

Nr. 05 / 2020



Newsletter Datenschutz

In dieser Ausgabe:

Verordnung zur Bekämpfung der Corona-Pandemie und verpflichtende Kundendatenverarbeitung	2
Schutz personenbezogener Daten bei der Übermittlung per E-Mail.....	3
BGH zur Einwilligung in telefonische Werbung und Cookie-Speicherung	4
Auskunftspflicht umfasst auch Angabe über die konkrete Herkunft der Daten	5
Kein Auskunftsanspruch, wenn Aufwand zu hoch	5
VERANSTALTUNGEN	6

Verordnung zur Bekämpfung der Corona-Pandemie und verpflichtende Kundendatenverarbeitung

Bereits mit Wirkung zum 18. Mai 2020 hat die Landesregierung eine Regelung für Gastronomiebetriebe zur Erhebung und Speicherung von Kundendaten geschaffen. Diese Regelung wurde mit Wirkung zum 1. Juni 2020 angepasst und auf Theater, Opern- und Konzerthäuser sowie auf Betreiber von Kinos und Indoorspielplätzen ausgedehnt.

Nach Maßgabe des Hygieneplans der saarländischen Landesregierung für Gaststätten und Beherbergungsstätten sind durch Gastronomen Name, Vorname, Wohnort und Erreichbarkeit in Form einer Telefonnummer oder der E-Mail-Adresse je eines Vertreters der anwesenden Haushalte sowie deren Ankunftszeit zu erheben und für die Dauer eines Monats zu speichern. Rechtsgrundlage für die Verarbeitung ist Art. 6 Abs. 1 lit. c in Verbindung mit Abs. 2 und 3 DSGVO.

In welcher Form diese Pflicht zur Datenverarbeitung umgesetzt wird, bleibt letztlich dem jeweiligen Verantwortlichen überlassen. So könnte beispielsweise - unter Verwendung der regelmäßig vorhandenen Reservierungsbücher - eine schriftliche Notiz bereits im Rahmen der Reservierung erfolgen oder die Gäste beim Eintreffen im Betrieb erfasst werden. Sofern bereits Online-Reservierungssysteme benutzt werden, könnten auch über diese die notwendigen Kontaktdaten der Kunden abgefragt werden. Nicht zulässig ist es, bei den Gästen Ausweisdokumente zu fotografieren, zu scannen oder zu kopieren. Sind die Gästelisten angefertigt, müssen diese sorgsam aufbewahrt werden. Sie dürfen nicht für jeden einsehbar sein oder unbeaufsichtigt beispielsweise auf einem Empfangstresen liegen gelassen werden.

Um die Nachverfolgbarkeit von Infektionsketten zu ermöglichen, muss der Unternehmer bei einer Anforderung durch das zuständige Gesundheitsamt die von ihm erhobenen Kundenkontaktdaten an dieses weitergeben. Die Anforderung des Gesundheitsamts selbst ist auch zu dokumentieren. Die Daten sollten dabei nur auf einem sicheren Übertragungsweg (per Post, per Fax oder per E-Mail mit Ende-zu-Ende-Verschlüsselung) zur Verfügung gestellt werden.

Die so erhobenen Kundenkontaktdaten müssen für einen Monat gespeichert werden. Nach Fristablauf müssen die gespeicherten Daten fristgerecht vernichtet bzw. gelöscht werden. Das kann beispielsweise durch Schreddern von papiergeführten Listen und Erfassungsbögen oder durch Löschen bei digitaler Speicherung erfolgen.

Absolut unzulässig ist eine zweckwidrige Weiterverarbeitung der Kundenkontaktdaten, wie beispielsweise eine Verwendung oder Weitergabe für Werbezwecke.

Die betroffenen Kunden sind durch Informationen im Sinne des Art. 13 DSGVO über Zweck und Ausgestaltung der Datenverarbeitung zu informieren.

Entsprechende Muster finden Sie bei der [Homepage des Unabhängigen Datenschutzzentrums \(UDZ\) Saarland](#).

Quelle: PM des UZD vom 3. Juni 2020

Schutz personenbezogener Daten bei der Übermittlung per E-Mail

Verantwortliche und Auftragsverarbeiter sind gesetzlich gehalten, die Risiken, die sich aus ihren Verarbeitungen personenbezogener Daten ergeben, hinreichend zu mindern. Das betrifft auch Risiken, die durch die Übermittlung personenbezogener Daten per E-Mail entstehen.

Der gesetzlich gebotene Schutz personenbezogener Daten im Zuge der Übermittlung von E-Mail-Nachrichten erstreckt sich sowohl auf die personenbezogenen Inhalte als auch auf die Umstände der Kommunikation, soweit sich aus Letzteren Informationen über natürliche Personen ableiten lassen.

Sowohl Transportverschlüsselung als auch Ende-zu-Ende-Verschlüsselung mindern für ihren jeweiligen Anwendungszweck Risiken für die Vertraulichkeit und Integrität der übertragenen personenbezogenen Daten. Der Einsatz von Transportverschlüsselung bietet lediglich einen Basis-Schutz und stellt eine Mindestmaßnahme zur Erfüllung der gesetzlichen Anforderungen dar. Der durchgreifendste Schutz der Inhaltsdaten wird hingegen durch Ende-zu-Ende-Verschlüsselung erreicht. Verantwortliche müssen beide Verfahren in der Abwägung der notwendigen Maßnahmen berücksichtigen.

In einer von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder mehrheitlich verabschiedeten Orientierungshilfe werden die Anforderungen an die Verfahren zum Versand und zur Entgegennahme von E-Mail-Nachrichten erläutert.

Dazu gehören

- **Obligatorische Transportverschlüsselung**
Verantwortliche, die E-Mail-Nachrichten mit personenbezogenen Daten versenden, bei denen ein Bruch der Vertraulichkeit ein normales Risiko für die Rechte und Freiheiten von natürlichen Personen darstellt, sollten sich an der TR 03108-1 orientieren und müssen eine obligatorische Transportverschlüsselung sicherstellen
- **Ende zu-Ende-Verschlüsselung:**
Verantwortliche, die E-Mail-Nachrichten versenden, bei denen ein Bruch der Vertraulichkeit von personenbezogenen Daten im Inhalt der Nachricht ein hohes Risiko für die Rechte und Freiheiten von natürlichen Personen darstellt, müssen regelmäßig eine Ende-zu-Ende-Verschlüsselung und eine qualifizierte Transportverschlüsselung vornehmen.

Die Datenschutzkonferenz empfiehlt den Verantwortlichen, ihren Auftragsverarbeitern und öffentlichen E-Mail-Diensteanbietern, die in der Orientierungshilfe genannten Anforderungen umzusetzen, um den Schutz personenbezogener Daten bei der Übermittlung per E-Mail zu gewährleisten.

Quelle: [Pressemitteilung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 26.05.2020](#)

BGH zur Einwilligung in telefonische Werbung und Cookie-Speicherung

Nachdem der EuGH mit Urteil vom 01.10.2019 eine Einwilligungspflicht für nicht essentielle Cookies festgestellt hat, hat sich nunmehr auch der BGH mit der Frage befasst, welche Anforderungen an die Einwilligung in telefonische Werbung und die Speicherung von Cookies auf dem Endgerät des Nutzers zu stellen sind.

Der Sachverhalt: Die Beklagte veranstaltete im September 2013 unter ihrer Internetadresse ein Gewinnspiel. Um an dem Gewinnspiel teilnehmen zu können, musste der Nutzer verschiedene Eingabefelder ausfüllen. Unter den Eingabefeldern befanden sich zwei mit Ankreuzfeldern versehene Einverständniserklärungen.

Mit Bestätigen des ersten Textes, dessen Ankreuzfeld nicht mit einem voreingestellten Häkchen versehen war, sollte der Nutzer sein Einverständnis dazu geben, per Post, Telefon, E-Mail oder SMS durch Sponsoren und Kooperationspartner der Beklagten zum Zwecke der Werbung kontaktiert zu werden. Dabei bestand die Möglichkeit, die werbenden Sponsoren und Kooperationspartner aus einer verlinkten Liste von 57 Unternehmen selbst auszuwählen. Andernfalls sollte die Beklagte diese Auswahl treffen.

Das zweite Ankreuzfeld war mit einem voreingestellten Häkchen versehen. Der Nutzer erklärte sich damit einverstanden, dass ein Webanalysedienst eingesetzt wird, der eine Auswertung des Surf- und Nutzungsverhaltens ermöglicht. Der voreingestellte Haken konnte entfernt werden. Eine Teilnahme am Gewinnspiel war aber nur möglich, wenn mindestens eines der beiden Felder mit einem Haken versehen war.

Der BGH hat vor seiner Entscheidung den EuGH im Wege eines sog. Vorabverfahrens zur Auslegung der einschlägigen Regelungen befragt. Der EuGH hat entschieden, dass keine wirksame Einwilligung vorliegt, wenn die Speicherung von Informationen mittels Cookies durch ein voreingestelltes Ankreuzkästchen erlaubt wird, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss. Irrelevant sei es zudem, ob es sich bei den Informationen um personenbezogene Daten handelt oder nicht. Dieser Entscheidung hat sich der BGH nunmehr angeschlossen.

Hinsichtlich der Einwilligung in die telefonische Werbung fehlt es an einer wirksamen Einwilligung. Die Einwilligung muss "für den konkreten Fall" erfolgen. Daran fehlt es, da der Verbraucher in der Einwilligungserklärung mit einer Auswahl von 57 Partnerunternehmen konfrontiert wurde, um ihn zu veranlassen, von dieser Auswahl abzuweichen und stattdessen der Beklagten die Wahl der Werbepartner zu überlassen.

Die Einwilligung in die Speicherung von Cookies durch den Webanalysedienst, die den Abruf von auf seinem Endgerät gespeicherten Informationen mithilfe von Cookies im Wege eines voreingestellten Ankreuzkästchens gestattet, ist ebenfalls unwirksam.

BGH, Urteil vom 28. Mai 2020, I ZR 7/16

Praxistipp: Nachdem sowohl der EuGH als auch der BGH nunmehr entschieden haben, dass eine aktive Einwilligung des Nutzers in die Speicherung von Cookies notwendig ist, sind Unternehmen gezwungen zu handeln und Ihre Homepage datenschutzsicher zu gestalten.

Auskunftspflicht umfasst auch Angabe über die konkrete Herkunft der Daten

Nach der DSGVO hat jeder Betroffene das Recht zu erfahren, ob und welche personenbezogenen Daten über ihn gespeichert werden. Dieser Auskunftsanspruch beinhaltet auch alle verfügbaren Informationen über die Herkunft der Daten. Dies bestätigte nun das LG Mosbach.

Die Beklagte wurde vom Amtsgerichts Wertheim zur Auskunftserteilung nach Art. 15 Abs. 1 a-h DSGVO verurteilt. Nach Ansicht des Klägers kam die Beklagte Ihrer Auskunftspflicht nach Art. 15 Abs. 1 h DSGVO (Herkunft der personenbezogenen Daten) nur unzureichend nach. Er beantragte die Festsetzung eines Zwangsgeldes von bis zu 25.000 €, ersatzweise Zwangshaft von bis zu sechs Monaten, um die Erfüllung der titulierten Verpflichtung durchzusetzen. Das Amtsgericht Wertheim gab dem Antrag statt. Hiergegen legte die Beklagte die sofortige Beschwerde ein. Das AG hat der sofortigen Beschwerden ohne besondere Begründung nicht abgeholfen und die Beschwerde dem Landgericht Mosbach zur Entscheidung vorgelegt.

Die sofortige Beschwerde war zulässig und hatte teilweise Erfolg. Soweit sich die Beklagte darauf beruft, auch der unter g titulierte Anspruch auf Auskunftserteilung, woher die Beklagte die persönlichen Daten des Klägers erhalten hat, ist dies jedoch unzutreffend. Jener Auskunftsanspruch ist noch nicht erfüllt. Die Beklagte hat nicht in genügender Tiefe mitgeteilt, woher sie diese Daten erhalten hat.

Nach Art. 15 ist stets Auskunft über "alle verfügbaren Informationen über die Herkunft" der Daten zu geben. Dabei sind auch die Mittel zu benennen, mit denen die personenbezogenen Daten erhoben wurden.

Die Beklagte erklärt lediglich - und dies auch nicht in ihrem ursprünglichen Auskunftsschreiben, sondern erst mit Schriftsatz im Beschwerdeverfahren - dass die bei ihr gespeicherten Daten alleine im Rahmen eines Bezahlvorgangs erhoben worden seien. Weitere Auskünfte zur Herkunft der Daten wurden verweigert. Aus den Angaben ergab sich nicht, wann, in welcher Form und von wem die Beklagte die persönlichen Daten des Klägers erlangt hat.

LG Mosbach, Beschluss vom 27. Januar 2020, 5 T 4/20

Praxistipp: Verlangt der Betroffene Auskunft, muss diese grundsätzlich spätestens innerhalb von einem Monat zur Verfügung gestellt werden. Hierzu sind konkrete Informationen notwendig. Ein Muster für ein Auskunftsschreiben finden Sie in unserem Infoblatt → **D12** „[Auftragsverarbeitung nach der DSGVO](#)“, [Kennzahl 2158](#).

Kein Auskunftsanspruch, wenn Aufwand zu hoch

Das LG Heidelberg hat entschieden, dass kein Auskunftsanspruch nach Art. 15 DSGVO besteht, wenn der Aufwand unverhältnismäßig ist. In dem vorliegenden Fall hat das Gericht eine Unverhältnismäßigkeit bei Sichtung und Anonymisierung von über 10.000 E-Mails bejaht.

Der Beklagte lehnte einen Auskunftsanspruch unter anderen ab, da die Auskunftsfrage zu unbestimmt sei und die Erfüllung des Auskunftsanspruchs für ihn einen unverhältnismäßigen Aufwand bedeute. Allein die hilfsweise begehrte E-Mail-Korrespondenz betreffe ca. 10.000 E-Mails, die zunächst auf den IT-Servern wiederhergestellt und geschwärzt werden müssen.

Das LG hat einen Auskunftsanspruch abgelehnt. Für Verantwortliche, die eine große Menge von Informationen über die betroffene Person verarbeiten, sieht Erwägungsgrund 63 eine Erleichterung bei einem (pauschalen) Auskunftersuchen vor. So darf der Verantwortliche vor Auskunftserteilung von der betroffenen Person eine Präzisierung des Auskunftsbegehrens verlangen. Der Verantwortliche muss zudem grundsätzlich keine Auskunft über Daten erteilen, die er in der Vergangenheit verarbeitet hat, über die er jedoch nicht mehr verfügt. Daten in Backups sind für den Verantwortlichen u.U. nicht unmittelbar greifbar. Nach dem „alten“ Datenschutzrecht durfte vormals die Auskunft entfallen, wenn die Daten ausschließlich der Datensicherung dienten und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordert. Der Wegfall dieser Spezialnorm bedeutet jedoch keineswegs, dass nun sämtliche Backups Gegenstand der Auskunftsverpflichtung geworden wären. Vielmehr kommt es auch hier auf den konkreten Aufwand auf Seiten des Verantwortlichen an.

LG Heidelberg, Urteil vom 06. Februar 2020, 4 O 6/19

VERANSTALTUNGEN

Aufgrund der aktuellen Entwicklung zum Coronavirus hat die IHK Saarland alle Präsenzveranstaltungen abgesagt. Vorläufig gilt die Absage bis 15. August 2020. Wir sind in Vorbereitung von Webinaren, über die wir Sie rechtzeitig auf unserer Homepage unter www.saarland.ihk.de informieren.

Verantwortlich und Redaktion:

Ass. iur. Heike Cloß, Tel.: (0681) 9520-600, Fax: (0681) 9520-690

E-Mail: heike.closs@saarland.ihk.de

IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken

Ihre Ansprechpartnerinnen:

Ass. iur. Heike Cloß

Tel.: (0681) 9520-600

Fax: (0681) 9520-690

E-Mail: heike.closs@saarland.ihk.de

Ass. iur. Kim Pleines

Tel.: (0681) 9520-640

Fax: (0681) 9520-690

E-Mail: kim.pleines@saarland.ihk.de

Impressum:

IHK Saarland, vertreten durch Präsident Dr. jur. Hanno Dornseifer und Hauptgeschäftsführer Dipl.-Volkswirt Dr. Heino Klingen, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken, E-Mail info@saarland.ihk.de, Tel. + 49 (0) 6 81/95 20-0, Fax + 49 (0) 6 81/95 20-8 88, UST.- Ident.- Nummer: DE 138117020