Geschäftsbereich
Recht und Zentrale Dienste

Nr. 03 / März 2022

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

EU-Kommission legt Vorschlag für ein Europäisches Datengesetz vor

Ende Februar 2022 hat die EU-Kommission ihren Vorschlag für ein Datengesetz (Data Act) vorgelegt. Die vorgeschlagene Verordnung sieht zahlreiche neue Regeln für den Zugang zu und den Austausch von Daten, bei denen mehrere Parteien mitgewirkt haben (co-generated data), vor. Darüber hinaus soll öffentlichen Stellen in begründeten Fällen ein Zugangsrecht zu Unternehmensdaten eingeräumt werden. Durch die neuen Regelungen würden insb. auf Dateninhaber, Hersteller und Cloudanbieter neue Pflichten zukommen.

Ziel und Hintergrund des Gesetzesvorhabens

Der Data Act verfolgt das Ziel, dass mehr Daten für eine innovative Nutzung zur Verfügung stehen und nicht einzelne, große Akteure die alleinige Kontrolle über die Daten haben. Gemeinsam mit Initiativen wie dem Data Governance Act soll der Data Act dabei helfen, das Potential bislang weitgehend ungenutzter industrieller Daten auszuschöpfen. Dabei handelt es sich aus Sicht der Kommission vorwiegend um Daten von IoT-Objekten, also mit dem Internet vernetzte Geräte wie Haushaltsgeräte, Maschinen oder Autos. Viele dieser Objekte sammeln Daten, deren Mehrwert durch das Zusammenspiel zwischen Nutzer und Gerät generiert wird. Die Nutzungsrechte an diesen Daten sind bislang rechtlich nicht eindeutig geregelt. Sie und müssen daher zwischen den Parteien vertraglich vereinbart werden. Dabei sind insbesondere kleinere Unternehmen häufig mit unfairen Vertragsbedingungen konfrontiert. Oftmals sehen die Verträge vor, dass die Daten eines Geräts nur vom Hersteller genutzt werden dürfen.

Um den Zugang und die faire Nutzung von Daten zu erleichtern, führt der Gesetzesentwurf neue Rechte und Pflichten für Nutzer bzw. Dateninhaber ein:

1. Rechte und Pflichten für Nutzer

Konkret sieht der Gesetzesentwurf vor, dass in Zukunft vorwiegend Nutzer darüber entscheiden können, wie mit Daten umgegangen werden soll, an deren Entstehung sie mitgewirkt haben. Nutzer können dabei Unternehmen wie auch Verbraucher sein. Der Data Act soll es den Nutzern ermöglichen, diese Daten auszuwerten und unter bestimmten Bedingungen an Dritte weiterzugeben. Dabei müssen alle konkret erforderlichen Maßnahmen getroffen werden, um die Vertraulichkeit der Geschäftsgeheimnisse insbesondere gegenüber Dritten zu wahren.

Eine Einschränkung gilt jedoch für die Weitergabe von Daten an besonders große und mächtige Unternehmen, die nach dem Digital Markets Act als „Gatekeeper“ definiert werden. Der Nutzer darf die Daten nicht an Gatekeeper weitergeben. Gleichzeitig ist es den Gatekeepern untersagt, den Nutzer aufzufordern, Daten mit ihnen zu teilen oder Daten zu erhalten.

2. Rechte und Pflichten für Hersteller und Dateninhaber

Damit der Zugang und die Weitergabe von Daten auch technisch möglich ist, müssen Hersteller ihre Produkte und Dienstleistungen so gestalten, dass ein Datenzugang „unverzüglich“, wenn möglich sogar in „real-time“ stattfinden kann. Hinzu kommen neue Transparenz- und Informationspflichten, etwa über die Art und den Umfang der Datenerhebung. Der Dateninhaber ist verpflichtet, dem Nutzer Daten zur Verfügung zu stellen. Kleinst- und Kleinunternehmen sind von diesen Verpflichtungen ausgenommen.

Werden Daten übertragen, muss dies unter fairen, angemessenen und nichtdiskriminierenden Bedingungen und in transparenter Weise erfolgen. Die für die Bereitstellung von Daten vereinbarte Vergütung muss angemessen sein. Der Dateninhaber muss transparent aufzeigen können, wie sich die Kompensation zusammensetzt. Falls sich die Parteien nicht einig werden, ist eine unabhängige Schlichtung durch eine jeweils von den Mitgliedsstaaten benannte Behörde oder sonstige Einrichtung vorgesehen. Falls der Datenempfänger ein KMU ist, darf die verlangte Kompensation nicht die Kosten übersteigen, die direkt durch das Verfügbarmachen entstanden sind.

Der Dateninhaber darf nicht-personenbezogene Daten, die durch die Nutzung eines Produkts oder eines damit verbundenen Dienstes entstehen, nur auf der Grundlage einer vertraglichen Vereinbarung mit dem Nutzer verwenden.

3. Rechte und Pflichten für Cloud-Anbieter

Den Nutzern soll es erleichtert werden, ihren Anbieter von Datenverarbeitungsdiensten zu wechseln. Dies bedeutet neue Verpflichtungen für Dateninfrastrukturanbieter. Sie müssen den Umstellungsprozess unterstützen und jegliche kommerzielle, technische, vertragliche und organisatorische Hindernisse beseitigen. Zudem ist ein schrittweiser Abbau von Umstellungsgebühren geplant. Darüber hinaus sollen Anbieter von Datenverarbeitungsdiensten wie Cloud-Services verpflichtet werden, die Interoperabilität durch offene Standards und Schnittstellen erleichtern.

4. Rechte für öffentliche Stellen

Neben privaten Akteuren sollen auch öffentlichen Einrichtungen erweiterte Zugangsrechte eingeräumt werden. So muss ein Dateninhaber einer öffentlichen Einrichtung auf Antrag Daten zur Verfügung stellen, wenn ein „außergewöhnlichen Bedarf“ an der Nutzung der Daten besteht. KMU sind von dieser Regelung ausgenommen. Ein außergewöhnlicher Bedarf lieg vor, wenn eine öffentliche Notlage vorliegt, eine Notlage verhindert bzw. bekämpft werden muss, oder die Einrichtung ohne die angeforderten Daten nicht ihren rechtlichen Verpflichtungen nachkommen kann. Während die Daten in Notstandssituationen unentgeltlich bereitgestellt werden müssen, kann der Dateninhaber in anderen Fällen eine Aufwandsentschädigung für die Herausgabe verlangen.

Relevanz für Unternehmen und weiteres Vorgehen

Insgesamt wurde von der Kommission mit dem Data Act ein komplexes neues Regelwerk vorgelegt, das für viele unterschiedliche Bereiche Regelungen vorsieht, um den Zugang zu Daten zu erleichtern und Klarheit in Bezug auf Zugriffs- und Nutzungsrechte an Daten schaffen soll. Offen bleibt in diesem Zusammenhang allerdings, wie sensible Daten und Geschäftsgeheimnisse geschützt werden können und vor allem welche Möglichkeiten im Falle von Verstößen gegen das Verbot bestehen, die Daten für die Entwicklung von konkurrierenden Produkten einzusetzen.

Europäische KMU sollen durch den Data Act besonders gestärkt werden, indem sie vor unfairen Verträgen geschützt werden. Ob der Anreiz für Hersteller, datengetriebene Geschäftsmodelle und Innovationen zu entwickeln, erhalten bleibt, ist fraglich. Für Unternehmen aller Größe ist es wichtig, dass die Vorschriften verständlich und praktisch umsetzbar sind, ohne hohe bürokratische Belastungen.

Die IHK-Organisation hatte sich im Voraus im Rahmen einer Konsultation der EU-Kommission positioniert und möchte den Prozess weiterhin eng begleiten.

BSI warnt vor Kaspersky-Virenschutzsoftware

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt vor dem Einsatz von Virenschutzsoftware des russischen Herstellers Kaspersky. Das BSI empfiehlt, Anwendungen aus dem Portfolio von Virenschutzsoftware des Unternehmens Kaspersky durch alternative Produkte zu ersetzen.

Antivirensoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, verfügt über weitreichende Systemberechtigungen und muss systembedingt (zumindest für Aktualisierungen) eine dauerhafte, verschlüsselte und nicht prüfbare Verbindung zu Servern des Herstellers unterhalten. Daher ist Vertrauen in die Zuverlässigkeit und den Eigenschutz eines Herstellers sowie seiner authentischen Handlungsfähigkeit entscheidend für den sicheren Einsatz solcher Systeme. Wenn Zweifel an der Zuverlässigkeit des Herstellers bestehen, birgt Virenschutzsoftware ein besonderes Risiko für eine zu schützende IT-Infrastruktur.

Das Vorgehen militärischer und/oder nachrichtendienstlicher Kräfte in Russland sowie die im Zuge des aktuellen kriegerischen Konflikts von russischer Seite ausgesprochenen Drohungen gegen die EU, die NATO und die Bundesrepublik Deutschland sind mit einem erheblichen Risiko eines erfolgreichen IT-Angriffs verbunden. Ein russischer IT-Hersteller kann selbst offensive Operationen durchführen, gegen seinen Willen gezwungen werden, Zielsysteme anzugreifen, oder selbst als Opfer einer Cyber-Operation ohne seine Kenntnis ausspioniert oder als Werkzeug für Angriffe gegen seine eigenen Kunden missbraucht werden.

Alle Nutzerinnen und Nutzer der Virenschutzsoftware können von solchen Operationen betroffen sein. Unternehmen und Behörden mit besonderen Sicherheitsinteressen und Betreiber Kritischer Infrastrukturen sind in besonderem Maße gefährdet. Sie haben die Möglichkeit, sich vom BSI oder von den zuständigen Verfassungsschutzbehörden beraten zu lassen.

Unternehmen und andere Organisationen sollten den Austausch wesentlicher Bestandteile ihrer IT-Sicherheitsinfrastruktur sorgfältig planen und umsetzen. Würden IT-Sicherheitsprodukte und insbesondere Virenschutzsoftware ohne Vorbereitung abgeschaltet, wäre man Angriffen aus dem Internet möglicherweise schutzlos ausgeliefert. Der Umstieg auf andere Produkte ist mit vorübergehenden Komfort-, Funktions- und Sicherheitseinbußen verbunden. Das BSI empfiehlt, eine individuelle Bewertung und Abwägung der aktuellen Situation vorzunehmen und dazu gegebenenfalls vom BSI zertifizierte IT-Sicherheitsdienstleister hinzuzuziehen.

Weitere Informationen sind in den FAQ zusammengefasst.

Quelle: PM des BSI vom 15. März 2022

Warnung vor Phishing-Mails

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt vor Phishing-Versuchen im Namen von Banken und der Sparkassen. Die Kriminellen geben bspw. vor, dass man kontrollieren müsse, ob sich die Kundinnen und Kunden an die Sanktionen der EU halten. Deswegen sei eine erneute Verifikation der Daten notwendig.

Daneben sind erste Phishing-Mails mit Bezug zum Ukraine-Krieg im Umlauf, bei denen die Mail-Empfänger z.B. gebeten werden, vermeintlichen Opfern des Krieges Geld für die Flucht zu überweisen. Daneben ist auch klassisches Phishing, das mit reißerischer Berichterstattung die Mail-Empfänger zum Klicken zum Beispiel auf einen "Weiterlesen"-Button verleiten soll. Auch Scam-Mails, die betrügerische Spendenaufrufe verbreiten, sind in Umlauf. Bei den aktuellen Phishing-Mails wird demnach der Krieg gegen die Ukraine zu kriminellen Zwecken genutzt. Nach Einschätzung des BSI dürfte das Aufkommen an Phishing-Mails auch im deutschsprachigen Raum weiter zunehmen.

Das BSI stellt auf seiner Webseite Informationen zu Phishing-Versuchen zur Verfügung

BGH verneint für bestimmte Fälle Klarnamenpflicht bei der Nutzung eines sozialen Netzwerks

Der BGH hat sich in zwei Urteilen mit der Frage befasst, ob der Anbieters eines sozialen Netzwerks die Nutzung unter Pseudonym ermöglichen muss.

Die Kläger betreiben jeweils ein Nutzerkonto auf dem sozialen Netzwerk des Beklagten – Facebook. In beiden Fällen gaben die Kläger ein Pseudonym als Nutzernamen an. Facebook sperrte die Konten daraufhin. Der BGH entschied in der Revision, dass Facebook die Nutzung eines Pseudonyms zu dulden hat.

Nach den Nutzungsbedingungen von Facebook hat der Kontoinhaber bei der Nutzung des Netzwerks den Namen zu verwenden, den er auch im täglichen Leben verwendet. Diese Bestimmung ist unwirksam, weil sie den Kläger unangemessen benachteiligte. Sie ist mit dem in § 13 Abs. 6 Satz 1 TMG in der bis zum 30. November 2021 geltenden Fassung zum Ausdruck kommenden Grundgedanken, dass der Diensteanbieter die Nutzung der Telemedien anonym oder unter Pseudonym zu ermöglichen hat, soweit dies technisch möglich und zumutbar ist, nicht zu vereinbaren.

Das Gericht sah es zwar als zulässig an, dass der Nutzer bei der Registrierung seinen Klarnamen angibt. Die anschließende Nutzung von Facebook sei jedoch mit einem Pseudonym zu ermöglichen. Die Nutzer eines Facebook-Kontos können auch nicht verpflichtet werden, den Profilnamen in den wahren Namen zu ändern.

BGH, Urteile vom 27. Januar 2022, III ZR 3/21 und III ZR 4/21

Quelle: PM des BGH vom 28.01.2022

Kein Schadensersatz bei verspäteter Auskunft

Die Beantwortung eines Auskunftsbegehrens hat grundsätzlich innerhalb eines Monats zu erfolgen. Eine verspätete Auskunft führt nicht automatisch zu einem Schadensersatz. Das entschied das LG Leipzig.

Die Klägerin verlangt Datenauskunft von der Beklagten, eine Anwaltskanzlei, die sie in einem Scheidungsverfahren vertreten hatte. Dem kam die Beklagte nach. Kopien der Handakten wurden nicht herausgegeben. Die Beklagte weist darauf hin, dass sämtliche Schriftsätze unverzüglich an die Mandanten versandt worden und damit bereits im Besitz der Klägerin seien. Es bestehe zudem nur ein Anspruch auf Kopien

derjenigen Daten, die konkrete Informationen über die betroffene Person beinhalteten. Die Klägerin verlangte daraufhin Schmerzensgeld aufgrund einer unvollständigen Datenauskunft.

Das LG Leipzig legt Art. 15 Abs. 3 Satz 1 DSGVO, wonach ein Anspruch auf Herausgabe einer Kopie der personenbezogenen Daten besteht, weit aus. zu verstehen. Er ist nicht auf sensible oder private Informationen beschränkt, sondern umfasst potentiell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur in Form von Stellungnahmen oder Beurteilungen unter der Voraussetzung, dass es sich um Informationen über die in Rede stehende Person handelt. Der Anspruch umfasst auch Kopien der Handakten zu einem gerichtlichen Verfahren.

Einen Anspruch auf Schmerzensgeld verneinte das Gericht aber. Nach Art. 82 Abs. 1 DSGVO sind auch immaterielle Schäden auszugleichen. Der Anspruch sei auch nicht abhängig von einer schwerwiegenden Persönlichkeitsrechtsverletzung. Allein der Verstoß gegen die DSGVO reicht jedoch für sich genommen noch nicht aus, einen Schadensersatzanspruch auszulösen. Für den Betroffenen muss vielmehr ein spürbarer Nachteil entstanden sein. Dies wurde von der Klägerin nicht dargelegt.

LG Leipzig, Urteil vom 23. Dezember 2021, 03 O 1268721

LfDI Bremen verhängt Geldbuße in Höhe von 1,9 Millionen Euro

Der Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) hat eine große Wohnbaugesellschaft aus Bremen mit einem Bußgeld in Höhe von 1,9 Millionen Euro belegt.

Das Unternehmen hat mehr als 9.500 Daten – wie z.B. über Haarfrisuren, den Körpergeruch und das persönliche Auftreten – über Mietinteressenten verarbeitet, ohne dass es hierfür eine Rechtsgrundlage gab. Bei mehr als der Hälfte der Fälle handelte es sich darüber hinaus um Daten, die nach der DSGVO besonders geschützt sind wie etwa die Hautfarbe, die ethnische Herkunft, die Religionszugehörigkeit, die sexuelle Orientierung und über den Gesundheitszustand. Auch hat das Unternehmen Anträge Betroffener auf Transparenz über die Verarbeitung ihrer Daten bewusst verhindert.

Aufgrund der Schwere des Verstoßes gegen die datenschutzrechtlichen Bestimmungen wäre eine deutlich höhere Geldbuße angemessen gewesen. Weil das Unternehmen im datenschutzrechtlichen Aufsichtsverfahren umfassend kooperierte, sich um Schadensminderung, eigene Aufklärung des Sachverhalts und darum bemühte, dass entsprechende Verstöße sich nicht wiederholen, konnte die Höhe der Geldbuße erheblich reduziert werden.

Quelle: PM des LfDI Bremen vom 3, März 2022

VERANSTALTUNGEN

Early Bird-Reihe zum Arbeitsrecht

„Der Arbeitsvertrag: Was muss und was sollte drinstehen?“
Dienstag, 12. April 2022, 08:30 - 09:30 Uhr, Onlineveranstaltung

Anmeldungen **bis 11. April 2022** unter E-Mail: veranstaltungen@saarland.ihk.de oder per Direktlink.

„Arbeitsvertrag: Befristen und zwar richtig!“
Dienstag, 31. Mai 2022, 08:30 - 09:30 Uhr, Onlineveranstaltung

Anmeldungen **bis 30. Mai 2022** unter E-Mail: veranstaltungen@saarland.ihk.de oder per Direktlink.

„Urlaub: Chef, ich bin dann mal weg!“
Dienstag, 21. Juni 2022, 08:30 - 09:30 Uhr, Onlineveranstaltung

Anmeldungen **bis 20. Juni 2022** unter E-Mail: veranstaltungen@saarland.ihk.de oder per Direktlink.

„Arbeitszeit: Was geht und was geht nicht?“
Dienstag, 27. September 2022, 08:30 - 09:30 Uhr, Onlineveranstaltung

Anmeldungen **bis 26. September 2022** unter E-Mail: veranstaltungen@saarland.ihk.de oder per Direktlink.

„Arbeitszeugnis: Wer schreibt, bleibt!?“
Dienstag, 08. November 2022, 08:30 - 09:30 Uhr, Onlineveranstaltung

Anmeldungen **bis 07. November 2022** unter E-Mail: veranstaltungen@saarland.ihk.de oder per Direktlink.

„Der Subunternehmervertrag und seine Gestaltung“
Donnerstag, 02. Juni 2022, 16:00 - 17:30 Uhr, Onlineveranstaltung

In unserer arbeitsteiligen Welt werden viele Aufträge nicht durch ein Unternehmen allein ausgeführt, sondern es kommen Subunternehmen zum Einsatz. Bei der Beauftragung von Subunternehmen bestehen für den Hauptunternehmer erhebliche Haftungsrisiken hinsichtlich des Einsatzes von Mitarbeitern des Subunternehmers. Die Zahlung der Sozialversicherungsbeiträge, der Beiträge zur Berufsgenossenschaft, der Urlaubskassenbeiträge, des Mindestlohns und die korrekte Abführung der Steuer: Das alles unterfällt diesen Haftungsrisiken. Es ist deshalb entscheidend, dass der Subunternehmervertag korrekte und umfassende Regelungen enthält, die dieses Haftungsrisiko beschränken.

Hinzu kommen etwaige Haftungsrisiken, die entstehen können, wenn ein Bauherr das Unternehmen, das er beauftragt hat, auf Gewährleistung in Anspruch nimmt. Haftet dann auch der Subunternehmer?

Unsere Referenten, **Frau Rechtsanwältin Almut Menn, Fachanwältin für Bau- und Architektenrecht, Fachanwältin für Transport- und Speditionsrecht und Herr Rechtsanwalt Dr. Kai Hüther, Fachanwalt für Arbeitsrecht, Kanzlei Rapräger, Saarbrücken,** zeigen im Rahmen ihres Vortrags, was bei Abschluss eines Subunternehmervertrags zu beachten ist und welche sozialrechtlichen Besonderheiten für die eingesetzten Mitarbeiter des Subunternehmers gelten.

Anmeldungen **bis 01. Juni 2022** unter E-Mail: veranstaltungen@saarland.ihk.de oder per Direktlink.

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 Dr. Frank Thomé, 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-IdNr.: DE 138117020