Geschäftsbereich
Recht, Zentrale Dienste

Nr. 06 / 2020

Newsletter Datenschutz

In dieser Ausgabe:

Industrie- und Handelskammer des Saarlandes
Postanschrift: IHK Saarland │ 66104 Saarbrücken │ Büroanschrift: Franz-Josef-Röder-Straße 9 │ 66119 Saarbrücken
Tel. 0681/9520-0 │ Fax 0681/9520-888 │ E-Mail: info@saarland.ihk.de │ Internet: www.saarland.ihk.de

EuGH kippt Privacy-Shield

Die DSGVO bestimmt, dass personenbezogene Daten grundsätzlich nur dann in ein Drittland übermittelt werden dürfen, wenn das betreffende Land für die Daten ein angemessenes Schutzniveau gewährleistet. Ein angemessenes Schutzniveau ist gewährleistet, wenn dies von der Kommission festgestellt wird, sog. Angemessenheitsbeschluss. Liegt ein solcher nicht vor, darf eine Übermittlung nur erfolgen, wenn der in der Union ansässige Exporteur der personenbezogenen Daten geeignete Garantien vorsieht. Bislang werden die meisten Datenübermittlungen in die USA auf den Durchführungsbeschluss (EU) 2016/1250, das sog. EU-US-Privacy Shield, gestützt. Mit aktuellem Urteil hat der EuGH entschieden, dass das Privacy-Shield-Abkommen unwirksam ist.

Ausgangspunkt für die Entscheidung des EuGH war die Beschwerde eines Facebook-Nutzers aus Österreich. Herr Schrems, so heißt der Nutzer, war nicht damit einverstanden, dass seine Daten ganz oder teilweise von Facebook Ireland an Server der Facebook Inc., die sich in den USA befinden, übermittelt und dort verarbeitet werden. Er legte bei der irischen Aufsichtsbehörde Beschwerde ein, die die Beschwerde mit der Begründung abwies, dass die USA durch das damalige „Safe-Harbour-Abkommen“ ein angemessenes Schutzniveau gewährleistet. Das irische High Court legte damals dem EuGH im Vorabentscheidungsverfahren die Frage vor, ob das Safe-Harbour-Abkommen gültig sei. Mit Urteil vom 6.Oktober 2015 erklärte der EuGH das Safe-Harbour-Abkommen für ungültig (Schrems I-Entscheidung). Als Folge des Urteils schloss die EU-Kommission mit den USA ein neues Abkommen, das sog. Privacy-Shield. Gegen das Abkommen und den Beschluss über Standardvertragsklauseln 2010/87 richtet sich Herr Schrems mit seiner neuformulierten Beschwerde, die ebenfalls dem EuGH zur Vorabentscheidung vorgelegt wurde.

In seinem aktuellen Urteil hat der EuGH den Angemessenheitsbeschluss zum Privacy Shield nun für ungültig erklärt. Er stellte fest, dass keine ausreichenden Regelungen getroffen wurden, um den Zugriff der USA auf die übermittelten Daten auf das zwingend erforderliche Maß zu beschränken. Die auf die amerikanischen Rechtsvorschriften gestützten Überwachungsprogramme sehen zwar Anforderungen vor, die von den amerikanischen Behörden bei der Durchführung der betreffenden Überwachungsprogramme einzuhalten sind. Diese verleihen den betroffenen Personen jedoch keine Rechte, die gegenüber den amerikanischen Behörden gerichtlich durchgesetzt werden können.

Der EuGH betont ausdrücklich, dass die Datenschutz-Aufsichtsbehörden verpflichtet sind, nach diesen Maßstäben unzulässige Datenexporte zu verbieten und dass betroffene Personen Schadensersatz für unzulässige Datenexporte verlangen können.

Der EuGH stellte weiter fest, dass der Beschluss über Standardvertragsklauseln 2010/87 für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern dagegen wirksam sei.

EuGH, Urteil vom 16. Juli 2020, C-311/18

Quelle: PM des EuGH vom 16. Juli 2020

Praxistipp: Die Entscheidung des EuGH sorgt erneut für Rechtsunsicherheit. Eine Möglichkeit, eine datenschutzkonforme Übermittlung sicherzustellen, ist, für die Übermittlung von Daten in Drittstaaten sog. Standarddatenschutzklauseln zu verwenden. Art. 49 DSGVO sieht als weitere Möglichkeit vor, dass die betroffene Person ausdrücklich in Datenübermittlung einwilligt. Problem: Die betroffene Person muss vorher umfassend über die für sie bestehenden möglichen Risiken einer solchen Datenübermittlung unterrichtet werden. Der sicherste Weg derzeit ist auf den Datentransfer in die USA vorerst zu verzichten und entsprechend verwendete Dienste zu deaktivieren.

EU-Kommission legt Evaluierungsbericht zur DSGVO vor

Leicht verspätet hat die EU-Kommission am 24.06.2020 ihren Evaluierungsbericht dem Europäischen Parlament vorgelegt. Darin wird der positive Effekt auf den Datenschutz hervorgehoben. Zugleich bemängelt die Kommission die teilweise schlechte Ausstattung der Aufsichtsbehörden in den Mitgliedstaaten.

Zurzeit liegt der Bericht nur in englischer Fassung vor.

Die Maßnahmen zur zulässigen Datenübermittlung in Drittstaaten, wie die Standardvertragsklauseln, müssen ohnehin aktualisiert werden. Damit wird die EU-Kommission aber bis nach dem Urteil des EuGH zu Schrems II warten, das in der Zwischenzeit vorliegt.

Inhaltlich wird es keine Änderungen der DSGVO geben, da eine Gesetzesänderung nach zwei Jahren Erfahrung zu früh sei.

DSK: Datenschutzfreundliches Grundkonzept der Corona-Warn-App

Mit der am 16. Juni 2020 durch den Bund vorgestellten Corona-Warn-App steht ein freiwilliges Instrument mit einer dezentralen Speicherung auf dem jeweiligen Smartphone zur Nachverfolgung eventueller Infektionen zur Verfügung. Dies teilt die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in einer Pressemitteilung mit.

Die DSK sieht das datenschutzfreundliche Grundkonzept als Realisierung des Grundsatzes von Datenschutz by Design. Sie weist allerdings darauf hin, dass insbesondere der Ansatz der Freiwilligkeit nicht durch eine zweckentfremdende Nutzung untergraben werden darf:

Der Zugang zu behördlichen Einrichtungen, Arbeitsstätten, Handelsgeschäften, Gastronomiebetrieben und Beherbergungsstätten, Sportstätten, etc. darf nicht vom Vorweisen der App abhängig gemacht werden.

Hierbei würde es sich um eine zweckwidrige Verwendung handeln, die bereits mit dem Konzept der Freiwilligkeit nicht vereinbar ist. Eine Diskriminierung von Personen, die die App nicht anwenden, ist auszuschließen.

Quelle: PM der DSK vom 16. Juni 2020

Berliner Datenschutzbeauftragte veröffentlicht Ergebnisse einer Kurzprüfung von Videokonferenzdiensten

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat die Ergebnisse einer Kurzprüfung von Videokonferenzdiensten verschiedener Anbieter auf ihrer Webseite veröffentlicht. Geprüft wurden die Auftragsverarbeitungsverträge, die die Verantwortlichen mit den Videokonferenz-Dienstanbietern standardmäßig schließen. Soweit die Auftragsverarbeitungsverträge rechtskonform sind, erfolgte zudem eine kursorische Untersuchung einiger technischer Aspekte der Dienste. Eine umfassende Prüfung der Dienste fand nicht statt. Insbesondere ist keine umfassende technische Prüfung und in der Regel auch keine Prüfung der Datenschutzerklärung erfolgt.

Bei der Bewertung der Dienste bedient sich die Aufsichtsbehörde eines Ampelsystems. Bei grün markierten Anbietern hat die Kurzprüfung keine Mängel ergeben. Die gelbe Markierung bedeutet bei der rechtlichen Bewertung, dass Mängel gefunden wurden, die eine rechtskonforme Nutzung des Dienstes zwar ausschließen, deren Beseitigung allerdings vermutlich ohne wesentliche Anpassungen der Geschäftsabläufe und der Technik möglich ist. In der technischen Prüfung bedeutet eine gelbe Markierung, dass die Anbieter unter Beachtung bestimmter Rahmenbedingungen nutzbar sind. Bei rot markierten Anbietern liegen Mängel vor, die eine rechtskonforme Nutzung des Dienstes ausschließen und deren Beseitigung vermutlich wesentliche Anpassungen der Geschäftsabläufe und/oder der Technik erfordern.

Die Liste wird von der Berliner Beauftragten für Datenschutz und Informationsfreiheit laufend ergänzt, wenn im Rahmen ihrer Aufsichts- und Beratungstätigkeit weitere Angebote geprüft wurden.

Die Ergebnisse der Kurzprüfung können auf der Homepage der Berliner Beauftragten für Datenschutz und Informationsfreiheit unter https://www.datenschutz-berlin.de/infothek-und-service/themen-a-bis-z/corona-Pandemie.html abgerufen werden.

Quelle: PM der Berliner Datenschutzbeauftragten vom 3. Juli 2020

Schutz personenbezogener Daten bei der Übermittlung per E-Mail

Wer Daten verarbeitet, ist dazu verpflichtet, die Risiken, die sich aus der Verarbeitung 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 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 Technische Richtlinie "Sicherer E-Mail-Transport" (BSI TR-03108) 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: PM der DSK vom 26. Juni 2020

LfDI Baden-Württemberg verhängt Bußgeld gegen AOK Baden-Württemberg

Wegen eines Verstoßes gegen die Pflichten zu sicherer Datenverarbeitung hat die Bußgeldstelle des LfDI Baden-Württemberg gegen die AOK Baden-Württemberg eine Geldbuße von 1.240.000,- Euro verhängt und – in konstruktiver Zusammenarbeit mit der AOK – zugleich die Weichen für eine Verbesserung der technischen und organisatorischen Maßnahmen zum Schutz persönlicher Daten bei der AOK Baden-Württemberg gestellt.

Die AOK Baden-Württemberg veranstaltete in den Jahren 2015 bis 2019 zu unterschiedlichen Gelegenheiten Gewinnspiele und erhob hierbei personenbezogene Daten der Teilnehmer, darunter deren Kontaktdaten und Krankenkassenzugehörigkeit. Dabei wollte die AOK die Daten der Gewinnspielteilnehmer auch zu Werbezwecken nutzen, sofern die Teilnehmer hierzu eingewilligt hatten. Mithilfe technischer und organisatorischer Maßnahmen, u. a. durch interne Richtlinien und Datenschutzschulungen, wollte die AOK hierbei sicherstellen, dass nur Daten solcher Gewinnspielteilnehmer zu Werbezwecken verwendet werden, die zuvor wirksam hierin eingewilligt hatten. Die von der AOK festgelegten Maßnahmen genügten jedoch nicht den gesetzlichen Anforderungen. In der Folge wurden die personenbezogenen Daten von mehr als 500 Gewinnspielteilnehmern ohne deren Einwilligung zu Werbezwecken verwendet. Versichertendaten waren hiervon nicht betroffen.

Die AOK Baden-Württemberg stellte unmittelbar nach Bekanntwerden des Vorwurfs alle vertrieblichen Maßnahmen ein, um sämtliche Abläufe grundlegend auf den Prüfstand zu stellen. Zudem gründete die AOK eine Task Force für Datenschutz im Vertrieb und passte neben den Einwilligungserklärungen insbesondere auch interne Prozesse und Kontrollstrukturen an. Weitere Maßnahmen sollen in enger Abstimmung mit dem LfDI erfolgen. Auf diese Weise konnte in kurzer Zeit eine Steigerung des Schutzniveaus für personenbezogene Daten bei Vertriebstätigkeiten der AOK erreicht werden.

Bei der Bemessung der Geldbuße wurde neben Umständen wie der Größe und Bedeutung der AOK Baden-Württemberg insbesondere auch berücksichtigt, dass sie als eine gesetzliche Krankenversicherung wichtiger Bestandteil unseres Gesundheitssystems ist. Schließlich obliegt der AOK die gesetzliche Aufgabe, die Gesundheit der Versicherten zu erhalten, wiederherzustellen oder zu verbessern. Weil Bußgelder nach der DSGVO nicht nur wirksam und abschreckend, sondern auch verhältnismäßig sein müssen, war bei der Bestimmung der Bußgeldhöhe sicherzustellen, dass die Erfüllung dieser gesetzlichen Aufgabe nicht gefährdet wird. Hierbei wurden die gegenwärtigen Herausforderungen für die AOK infolge der aktuellen Corona-Pandemie in besonderem Maße berücksichtigt.

Quelle: PM des LfDI Baden-Württemberg vom 30. Juni 2020

VERANSTALTUNGEN

„Insolvenzgründe und Corona“
Dienstag, 1. September 2020, 14.00 - 16.00 Uhr, Onlineveranstaltung

Herr Dr. Michael Bach, Heimes und Müller Rechtsanwälte, Saarbrücken, erklärt die Insolvenzgründe unter Berücksichtigung der Corona-Pandemie. Die Insolvenzantragspflicht ist temporär, zunächst bis zum 30. September dieses Jahres, ausgesetzt. Das bedeutet, dass die Insolvenzgründe selbst in Kraft bleiben, lediglich die Pflicht zur Antragstellung wurde ausgesetzt. Deshalb ist jeder Unternehmer gut beraten, die Insolvenzgründe zu überwachen, insbesondere wenn es darum geht, rechtzeitig die Weichen in Richtung gerichtliche Sanierung zu stellen.

Anmeldungen **bis 31. August 2020** unter E-Mail: veranstaltungen@saarland.ihk.de

„Datenschutz im Marketingbereich“
Montag, 21. September 2020, 14.00 - 16.00 Uhr, Onlineveranstaltung

Herr Stefan Staub, Geschäftsführer der Verimax GmbH, Saarbrücken, erklärt in seinem Vortrag, welche Datenschutzregelungen für die Unternehmerhomepage einzuhalten sind. Auch für die Werbemaßnahmen im Netz ist es wichtig, die Datenschutzvorgaben zu kennen. Keine Homepage kommt zudem mehr ohne Cookies aus. Die Rechtsprechung hat hier neue Maßstäbe gesetzt, wie Cookies rechtskonform eingebaut werden können. Er informiert außerdem über den Stand der ePrivacy-Verordnung.

Anmeldungen **bis 18. September 2020** unter
E-Mail: veranstaltungen@saarland.ihk.de

„Arbeitsschutz nach der Krise“
Montag, 28. September 2020, 14.00 - 16.00 Uhr, Onlineveranstaltung

Herr Rechtsanwalt Frank Gust, GUST Arbeitsrecht, Saarbrücken, geht in seinem Onlineseminar darauf ein, welche Fürsorgepflichten den Arbeitgeber für seine Mitarbeiter gerade in Krisenzeiten treffen. Er stellt vor, welche Arbeitsanweisungen deshalb der Arbeitgeber geben darf. Und auch, welche vertraglichen Regelungen schon im Vorfeld getroffen werden sollen. Zudem wird er darauf eingehen, was arbeitsschutzrechtlich zu beachten ist.

Anmeldungen **bis 25. September 2020** unter
E-Mail: veranstaltungen@saarland.ihk.de

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