In diesem Verzeichnis müssen folgende Angaben enthalten sein:

- Name + Kontaktdaten des Verantwortlichen sowie des Vertreters und evtl. des Datenschutzbeauftragten
- Zwecke der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und personenbezogener Daten (Beschäftigte, Kunden, Lieferanten…)
- Kategorien von Empfängern, gegenüber denen personenbezogene Daten offengelegt worden sind oder noch offengelegt werden
- Ggfls. Übermittlungen von personenbezogenen Daten an ein Drittland
- Wenn möglich, die selbst festgelegten Fristen für die Löschung der verschiedenen Datenkategorien
- Wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Das VVT muss der Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden.

Ausnahme: In Unternehmen, die weniger als 250 Mitarbeiter beschäftigen muss kein VVT geführt werden, sofern die Verarbeitung personenbezogener Daten nur gelegentlich erfolgt. Auch wenn für solche Unternehmen keine Pflicht zur Führung eines VVT besteht, ist es für diese Unternehmen nicht ratsam auf ein VVT zu verzichten, da das Unternehmen der Aufsichtsbehörde im Falle einer Kontrolle generell nachweisen können muss, dass die Vorgaben der DSGVO und des BDSG-neu eingehalten werden. Ein korrekt geführtes VVT dürfte hierzu dienlich sein.

In der Anlage zu dieser Publikation übersenden wir ein **Muster-VVT**, welches von den deutschen Aufsichtsbehörden erstellt wurde. Benutzen Sie dieses Muster, um im Falle einer Kontrolle nachweisen zu können, dass Prozesse, welche personenbezogene Daten betreffen, im Einklang mit den neuen Vorschriften ablaufen. Zusätzlich finden Sie in der Anlage auch **Erläuterungen zur Verwendung des Muster-VVT.** Sie können natürlich auch eine eigene Dokumentationsvorlage erstellen.

8. Rechte der Gäste/Pflichten des Unternehmens

Werden personenbezogene Daten in Ihrem Unternehmen verarbeitet, muss auch beachtet werden, dass Personen, deren personenbezogene Daten verarbeitet werden, bestimmte Rechte zustehen. Somit bestehen auch bestimmte Pflichten Ihrerseits:

- **Informationspflicht des Unternehmers!**

Zum Zeitpunkt der Erhebung von personenbezogenen Daten muss der entsprechenden Person Folgendes mitgeteilt werden:

- Name und Kontaktdaten des Verantwortlichen (außerdem ggfls. Kontaktdaten des Datenschutzbeauftragten)
- Den Zweck (oder die Zwecke) der Verarbeitung, sowie die Rechtsgrundlage für die Verarbeitung (es sollte die einschlägige Voraussetzung der Rechtmäßigkeit der Verarbeitung genannt werden, siehe Punkt 5 dieser Publikation. Außerdem sollte stets **„Artikel 6 DSGVO"** als Rechtsgrundlage genannt werden). Neben dem Zweck sollte auch über Art und Umfang der Datenverarbeitung informiert werden
- Sofern die Verarbeitung aufgrund eines berechtigten Interesses des Unternehmens erfolgt, die Nennung des berechtigten Interesses
- Ggfls. die Empfänger der personenbezogenen Daten
- Ggfls. die Absicht, die personenbezogenen Daten an ein Drittland zu übermitteln
- Dauer der Speicherung der personenbezogenen Daten
- Das Bestehen eines Rechts auf Auskunft/Löschung/Einschränkung der Verarbeitung/Widerspruchsrecht über die betreffenden personenbezogenen Daten
- Das Bestehen eines Widerrufsrecht, wenn die Verarbeitung aufgrund einer Einwilligung erfolgt
- Das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde

Sofern Sie eine eigene Webseite betreiben, ist es zu empfehlen, dass Sie Ihren Informationspflichten in der Datenschutzerklärung nachzukommen. Insofern sollten Sie diese bis spätestens 25. Mai 2018 aktualisieren.

Beispiel: *Ein Gast trägt auf Ihrer Webseite mittels eines* ***Reservierungsformulars*** *die erforderlichen personenbezogenen Daten ein. Hier kann dem Gast beispielsweise eine Reservierungsbestätigung mit den aufgeführten Informationen angezeigt werden (bzw. kann ein Link zu einer Webseite oder einem entsprechenden Dokument bereitgestellt werden, wo die erforderlichen Informationen eingesehen werden können. Da die Informationen auch jedenfalls in der Datenschutzerklärung bereitgestellt werden sollten, bietet es sich alternativ auch an, in der jeweiligen Situation auf die DSGVO-konforme Datenschutzerklärung zu verlinken).*

Die Informationspflicht muss beispielswiese auch beachtet werden, wenn personenbezogene Daten wie Name und E-Mail-Adresse in ein ***Kontaktformular*** *auf der Unternehmenswebseite eingetragen werden.*

Sofern die betroffene Person bereits über die Informationen verfügt, müssen diese nicht „doppelt" zur Verfügung gestellt werden.

- **Recht auf Auskunft**
  Natürliche Personen können eine Bestätigung darüber verlangen, ob sie betreffende Daten verarbeitet werden. Ist dies der Fall, so besteht ein Recht auf Auskunft über die verarbeiteten Informationen.

- **Recht auf Berichtigung**
  Falls personenbezogene Daten unrichtig oder unvollständig verarbeitet wurden, kann die betroffene Person **unverzüglich** die Berichtigung bzw. Vervollständigung der Daten verlangen.

- **Recht auf Datenübertragbarkeit**
  Sofern die Verarbeitung mithilfe automatisierter Verfahren erfolgt und die Verarbeitung aufgrund einer Einwilligung oder zur Erfüllung des Vertrages erfolgt, besteht ein Recht auf Datenübertragbarkeit. Die betroffenen Personen können aufgrund dieses Rechts verlangen, dass die sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format bereitgestellt werden. In der Praxis bietet sich etwa an, die betreffenden Daten z. B. im Word oder Excel Format zu übermitteln, falls ein Gast von diesem Recht Gebrauch macht.

- **Widerspruchsrecht**
  Sofern die Verarbeitung der personenbezogenen Daten zur Wahrung der berechtigten Interessen des Unternehmens erforderlich ist, kann die Person, bei der die Daten erhoben wurden, jederzeit Widerspruch gegen die Verarbeitung einlegen. Sofern seitens des Unternehmens keine zwingenden schutzwürdige Gründe nachgewiesen werden können oder die Verarbeitung nicht der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient, dürfen die entsprechenden Daten nicht mehr verarbeitet werden. Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so kann die betroffene Person jederzeit Widerspruch einlegen.

- **Recht auf Löschung („Recht auf Vergessenwerden")**
  Jede betroffene Person kann verlangen, dass die sie betreffenden personenbezogenen Daten **unverzüglich** gelöscht werden, sofern ein gesetzlich definierter Grund zutrifft. Für das Gastgewerbe sind dabei folgende Gründe relevant:

  – die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig
  – falls die Verarbeitung aufgrund einer Einwilligung erfolgte: Widerruf der Einwilligung
  – die betroffene Person legt Widerspruch gegen die Verarbeitung ein
  – die personenbezogenen Daten wurden unrechtmäßig verarbeitet

Ausnahmen:

➔ Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich.

Beispiel: *Da für geschäftsrelevante Unterlagen eine gesetzliche Aufbewahrungsfrist gilt (6 bzw. 10 Jahre gemäß Handelsgesetzbuch und Abgabenordnung), bestünde kein Löschanspruch bezüglich dieser Unterlagen seitens einer Person, deren personenbezogene Daten aus diesen Unterlagen hervorgehen.*

oder

➔ Die Verarbeitung der personenbezogenen Daten ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich.

Beispiel: *Ein Gast hat einen Veranstaltungsraum in Ihrem Restaurant reserviert, um dort eine große Feier auszurichten. Zu diesem Zweck speichern Sie Name, Telefonnummer und E-Mail-Adresse auf Ihrem Arbeitscomputer. Nachdem die Feier durchgeführt wurde, moniert der Ausrichter der Feier, dass der Service nicht vertragsgemäß durchgeführt wurde und das von Ihnen bereitgestellte Essen nicht der vertragsgemäßen Vereinbarung entsprach. Daher verweigert dieser die Zahlung des vollen vereinbarten Betrages und bezahlt stattdessen nur 50% des Betrages. Da Sie der Meinung sind, dass alle erbrachten Leistungen der vertraglichen*

Vereinbarung entsprachen, bestehen Sie auf die Zahlung des vollen Betrages. Nun verlangt der Ausrichter der Feier die Löschung sämtlicher personenbezogener Daten, da der Vertrag ja nun durchgeführt sei und Sie die Daten somit nicht mehr benötigen würden. Da Sie die Daten jedoch zur Geltendmachung Ihrer Rechtsansprüche benötigen, sind Sie nicht verpflichtet diese Daten zu löschen.

Recht auf Einschränkung der Verarbeitung

Unter folgenden Voraussetzungen kann die Einschränkung der Verarbeitung der erhobenen Daten verlangt werden:

- Die Richtigkeit der personenbezogenen Daten wird bestritten
- Die Verarbeitung ist unrechtmäßig und statt Löschung wird die Einschränkung der Nutzung der personenbezogenen Daten verlangt
- Die personenbezogenen Daten werden für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person benötigt diese Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
- Eine Person hat Widerspruch gegen die Verarbeitung eingelegt und es steht noch nicht fest, ob die berechtigten Gründe des Unternehmens überwiegen

Wurde das Recht auf Einschränkung der Verarbeitung ausgeübt, dürfen die entsprechenden Daten, abgesehen von der Speicherung, nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen verarbeitet werden.

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

Sofern personenbezogene Daten verloren gehen oder Unbefugte Zugriff darauf erhalten (etwa durch einen Computer-Hack), muss dies grundsätzlich binnen 72 Stunden nachdem der Vorfall bekannt wurde der zuständigen Aufsichtsbehörde gemeldet werden.

9. E-Mail-Werbung (Direktwerbung) / Newsletter

Bereits nach bisheriger Rechtslage ist für die E-Mail-Werbung **grundsätzlich eine Einwilligung erforderlich.**

Sofern folgende Voraussetzungen vorliegen, ist **keine** Einwilligung nötig:

1. **Der Unternehmer hat im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden/Gast dessen E-Mail-Adresse erhalten,**
2. **der Unternehmer verwendet die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen,**
3. **der Kunde hat der Verwendung nicht widersprochen und**
4. **der Kunde wird bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.**

Falls diese Voraussetzungen nicht vorliegen und somit eine Einwilligung erforderlich ist, sollte das sogenannte Douple Opt-In Verfahren angewendet werden, um im Streitfall beweisen zu können, dass die Einwilligung tatsächlich eingeholt wurde. Beim Double-Opt-In-Verfahren muss der Werbeempfänger nach der Eintragung seiner E-Mail-Adresse und ggf. der sonstigen Daten seine Einwilligung durch Anklicken eines Links in einer Bestätigungsmail nochmal bestätigen. Erst dann ist das Zusenden von Werbung zulässig. Reagiert der Empfänger auf die Bestätigungsmail nicht, gilt dies als Ablehnung. Außerdem sollten Datum, Uhrzeit und IP-Daten protokolliert werden, um der Nachweispflicht nachkommen zu können. **Sofern eine Einwilligung erforderlich ist, muss die betroffene Person über das bestehende Widerrufsrecht informiert werden.**

An diesen Anforderungen dürfte sich auch mit Geltung der neuen Vorschriften nichts ändern. Zwar kann gemäß der DSGVO die Verarbeitung von personenbezogenen Daten zum Zwecke der Direktwerbung als ein berechtigtes Interesse des Unternehmens betrachtet werden, allerdings bleiben die oben aufgeführten Voraussetzungen für E-Mail-Werbung ohne Einwilligung auch unter der neuen Rechtslage gültig.

Zu beachten ist, dass der Widerruf der Einwilligung nach neuer Rechtslage so einfach wie die Erteilung der Einwilligung sein muss **(Simplizitätsgebot)**.

Hinweis: *Diesem Gebot dürfte mit einem „Unsubscribe-Link" am Ende der entsprechenden E-Mail hinreichend Rechnung getragen sein.*

Sofern nach bisherigem Recht wirksame Einwilligungen betreffend E-Mail-Werbung eingeholt wurden, muss keine erneute Einwilligung für den Altdatenbestand ab 25. Mai 2018 eingeholt werden.

Sofern Sie Zweifel haben, ob Sie im Falle eine Kontrolle die Einwilligungen bezüglich des Altdatenbestands nachweisen können, ist es empfehlenswert, sämtliche betroffenen Altkunden zu kontaktieren und eine ausdrückliche nachweisbare Einwilligung einzuholen.

➔ **Denken Sie in jedem Fall daran, über die Datenerhebung und Datenverarbeitung im Zusammenhang mit E-Mail-Werbung/Newslettern zu informieren.** Dies kann beispielswiese in der **Datenschutzerklärung** auf Ihrer Webseite erfolgen, sofern die betroffene Person die Möglichkeit hat, vor Verarbeitung der Daten davon Kenntnis zu nehmen.

10. Arbeitnehmerdatenschutz

Grundsätzlich gilt, dass personenbezogene Daten von Beschäftigten nur für Zwecke des Beschäftigungsverhältnisses verarbeitet werden dürfen, wenn dies für die Entscheidung über die Begründung, Durchführung oder Beendigung eines Beschäftigtenverhältnisses erforderlich ist.

Die Daten dürfen auch dann verarbeitet werden, wenn dies zur Ausübung oder Erfüllung der sich aus einem Gesetz, einem Tarifvertrag oder einer Betriebsvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

In Bezug auf diese zweckgebundenen Daten, muss keine gesonderte Einwilligung von den Beschäftigten eingeholt werden. Dies betrifft Daten wie den Namen, die Steueridentifikationsnummer und die Daten zur Sozialversicherung.

Sofern der Arbeitgeber darüber hinausgehende Daten erfassen und speichern möchte, braucht er dafür eine Einwilligung in Schriftform. Dies betrifft beispielsweise Angaben zu Hobbys und Interessen des Arbeitnehmers.

Die schriftliche Einwilligung wird auch benötigt, wenn Daten an andere weitergegeben werden.

Beispiel: *Das Geburtsdatum wird in einem von den Kollegen einsehbaren Geburtstagskalender veröffentlicht.*

Bei der Einholung von Einwilligungen im Beschäftigtenverhältnis ist weiterhin darauf zu achten, dass diese freiwillig erfolgen müssen. Dabei sind insbesondere die Abhängigkeit des Beschäftigten und die konkreten Umstände, unter denen die Einwilligung zu erteilen ist, zu berücksichtigen. Die Arbeitnehmer müssen außerdem in Textform über die Zwecke der Datenverarbeitung und über ihr Widerrufsrecht aufgeklärt worden sein. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird.

Die Verarbeitung **besonderer Kategorien** personenbezogener Daten (dazu gehört z. B. die Gewerkschaftszugehörigkeit) ist dann für die Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung nicht überwiegt. Alternativ ist auch eine ausdrückliche Einwilligung der betroffenen Person möglich.

- Zu beachten ist, dass diese Regelungen auch dann gelten, wenn personenbezogene Daten von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

- Das Unternehmen muss sicherstellen, dass insbesondere die unter Punkt 4 dieser Publikation dargelegten Grundsätze bzgl. der personenbezogenen Arbeitnehmerdaten eingehalten werden.

Beachten Sie, dass unter dem Beschäftigtenbegriff auch **Zeitarbeitskräfte** zu verstehen sind.

11. In welchen Fällen muss ein Datenschutzbeauftragter benannt werden?

Sofern im Unternehmen

- **in der Regel**
- **mindestens zehn Personen**
- **ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind,**

ist wie auch schon nach bisherigem Datenschutzrecht ein Datenschutzbeauftragter zwingend zu benennen.

Die Formulierung **„in der Regel"** stellt auf die Fluktuation innerhalb der Beschäftigtenzahl bei der verantwortlichen Stelle ab. Der Gesetzgeber geht hiernach von einem längeren Zeitraum aus und toleriert vorübergehende Schwankungen. **Die kurzzeitige Überschreitung der maßgeblichen Beschäftigtenzahl löst die Pflicht zur Bestellung noch nicht aus.** Bei einem Überschreiten für einen Zeitraum von einem Jahr an wird die Kurzfristigkeit nicht mehr vorliegen. Maßgeblich ist der im größten Teil des Jahres bestehende normale Beschäftigungsstand, nicht die durchschnittliche Beschäftigtenzahl.

Das Merkmal **„ständig"** setzt voraus, dass die Person für eine längere, meist unbestimmte Zeit mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt ist, ohne dass dies die ausschließliche Beschäftigung sein muss. **Auch eine nur gelegentlich, etwa einmal im Monat anfallende Aufgabe erfüllt das Merkmal „ständig", wenn die Person sie stets wahrzunehmen hat. Die Beschäftigung muss zu einem regelmäßig wiederkehrenden und festen Bestandteil ihrer Aufgaben zählen. Der zeitliche Einsatz im Verhältnis zur Gesamtarbeitszeit ist ohne Relevanz.** Auch eine stundenweise Beschäftigung ist „ständig", sofern sie auf unbestimmte oder längere Zeit ausgeübt wird. Personen, die nur gelegentlich oder vorübergehend eine Aufgabe mit übernehmen, wie z. B. während einer Urlaubsvertretung, sind hingegen nicht „ständig" beschäftigt.

Zu beachten ist, dass nicht jeder Mitarbeiter die Rolle des Datenschutzbeauftragten übernehmen darf, da Interessenkonflikte vermieden werden müssen. **So darf beispielsweise der Geschäftsführer nicht als Datenschutzbeauftragter benannt werden.**

Sofern ein Datenschutzbeauftragter benannt wird oder benannt werden muss, muss dieser die erforderliche Fachkunde und Zuverlässigkeit besitzen. Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten, hinsichtlich ihrer datenschutzrechtlichen Pflichten
- Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter
- Überwachung der Einhaltung der neuen datenschutzrechtlichen Regelungen sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten
- Zusammenarbeit mit der Aufsichtsbehörde

Es kann sowohl ein unternehmensinterner als auch ein unternehmensexterner Datenschutzbeauftragter benannt werden. Zwar ist für die Tätigkeit eines unternehmensinternen Datenschutzbeauftragten keine bestimmte Ausbildung vorgesehen, jedoch setzt diese Tätigkeit entsprechende technische und juristische Kenntnisse voraus. Insofern sind entsprechende regelmäßige Fortbildungen für unternehmensinterne Datenschutzbeauftragte zu empfehlen.

Die Kosten der Bestellung eines externen Datenschutzbeauftragten können nicht pauschal beziffert werden und hängen von der vertraglichen Vereinbarung und dem Umfang der zu erbringenden Leistungen ab.

12. Auftragsverarbeiter

Sofern eine Verarbeitung von personenbezogenen Daten durch einen sog. Auftragsverarbeiter erfolgt, müssen diese Auftragsverarbeiter hinreichend Garantien dafür bieten können, dass die Verarbeitung der Daten im Einklang mit der DSGVO erfolgt. Typische Fälle einer Auftragsverarbeitung stellen die externe Lohn- oder Gehaltsabrechnung oder das Webhosting der Unternehmenswebseite durch einen Dienstleister dar. **Grundlage für die Auftragsverarbeitung muss ab 25. Mai 2018 ein Vertrag sein, in dem Dauer, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind.** Sofern Sie also mit einem Auftragsverarbeiter zusammenarbeiten, sollten Sie den Kontakt zu diesem suchen und die Anpassung des Vertrags unter Berücksichtigung der neuen Vorgaben erörtern. Neben weiteren detaillierten Vertragsbestandteilen, welche sich aus **Artikel 28 Absatz 3 Satz 2 Buchstabe a) – h) DSGVO** ergeben, muss beispielsweise eine **Vertraulichkeitsklausel** Bestandteil des Vertrags sein.

13. Mitarbeiterschulung

Auch wenn Mitarbeiterschulungen für den Verantwortlichen grundsätzlich nicht verpflichtend sind - dies gehört zum Aufgabenbereich des Datenschutzbeauftragten – raten wir auch Unternehmen ohne Datenschutzbeauftragten dazu, Mitarbeiter, die regelmäßig mit personenbezogenen Daten umgehen, zu schulen und für das Thema Datenschutz zu sensibilisieren. Letztlich kann den Vorgaben der DSGVO und des BDSG-neu nur in vollem Umfang nachgekommen werden, wenn alle Mitarbeiter hinreichend sensibilisiert sind und über die neue Rechtslage in Kenntnis gesetzt wurden.

Haben Sie weitere Fragen zur Bedeutung des neuen Datenschutzrechts für die Gastronomie?

Bei weiteren Fragen zum Thema DSGVO können sich DEHOGA-Mitglieder jederzeit direkt an den DEHOGA Bundesverband wenden (reuter@dehoga.de).

Falls es sich bei Ihrem Unternehmen um ein Hotel oder eine Hotelkette handelt, weisen wir auf das DSGVO-Leitfaden des Hotelverbandes (IHA) hin, welches Sie hier downloaden können: https://www.hotellerie.de/go/iha-leitfaden-das-neue-datenschutzrecht-informationen-praxistipps. Bei weiteren hotelspezifischen Fragen können sich IHA-Mitglieder direkt an den Hotelverband wenden (franze@hotellerie.de).

Rechtlicher Hinweis: *Trotz sorgfältiger inhaltlicher Kontrolle übernehmen wir keine Haftung für die Richtigkeit, Vollständigkeit und Aktualität dieser Publikation nebst Anlagen. Sie soll gastronomischen Betrieben als Überblick über die neuen Vorschriften dienen und sie diesbezüglich sensibilisieren. Sie ist jedoch keine Rechtsberatung und vermag eine Rechtsberatung durch einen Rechtsanwalt im Einzelfall auch nicht zu ersetzen.*

Anlage 1: Verzeichnis von Verarbeitungstätigkeiten (Muster-VVT)
Anlage 2: Erläuterungen zur Verwendung des Muster-VVT

Deutscher Hotel- und Gaststättenverband e.V. (DEHOGA Bundesverband)
Verbändehaus Handel-Dienstleistung-Tourismus · Am Weidendamm 1A · 10117 Berlin
Fon 030/72 62 52-0 · Fax 030/72 62 52-42 · info@dehoga.de · www.dehoga.de

Verzeichnis von Verarbeitungstätigkeiten **Verantwortlicher** **gem. Artikel 30 Abs. 1 DSGVO**	Vorblatt

Angaben zum Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Hauptniederlassung: ☐ ja ☐ nein

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Internet-Adresse

Angaben zum ggf. gemeinsam mit diesem Verantwortlichen

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Angaben zum Vertreter des Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Angaben zur Person des Datenschutzbeauftragten * (extern mit Anschrift)

* sofern gem. Artikel 37 DS-GVO benannt

Anrede Titel

Name, Vorname

Straße

Postleitzahl

Ort

Telefon

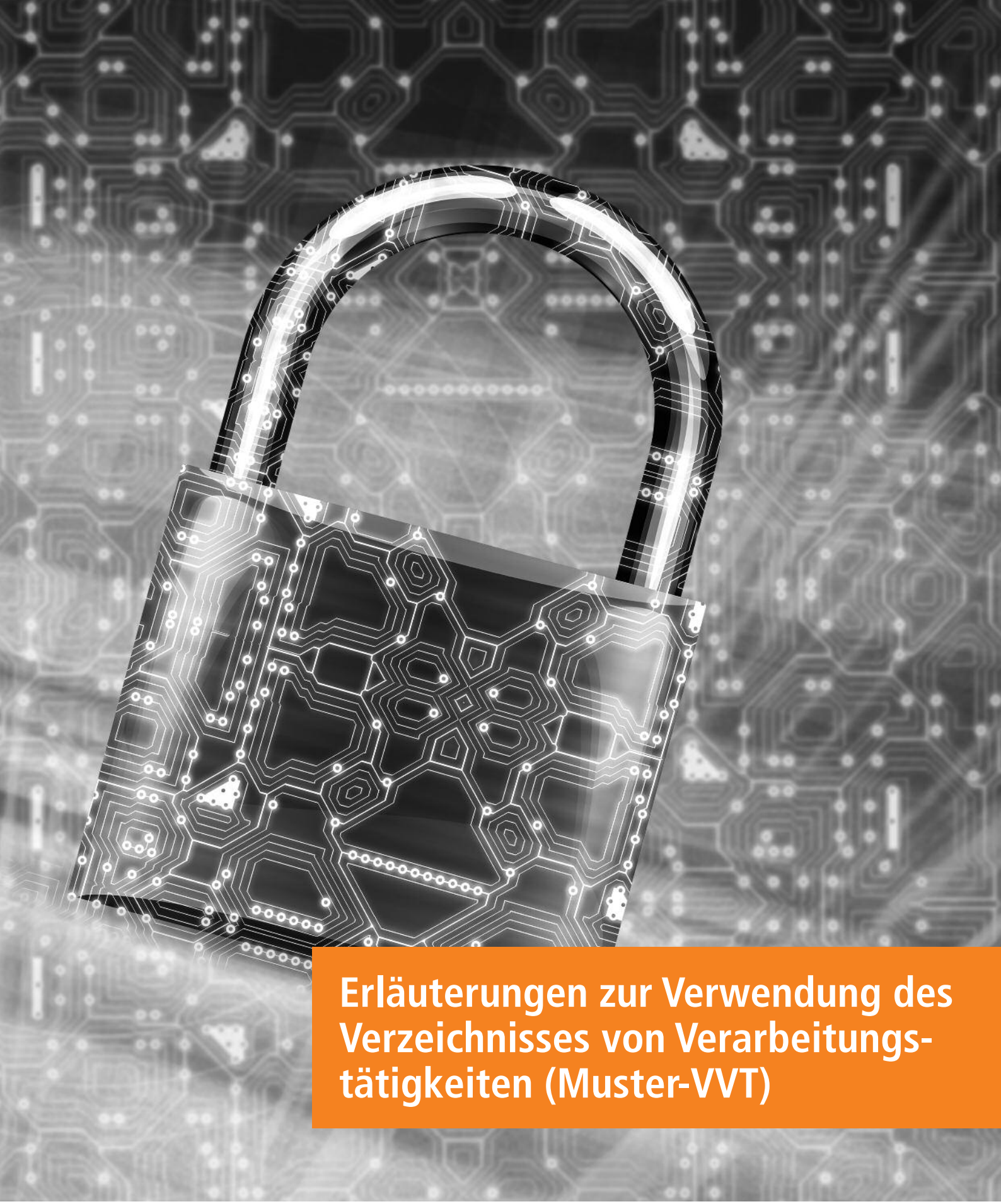
E-Mail-Adresse

Bezeichnung der Verarbeitungstätigkeit	Anlage
Datum der Anlegung:	Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse	
Bezeichnung der Verarbeitungstätigkeit	
Zwecke der Verarbeitung	
Beschreibung der Kategorien betroffener Personen	☐ Beschäftigte ☐ Interessenten ☐ Lieferanten ☐ Kunden ☐ Patienten ☐ Sonstige:
Beschreibung der Datenkategorien	☐ ☐ ☐ Sonstige: Besondere Arten personenbezogener Daten: ☐

Kategorien von Empfängern, gegenüber denen die personen-bezogenen Daten offen gelegt worden sind oder noch werden	☐ intern Abteilung/ Funktion
	☐ extern Empfängerkategorie
Datenübermittlung Nennung der konkreten Datenempfänger Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	☐ Datenübermittlung findet nicht statt und ist auch nicht geplant ☐ Datenübermittlung findet wie folgt statt: ☐ Drittland, Name: ☐ internationale Organisation, Bezeichnung: Empfängerkategorie Dokumentation geeigneter Garantien
Fristen für die Löschung der verschiedenen Datenkategorien	

Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs.1 DSGVO Bemerkungen*: siehe TOM-Beschreibung*

…… …… .....
Verantwortlicher Datum Unterschrift



Erläuterungen zur Verwendung des Verzeichnisses von Verarbeitungstätigkeiten (Muster-VVT)

DEHOGA
BUNDESVERBAND

Seite 1 des Muster-VVT

Hinweis: *Seite 1 muss nur einmalig ausgefüllt werden.*

Im Feld **„Angaben zum Verantwortlichen"** geben Sie die Angaben zu Ihrem Unternehmen an.

Das Feld **„Angaben zum ggf. gemeinsam mit diesem Verantwortlichen"** muss in der Regel nicht ausgefüllt werden.

Das Feld **„Angaben zum Vertreter des Verantwortlichen"** muss in der Regel nicht ausgefüllt werden. Nur Unternehmen, die nicht in der EU niedergelassen sind, müssen laut DSGVO einen „Vertreter" benennen.

Das Feld **„Angaben zur Person des Datenschutzbeauftragten"** muss nur ausgefüllt werden, sofern ein Datenschutzbeauftragter benannt wurde.

Seite 2 des Muster-VVT

Hinweis: *Seiten 2 und 3 müssen in der Regel kopiert werden und für jede Verarbeitungstätigkeit, bei der personenbezogene Daten verarbeitet werden, separat ausgefüllt werden. So müssen Seite 2 und 3 beispielsweise jeweils für die Verarbeitung von*

- Gästedaten, die über die Unternehmenswebseite erfasst werden,
- Personaldaten, die in der Personalabteilung verarbeitet werden
- Daten von Vertragspartnern, die aufbewahrt werden

ausgefüllt werden.

„Datum der Anlegung": Tragen Sie hier das Datum der Anlegung ein.

„Datum der letzten Änderung": Sofern sich Datenverarbeitungsprozesse geändert haben (z.B. neuer Ansprechpartner aufgrund von Personalwechsel), müssen Sie auch das VVT anpassen und hier das Datum der letzten Änderung eintragen.

„Verantwortliche Fachabteilung“: z.B. „Buchhaltung“, „Personalwesen“, „Marketing“, „Geschäftsführung“

„Ansprechpartner“: Name des entsprechenden Mitarbeiters

„Telefon“: Dienstliche Telefonnummer des entsprechenden Mitarbeiters

„E-Mail-Adresse“: Dienstliche E-Mail-Adresse des entsprechenden Mitarbeiters

„Bezeichnung der Verarbeitungstätigkeit“: In diesem Feld wird die konkrete Bezeichnung der entsprechenden Verarbeitungstätigkeit, bei der personenbezogene Daten eine Rolle spielen, eingetragen.

Bespiele für typische Verarbeitungstätigkeiten, bei denen personenbezogene Daten eine Rolle spielen:

- Erfassen und Speichern von Personaldaten der Mitarbeiter,
- Speichern von Gästedaten, die über die Unternehmenswebseite erfasst werden,
- Aufbewahrung von vertraglichen Unterlagen

„Zwecke der Verarbeitung“: Hier wird eingetragen, zu welchem Zweck personenbezogene Daten verarbeitet werden.

Beispiele für typische Verarbeitungszwecke:

- Lohnabrechnung,
- Restaurantreservierung über die Webseite,
- Aufbewahrung von Dokumenten gemäß Handelsgesetzbuch/Abgabenordnung um gesetzliche Aufbewahrungsfristen einzuhalten

„Beschreibung der Kategorien betroffener Personen“: Kreuzen Sie hier die betroffene Personengruppe(n) an, deren personenbezogene Daten bei der entsprechenden Verarbeitungstätigkeit verarbeitet werden.

„Beschreibung der Datenkategorien“: Hier können Sie die personenbezogenen Daten, die verarbeitet werden, kategorisieren. Es bietet sich beispielsweise an folgende Kategorien hinter den Kästchen zu notieren:

- Daten, die der 6 bzw. 10 jährigen Aufbewahrungsfrist gemäß Handelsgesetzbuch und Abgabenordnung unterliegen
- Daten die keiner gesetzlich geregelten Aufbewahrungsfrist unterliegen

Das Feld **„Besondere Arten personenbezogener Daten“** muss in der Regel nicht angekreuzt werden. „Sensible Daten“ werden in der Gastronomie regelmäßig nicht verarbeitet.

„Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden“: Unterscheiden Sie hier zwischen internen und externen Empfängern. Interne Empfänger können andere Fachabteilungen innerhalb des Unternehmens sein. Externe Empfänger können beispielsweise Dienstleister sein, die im Rahmen einer Auftragsverarbeitung tätig werden. Bei externen Empfängern sollten auch die Kontaktdaten angegeben werden.

„Datenübermittlung“: Dieses Feld muss in der Regel nicht ausgefüllt werden, da damit die Datenübermittlung an ein Land außerhalb der EU gemeint ist.

„Nennung der konkreten Datenempfänger“: Dieses Feld muss in der Regel nicht ausgefüllt werden.

„Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DSGVO genannte Datenübermittlung handelt.“: Dieses Feld muss in der Regel nicht ausgefüllt werden.

„Fristen für die Löschung der verschiedenen Datenkategorien“: Tragen Sie hier jeweilige Löschfristen ein. Wenn sich die Fristen aus dem Gesetz ergeben (6/10 Jahre), können Sie sich einfach an diesen Fristen orientieren. Sobald die Daten für den jeweiligen Zweck nicht mehr benötigt werden, sollten diese in der Regel gelöscht werden.

„Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs.1 DSGVO Bemerkungen: siehe TOM-Beschreibung“: In einer sogenannten „TOM-Beschreibung“ sollten Sie die technischen und organisatorischen Maßnahmen niederschreiben, die je nach Status quo des Datenschutzes und Art und Umfang der Datenverarbeitungsprozesse variieren können (Siehe dazu Punkt 6 der Publikation). Folgende Standardmaßnahmen kommen typischerweise in Betracht:

- Regelmäßige Updates des verwendeten Computersystems und des Anti-Virenprogramms.
- Aktenschränke, welche Dokumentenordner mit personenbezogenen Daten enthalten, stets verschlossen halten.
- Regelmäßige Back-Ups.
- Sicherstellung, dass Mitarbeiter nur auf Dateien zugreifen können, die für die jeweils entsprechende Tätigkeit nötig sind.
- Regelmäßige Schulungen der Mitarbeiter hinsichtlich Datenschutz (z.B. einmal jährlich).
- Regelmäßige Überprüfung, ob die Maßnahmen wirksam sind oder Anpassungen erforderlich sind (z.B. alle 6 Monate).