

DATENSCHUTZ- BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Chefredakteur: Dr. Carlo Piltz

Schriftleitung: Dr. Alexander Golland, Adrian Schneider, Philipp Quiel, Tilman Herbrich

Datenschutz im Fokus

Öffnungsklauseln und Drittstaaten: Eine übersehene Lücke?

Fast alle Öffnungsklauseln der DSGVO gelten nur für die Union und Mitgliedsstaaten – ein grundlegender Konflikt für Verarbeitungen im Ausland.

Seite 24

Kaliforniens neues Datenschutzgesetz:

Der „California Consumer Privacy Act of 2018“ (CCPA)

Vom „right to know“ zum „right to say no“: Rechte von Verbrauchern, Pflichten von Unternehmern und Klagebefugnisse von Behörden im Golden State der USA.

Seite 26

Datenschutzrechtliche Anforderungen bei Online-Mitarbeiterbefragungen nach DSGVO und BDSG

Datenschutzrechtliche Aspekte bei der Durchführung von Online-Mitarbeiterbefragungen – was ist zu beachten?

Seite 28

Fragen aus der Praxis

„Privacy by Design“ – Vorgaben für Softwarehersteller im Datenschutzrecht?

Welche Bedeutung haben die Vorgaben aus Art. 25 Abs. 1 DSGVO für Softwarehersteller? Unter welchem Rechtsregime werden Haftungsfragen geklärt?

Seite 30

Aktuelles aus den Aufsichtsbehörden

Bereits 64 aus Deutschland stammende Bußgelder unter Anwendung der DSGVO

Eine Zusammenfassung der bisherigen Erkenntnisse zu den in Deutschland unter DSGVO erlassenen Bußgeldern – Bundesländer, Bußgeldhöhen und DSGVO-Verstöße.

Seite 31

CNIL Löschanordnung gegenüber französischem AdTech-Unternehmen

„Vectaury“

Seite 32

LDI NRW: Kommunikation per E-Mail bedarf mindestens der Transport-Verschlüsselung

Seite 33

Rechtsprechung

Einschränkbarkeit der Datenverarbeitung nach Art. 18 DSGVO: Die Pflichten des Betroffenen

Seite 34

Zulässigkeit einer Abmahnung nach dem UWG wegen Verstößen gegen die DSGVO

Seite 36

▪ Nachrichten Seite 22 ▪ Service Seite 40

Peter Hense, Celin Fischer

Kaliforniens neues Datenschutzgesetz: Der „California Consumer Privacy Act of 2018“ (CCPA)

In den USA gibt es bislang kein umfassendes Bundesgesetz zum Datenschutz. Lediglich Spezialvorschriften beispielsweise im „Children Online Privacy Protection Act“ (COPPA) oder im „Health Insurance Portability and Accountability Act“ (HIPPA) lassen Fragmente im Datenschutz erkennen. Damit liegen die USA mit ihrer Gesetzgebung hinter der Europäischen Union oder Technologiehubs wie Südkorea und Singapur, die jeweils über moderne und weitreichende Datenschutzbestimmungen verfügen. Das umfassendste US-amerikanische Datenschutzgesetz auf bundesstaatlicher Ebene war bislang der „California Online Privacy Protection Act of 2003“ (CalOPPA). Kalifornien ist seit langem führend bei der Regulierung des Datenschutzes in den Vereinigten Staaten; so räumte Kalifornien als erster US-Bundesstaat 1972 dem „Right to Privacy“ Verfassungsrang ein. Neben CalOPPA und anderen Spezialgesetzen tritt nunmehr ein im Juni 2018 verabschiedetes neues Datenschutzgesetz in Kraft: Der „California Consumer Privacy Act of 2018“ (CCPA). Da der Handel mit Waren und Dienstleistungen global ist, sollten auch europäische Unternehmen prüfen, inwieweit sie in den Anwendungsbereich des CCPA fallen und welche Pflichten ihnen daraus erwachsen.

Kaliforniens Antwort auf die DSGVO

Nach dem CalOPPA verabschiedet Kalifornien nun bereits das zweite umfassende Datenschutzgesetz. In dem bevölkerungsreichsten und wirtschaftsstärksten US-Bundesstaat herrschte auch in der Zwischenzeit alles andere als Stillstand: Man verfolgte vielmehr konsequent den Ansatz des Vorrangs spezialgesetzlicher Regelungen vor einer umfassenden Datenschutzregulierung wie in Europa. Weltweit beachtet wurde das sogenannte „Eraser Button Law“ (CA Senate Bill 568), welches seit dem Jahr 2015 Minderjährigen bei Erreichen der Volljährigkeit einen Lösch- bzw. Anonymisierungsanspruch für selbst eingegebene Daten auf Websites und Apps, z. B. in sozialen Netzwerken, gewährt.

Der neue CCPA hingegen hat einen durchaus breiten Geltungsanspruch. Regelte der CalOPPA bereits dem Namen nach nur Online-Sachverhalte, so wird durch den CCPA jegliche Datenverarbeitung von natürlichen Personen mit Wohnsitz in Kalifornien („Consumer“) betroffen sein. Entgegen dem Anschein des Gesetzstitels werden diese Menschen nicht nur als Verbraucher, sondern auch in ihrer Rolle z. B. als Arbeitnehmer, Mieter oder Patienten geschützt. Das neue Gesetz richtet sich an Wirtschaftsunternehmen, unabhängig davon, ob diese in Kalifornien niedergelassen sind oder nicht, d. h. auch Unternehmen aus Europa sind Normadressaten kalifornischen Datenschutzrechts, soweit und solange sie Daten von Kaliforniern verarbeiten. Aufgrund des komplizierten Gesetzgebungsverfahrens steht der finale Gesetzestext noch nicht fest, so dass auch noch einige Änderungen bis zum Inkrafttreten zu erwarten sind.

Welche Unternehmen sind betroffen?

Während es nach dem CalOPPA maßgeblich ist, dass eine kommerzielle Website personenbezogene Daten über Ka-

lifornier verarbeitet, fallen in den Anwendungsbereich des CCPA alle Unternehmen, die folgende drei Kriterien erfüllen: (1) ein Jahresumsatz von mindestens 25 Millionen US-Dollar (weltweit); (2) die Verarbeitung der Daten von mindestens 50.000 Kaliforniern; oder (3) wenn 50 % oder mehr der Erlöse mit der weit auszulegenden kommerziellen Verwertung von Daten erwirtschaftet werden. Um dem Territorialitätsprinzip Geltung zu verschaffen, sind Unternehmen ausgenommen, die personenbezogene Daten von Kaliforniern zwar erfassen, diese aber ausschließlich außerhalb Kaliforniens sammeln und die kommerzielle Verwertung dieser Daten auch nur außerhalb Kaliforniens erfolgt.

Neue Definition von „Personal Information“

Entsprechend der Taktvorgabe des reformierten europäischen Datenschutzrechts liegt auch dem CCPA ein neues, weitgehendes Verständnis von „Personal Information (PI)“ zugrunde. Der Begriff „Personal Information“ oder „Personally Identifiable Information (PII)“ wird in nahezu jedem US-Bundesstaat eigenständig definiert, was für Unternehmen erheblichen Abstimmungsaufwand verursacht. Als „Personal Information“ im Sinne des neuen CCPA gilt jedes Datum, das auf eine Person oder einen (nicht legaldefinierten) „Haushalt“ bezogen werden kann. Für US-Verhältnisse neu ist, dass neben Identifikatoren wie Sozialversicherungsnummern auch Aliase, IP-Adressen, Standortdaten, die Kaufhistorie, der Browserverlauf sowie Beschäftigungsdaten in den Schutzbereich fallen. Der technologisch-praktische Einfluss auf das Gesetzgebungsverfahren des CCPA zeigt sich auch darin, dass thermische und olfaktorische Daten explizit in den Schutzbereich einbezogen werden, was zumindest aus US-amerikanischer Sicht bemerkenswert ist. Damit setzt sich der CCPA von anderen US-bundesstaatlichen Gesetzen ab, die z. B. IP-Adressen

nicht *per se* als Personal Information ansehen. Angesichts aktueller europäischer Diskussionen um die Aufnahme von abgeleiteten Informationen und informationsbasierter Annahmen in den Schutzbereich der Definition von „personenbezogenen Daten“ unter der DSGVO ist die explizite Aufnahme von „inferences“ im CCPA als *Personal Information* ein bemerkenswerter Schritt, der zu Recht auf eine stärkere Kontrolle algorithmisch determinierter Entscheidungen abzielt.

Ausgewählte Rechte und Pflichten nach dem CCPA

Rechte der Verbraucher

Der CCPA listet in plakativer Sprache auf, worum es dem Gesetzgeber geht: Verbraucher sollen einen effektiven Weg erhalten, den Fluss ihrer *Personal Information* zu kontrollieren, indem sie unter anderem die folgenden Rechte erhalten: (1) Ein „*right to know*“ und damit ein Recht auf Information für Verbraucher, wer welche Daten über sie gespeichert hat sowie (2) das Recht zu wissen, ob diese Daten verkauft wurden und an wen, (3) ein „*right to say no*“, also ein Widerspruchsrecht gegen den Verkauf von Daten, (4) ein „*right to access*“, wonach Verbraucher Zugang zu ihren Daten gewährt werden muss, (5) ein „*right to erasure*“, also ein Recht auf Löschung von Daten, das jedoch durch berechnete Interessen von Unternehmen wie Vertragsdurchführung und Betrugsprävention begrenzt ist sowie (6) ein „*right to equal service and price*“, also ein Preisdiskriminierungs- und Vorenthaltungsverbot für den Fall, dass Verbraucher die obigen Rechte in Anspruch nehmen. Dieser Wunsch nach freier Ausübung der Rechte von Verbrauchern ist ein wesentliches Anliegen des Gesetzgebers und wird nach Ansicht von Beobachtern dazu führen, dass Unternehmen gezwungen sind, bisher kostenlose Dienste wie Social Media, Navigationsdienste und Messenger nun alternativ auch auf Bezahlbasis anzubieten.

Auffällig ist, dass Unternehmen von Minderjährigen (unter 16 Jahren) das Einverständnis einholen müssen, sofern deren Daten kommerziell durch Dritte verwertet werden sollen. Um die Ausübung dieses Rechts zu ermöglichen, fordert der CCPA von Websitebetreibern die Darstellung eines deutlichen und auffälligen Hyperlinks, der mit „*Do Not Sell My Personal Information*“ bezeichnet ist und der einen Opt-out-Mechanismus auslöst.

Keine neuen Hindernisse für den Datentransfer

Kalifornien hat sich gegen den protektionistischen Ansatz der Europäischen Union entschieden und erlegt seinen Unternehmen keine Beschränkungen zur Datenübermittlung außerhalb der USA auf. Es bleibt damit beim Grundsatz, dass eine Datenübermittlung aus Europa heraus z. B. über eine Zertifizierung nach Privacy Shield sowie gegebenenfalls über Standardvertragsklauseln abgesichert werden muss. In der entgegengesetzten Richtung jedoch sind

keine weiteren Sicherungsmaßnahmen erforderlich. Gleichfalls nicht erforderlich ist es, dass kalifornische Unternehmen einen spezifischen Datenschutzbeauftragten bestimmen, sofern sich eine Pflicht nicht aus anderen Gesetzen wie HIPPA ergibt. Dies ändert nichts daran, dass jede Unternehmensführung für die Einhaltung von Compliance-Vorgaben zu sorgen hat. Unternehmer sollen aber selbst entscheiden dürfen, auf welche Weise sie ihre Aufgaben erfüllen.

Sanktionen

Der CCPA sieht kein ausdrückliches Recht zur Klage von einzelnen Betroffenen bei Datenschutzverstößen vor. Damit liegt das Gesetz auf Linie mit weiteren aktuellen bundesstaatlichen Datenschutzgesetzen wie dem im Januar 2019 vorgestellten „*Washington Privacy Act*“. Auch die bundesstaatlichen Gesetzgeber in den USA haben die Befürchtung, dass ein allgemeines Klagerecht im Bereich des Datenschutzes aufgrund der Besonderheiten des US-Justizsystems zu einer Klagewelle und damit zu einer Lähmung von Gerichten und Unternehmen führt und damit der gewünschten Innovationskraft des Landes schadet. Allerdings ist der California Attorney General als Behörde berechtigt, Unternehmen auf dem Zivilrechtsweg wegen Verstöße gegen den CCPA auf Schadensersatz zu verklagen. Das Gesetz legt sogar Berechnungsgrößen fest, indem es jeweils bei Nichtabhilfe binnen 30 Tagen nach einer ersten Warnung bei vorsätzlichen Verstößen USD 7.500,00 und bei fahrlässigen Verstößen USD 2.500,00 als Sanktionen bestimmt. Diese Beträge wirken auf den ersten Blick wenig beeindruckend. Da aber im US-Recht der Begriff des einzelnen Verstoßes z. B. im Geltungsbereich von COPPA recht kleinteilig ausgelegt wird, können sich bei einer großen Menge an Nutzern oder einzelnen Datensätzen diese Beträge existenzbedrohend summieren.

Fazit und Ausblick

Der noch unfertige CCPA soll am 1. Januar 2020 in Kraft treten und gilt als Kaliforniens Antwort auf die DSGVO. Auch wenn die Betroffenenrechte der DSGVO und die Rechte der Verbraucher im Sinne des CCPA im Detail Unterschiede aufweisen, kann man davon ausgehen, dass sich der Handlungsbedarf für Unternehmen, die bereits die Vorgaben der DSGVO umgesetzt haben, in überschaubaren Grenzen hält.

Autoren: Peter Hense ist Rechtsanwalt und Partner bei SPIRIT LEGAL LLP Rechtsanwälte in Leipzig, Celin Fischer ist wissenschaftliche Mitarbeiterin ebenda.

