Ausgabe 4 August 2024

Revisionspraxis

PRev

Journal für Revision, IT-Sicherheit, SAP-Sicherheit und Datenschutz

www.prev.de

ISSN 1862-9032

BOORBERG

Inhalt

Datenschutz

Dr. Michael Foth

Liebe Leserinnen und Leser,

in seinem Beitrag „Datenschutz in Nordamerika“ untersucht Karsten Kinast die Entwicklung und den aktuellen Stand der Datenschutzgesetze in den USA, sowohl auf föderaler Ebene als auch auf Ebene der einzelnen Bundesstaaten. Zudem wird das neue EU-US Data Privacy Framework analysiert, das den Datenaustausch zwischen der EU und den USA regelt. Besondere Aufmerksamkeit wird dabei den Herausforderungen und Unterschieden im Vergleich zur Datenschutz-Grundverordnung der EU gewidmet.

Thomas Kolb und Stephania Loukanova behandeln in Ihrem Beitrag „Zwischen Innovation und Privatsphäre: Die Regulierung von KI unter der DSGVO“ die Einführung und Integration von Künstlicher Intelligenz in zahlreiche Lebens- und Wirtschaftsbereiche und die damit einhergehenden Bedenken hinsichtlich des Datenschutzes und der Privatsphäre der Nutzer.

In einer zunehmend u. a. durch KI beschleunigten digitalisierten Welt steigen auch die Risiken betr. Datenschutz und Datensicherheit. Während der Datenschutzbeauftragte die Einhaltung der Datenschutzvorschriften sicherstellt, konzentriert sich der KI-Beauftragte auf die Überwachung und Steuerung des Einsatzes und der Verwendung von Künstlicher Intelligenz innerhalb eines Unternehmens. Beide Rollen sind essenziell, um Vertrauen und Sicherheit in der modernen Technologieumgebung zu gewährleisten. Mara-Lia Schilling geht in ihrem Beitrag „DS-Beauftragter und KI-Beauftragter: Was ist der Unterschied?“ näher darauf ein.

Viel Spaß und neue Erkenntnisse wünscht Ihnen

Ihr
Dr. Michael Foth

Karsten Kinast

Datenschutz in Nordamerika: Ein Blick auf die USA auf föderaler und Bundesstaatenebene sowie das Privacy Framework

A. Einleitung

Der Datenschutz hat in den letzten Jahren enorm an Bedeutung gewonnen, da die Digitalisierung und damit der Umfang und die Intensität der Nutzung personenbezogener Daten in nahezu allen Lebensbereichen voranschreiten. Von sozialen Medien über Online-Shopping bis hin zu digitalen Gesundheitsakten – persönliche Daten werden in einem Ausmaß gesammelt, gespeichert und verarbeitet, das noch vor wenigen Jahrzehnten undenkbar gewesen wäre. Diese Entwicklung hat jedoch auch neue Risiken und Herausforderungen mit sich gebracht, darunter Datenschutzverletzungen, Identitätsdiebstahl und Missbrauch von personenbezogenen Daten zu kommerziellen oder politischen Zwecken.

In einer Zeit, in der Daten als die „Währung" des digitalen Zeitalters betrachtet werden, ist der Schutz dieser Daten von entscheidender Bedeutung, um die Privatsphäre und die Grundrechte der Bürger und letztlich auch die Rechtsstaatlichkeit als Kernbestandteil der Demokratie zu wahren. Datenschutzgesetze und -vorschriften spielen eine zentrale Rolle bei der Sicherstellung eines angemessenen Schutzes personenbezogener Daten und bei der Regulierung des Umgangs mit diesen Daten durch Regierungen, Unternehmen und sonstige Organisationen. Dabei wird teilweise die DSGVO der EU als Vorreiter für die Schaffung von Datenschutzgesetzen in anderen Staaten gesehen. Im ersten Beitrag dieser Reihe[1] analysieren wir diese sogenannte globale Vorbildfunktion der DSGVO.

1 *Kinast*, PRev, 2024, 30 ff.

Der Datenaustausch zwischen der EU bzw. dem EWR und den USA war in jüngster Zeit aufgrund unterschiedlicher Voraussetzungen häufig problematisch. Der Europäische Gerichtshof (EuGH) hatte das ursprünglich geltende Datenschutzabkommen „Privacy Shield" zwischen der EU und den USA mit der Begründung gekippt, dass das Datenschutzniveau in den USA nicht den europäischen Standards entspreche.[2] Die Richter bemängelten vor allem die weitreichenden Zugriffsmöglichkeiten von US-Behörden auf personenbezogene Daten von Europäern.[3] Die EU-Kommission hat inzwischen einen neuen Angemessenheitsbeschluss für den Datenschutzrahmen EU-USA (engl. EU-US Data Privacy Framework)[4] erlassen. Dieser legt fest, dass die Vereinigten Staaten ein angemessenes Schutzniveau – vergleichbar mit dem der Europäischen Union – für personenbezogene Daten gewährleisten, die innerhalb des neuen Rahmens aus der EU an Empfänger in den USA übermittelt werden.[5] Es ist jedoch ungewiss, ob der Beschluss den strengen Anforderungen des EuGH standhalten wird.[6] Bei der Einschätzung, ob ein gleichwertiges Datenschutzniveau vorliegt, werden zukünftig auch die datenschutzrechtlichen Regime der einzelnen Bundesstaaten sowie das des Bundes eine Rolle spielen.

Gerade vor dem Hintergrund der Fluten an personenbezogenen Daten, die mit den USA ausgetauscht werden, ist die Schaffung eines sicheren Rechtsrahmens dringender denn je. Das wird umso deutlicher, wenn man beachtet, dass der Großteil der Softwareunternehmen im Cloud- und Textverarbeitungsbereich seinen Sitz in den USA hat und Europa insofern mangels eigener europäischer Player abhängig ist. Angesichts dieser Herausforderungen ist es unerlässlich, die US-amerikanische Datenschutzgesetzgebung zu verstehen. Deshalb widmet sich dieser Beitrag dem aktuellen Stand der Datenschutzregulierung in den USA.

B. Transatlantische Datenschutzperspektiven: Historische Entwicklungen und aktuelle Divergenzen

Der Unterschied in der Herangehensweise an den Datenschutz zwischen der EU und den USA hat seinen Ursprung in einer anderen Sichtweise. Während in Europa der Schutz personenbezogener Daten als Grundrecht betrachtet wird, gilt Datenschutz in den USA eher als Teil des Verbraucherschutzrechts und als Element des Wirtschaftslebens. Diese Differenz resultiert aus der unterschiedlichen historischen Entwicklung auf beiden Seiten des Atlantiks.

Das Verlangen nach Privatheit und Datenschutz wurzelt tief in der menschlichen Natur und reicht bis in vergangene Epochen zurück. Mit dem Aufkommen des modernen Staates und technologischer Fortschritte im 19. Jahrhundert geriet die Privatsphäre jedoch zunehmend in Gefahr. In Europa begann bereits im 16. Jahrhundert eine Debatte über den individuellen informationellen Schutz, während in den USA bahnbrechende Aufsätze wie das „Right to Privacy" von Warren und Brandeis im Jahr 1890 die Diskussion vorantrieben.[7] Hierbei wurde insbesondere – ganz dem US-amerikanischen Liberalismus entsprechend – ein „right to be left alone" verstanden, also ein Recht frei von Einflüssen Dritter zu bleiben. Damals betraf dies vorrangig die Veröffentlichung von Informationen durch die Presse.

In der Datenschutzdebatte werden die Unterschiede zwischen Europa und den USA oft mit einem würdebasierten Ansatz in Europa und einem freiheitsbasierten Ansatz in den USA erklärt.[8] Während in Europa die Menschenwürde und das Recht auf informationelle Selbstbestimmung im Vordergrund stehen, betont man in den USA eher die individuelle Freiheit und die Möglichkeit zur Verfügungsgewalt über persönliche Daten. Diese Differenz ist heute besonders relevant, da sie sich in der Struktur des Internetdienstleistungsmarktes widerspiegelt. In den USA begünstigt ein flexiblerer Datenschutzansatz die dort ansässigen Anbieter, während in Europa ein stärkerer Fokus auf dem Schutz der betroffenen Personen liegt. Trotz dieser Unterschiede teilen Europa und die USA das gemeinsame Verständnis, dass Datenschutz vom Individuum her gedacht ist. Dies wird besonders wichtig sein, wenn man sich mit den Datenschutzvorstellungen in aufstrebenden digitalen Wirtschaftszentren wie Asien und Afrika auseinandersetzt, wo eher kollektive als individuelle Ansätze dominieren.

Im Laufe der Zeit spalteten sich die Datenschutzkonzepte in der westlichen Welt: Während die USA einen sektoriellen Ansatz verfolgten, setzte Europa auf ein umfassendes Regelungsmodell, das Unternehmen in den Fokus nahm.[9] Diese unterschiedlichen Ansätze

2 Glocker: Der neue Angemessenheitsbeschluss zum EU–U.S. Data Privacy Framework (RDi 2023, 466)

3 Glocker: Der neue Angemessenheitsbeschluss zum EU–U.S. Data Privacy Framework (RDi 2023, 466)

4 EU-US Data Privacy Framework, abrufbar unter https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcbofddf, zuletzt geöffnet am 10. Juni 2024

5 Glocker: Der neue Angemessenheitsbeschluss zum EU–U.S. Data Privacy Framework (RDi 2023, 465)

6 Glocker: EU-US Data Privacy Framework: Update des Privacy Shield mit Augenmaß (ZD 2023, 193)

7 Warren/Brandeis: The Right to Privacy, Harvard Law Review, Vol. IV, Dec 15, 1890 No. 5

8 Determann: Datenschutz in den USA – Dichtung und Wahrheit(NVwZ 2016, 564)

9 Determann: Datenschutz in den USA – Dichtung und Wahrheit(NVwZ 2016, 564)

prägen bis heute die Datenschutzregelungen auf beiden Seiten des Atlantiks.

In den folgenden Abschnitten werden wir uns eingehend mit den verschiedenen Aspekten der Datenschutzgesetzgebung in Nordamerika befassen und dabei wichtige Erkenntnisse und Einsichten liefern, die für eine fundierte Diskussion über dieses Thema unerlässlich sind.

C. Datenschutzregime in den USA

I. Die facettenreiche Datenschutzlandschaft der USA: Zwischen Fragmentierung und Sensibilisierung

Die Datenschutzlandschaft in den USA ist geprägt von einer Vielzahl unterschiedlicher Gesetze, Regelungen und Bestimmungen auf föderaler, Bundesstaaten- und Provinzebene. Während einige Länder wie Kanada bereits seit langem umfassende Datenschutzgesetze haben, sind andere wie die USA eher durch eine fragmentierte und sektorale Regulierung gekennzeichnet. Dennoch gibt es in den letzten Jahren eine zunehmende Sensibilisierung für Datenschutzfragen und eine wachsende Anzahl von Initiativen zur Stärkung des Datenschutzes in der Region.

II. Föderale Gesetzgebung

In den USA gibt es auf föderaler Ebene bisher noch keine umfassende Datenschutzgesetzgebung, die alle Bereiche des Datenschutzes abdeckt.[10] Stattdessen sind föderal bislang lediglich verschiedene sektorale Gesetze und Regelungen in Kraft, die den Datenschutz in bestimmten Branchen oder für bestimmte Arten von persönlichen Daten regeln. Dazu gehören Gesetze wie der Health Insurance Portability and Accountability Act (HIPAA) im Gesundheitswesen, der Gramm-Leach-Bliley Act (GLBA) im Finanzsektor und der Children's Online Privacy Protection Act (COPPA) zum Schutz der Privatsphäre von Kindern im Internet.

III. Bundesstaatliche Gesetzgebung

Da es auf föderaler Ebene bisher wie erwähnt keine einheitliche Datenschutzgesetzgebung gibt, haben viele Bundesstaaten in den USA eigene Datenschutzgesetze verabschiedet, um einen Schutz personenbezogener Daten zu etablieren. Diese Gesetze variieren je nach Bundesstaat in ihrem Umfang und ihren konkreten Bestimmungen, ähneln sich jedoch strukturell hinsichtlich Regelungen zur Datenverarbeitung, Datensicherheit, Datenübermittlung und Benachrichtigung im Falle von Datenschutzverletzungen.

Insgesamt zeigt die Datenschutzgesetzgebung auf Bundesstaatenebene in den USA eine zunehmende Tendenz zur Stärkung des Datenschutzes und zur Gewährleistung eines angemessenen Schutzes personenbezogener Daten. Dennoch bleibt die fragmentierte Natur der Regulierung eine Herausforderung, da Unternehmen, die in mehreren Bundesstaaten tätig sind, möglicherweise unterschiedlichen Datenschutzvorschriften unterliegen.

1. Kalifornien

Ein bemerkenswertes Beispiel ist der California Consumer Privacy Act (CCPA), der als eines der strengsten Datenschutzgesetze in den USA gilt.[11] Der CCPA gewährt den Verbrauchern umfassende Rechte in Bezug auf ihre persönlichen Daten, einschließlich des Rechts auf Zugang, Löschung und Einspruch gegen die Weitergabe ihrer Daten an Dritte.[12] Darüber hinaus verpflichtet der CCPA Unternehmen, transparent über ihre Datenschutzpraktiken zu informieren und angemessene Sicherheitsmaßnahmen zum Schutz personenbezogener Daten zu ergreifen.

2. Virginia

Der Virginia Consumer Data Protection Act (VCDPA) ist ein Gesetz des Staates Virginia, das am 1. Januar 2023 in Kraft getreten ist und das Recht der Verbraucher auf Datenschutz und Datensicherheit in Virginia stärkt. Viele der VCDPA-Rechte, die Virginia-Verbrauchern gewährt werden, ähneln den Rechten, die die DSGVO bietet, einschließlich der Verbraucherrechte wie die Rechte auf Zugriff, Löschung und Portabilität personenbezogener Daten.

a. Welche Auswirkungen hat das VCDPA auf die Verantwortlichen?

Das Gesetz fordert von Unternehmen, die personenbezogene Daten von Einwohnern Virginias verarbeiten, verschiedene Schutzmaßnahmen zu ergreifen. Dazu gehört unter anderem die Einhaltung von Datensicherheitsstandards, die Durchführung von Datenschutz-Audits, sowie die Benachrichtigung von Verbrauchern im Falle eines Datenverlusts oder eines Datenschutzverstoßes.[13]

10 Zurzeit liegt einem Ausschuss des Repräsentantenhauses der Entwurf des American Privacy Rights Act (APRA) als neues föderales Datenschutzgesetz vor, abrufbar unter https://d1dth6e84htgma.cloudfront.net/PRIVACY_04_xml_d1d6b82f10.pdf, zuletzt geöffnet am 12. Juni.2024.

11 Halim/Klee: Aktuelle Entwicklungen in den USA – Risiken der Datenschutz Compliance bei M&A-Transaktionen nach dem neuen CPRA und der DSGVO CCZ 2021, 300.

12 Halim/Klee: Aktuelle Entwicklungen in den USA – Risiken der Datenschutz Compliance bei M&A-Transaktionen nach dem neuen CPRA und der DSGVO CCZ 2021, 300.

13 Spies: USA: Neues Datenschutzgesetz im US-Staat Virginia ZD-Aktuell 2021, 05047

Ein zentraler Bestandteil des VCDPA ist das Recht der Verbraucher, ihre personenbezogenen Daten einzusehen, zu ändern oder zu löschen. Unternehmen müssen solche Anfragen innerhalb von 45 Tagen bearbeiten und dürfen hierfür keine Gebühren erheben.[14]

Darüber hinaus müssen Unternehmen, die dem Gesetz unterliegen, vor der Erhebung und Verarbeitung bestimmter sensibler personenbezogener Daten eine Einwilligung der Verbraucher einholen.[15] Ähnlich wie der kalifornische CCPA (California Consumer Privacy Act) schreibt auch der VCDPA vor, dass Unternehmen, die Dienstleister mit der Datenverarbeitung beauftragen, spezielle Verträge abschließen müssen, um die gesetzlichen Anforderungen zu erfüllen.[16]

b. Weitere Vorgaben umfassen (nicht abschließend):

- Zweckbindung
- Datenschutz-Risikobewertungen
- Schaffung technischer und organisatorischer Sicherheitsmaßnahmen
- Dokumentationspflichten
- Widerspruchsverfahren für Verbraucheranträge
- Schutz vor Diskriminierung
- Datenschutzerklärungen

c. Das VCDPA gilt für Unternehmen, die:

- Geschäfte in Virginia tätigen oder ihre Waren und Dienstleistungen an Einwohner von Virginia vermarkten; und
- Entweder: die personenbezogenen Daten von mindestens 100.000 Einwohnern Virginias kontrollieren oder verarbeiten; oder die personenbezogenen Daten von mindestens 25.000 Einwohnern Virginias kontrollieren oder verarbeiten und mehr als 50 % ihrer Bruttoeinnahmen aus dem Verkauf von personenbezogenen Daten erzielen.

d. Bestimmte Organisationen sind vom VCDPA ausgenommen, einschließlich:

- Behörden des Bundesstaats Virginia
- Finanzinstitute, die dem Gramm-Leach-Bliley Act unterliegen
- Erfasste Unternehmen oder Geschäftspartner, die den Datenschutz-, Sicherheits- und Verletzungsbenachrichtigungsregeln unterliegen, die gemäß dem Health Insurance Portability and Accountability Act festgelegt wurden
- Gemeinnützige Organisationen; und Hochschuleinrichtungen

e. Was schützt das Gesetz?

- Das Recht auf Kenntnis, Zugang und Bestätigung der personenbezogenen Daten
- Das Recht auf Löschung personenbezogener Daten
- Das Recht auf Berichtigung unrichtiger personenbezogener Daten
- Das Recht auf Datenübertragbarkeit (d. h. einfacher, übertragbarer Zugang zu allen personenbezogenen Daten, die sich im Besitz eines Unternehmens befinden)
- Das Recht, der Verarbeitung personenbezogener Daten für gezielte Werbezwecke zu widersprechen
- Das Recht, dem Verkauf von personenbezogenen Daten zu widersprechen
- Das Recht, der Erstellung von Profilen auf der Grundlage personenbezogener Daten zu widersprechen
- Das Recht, wegen der Ausübung eines der vorgenannten Rechte nicht diskriminiert zu werden

Ein weiteres wichtiges Element des VCDPA ist die Schaffung einer Datenschutzbehörde, die für die Überwachung der Einhaltung des Gesetzes zuständig ist und Strafen für Verstöße verhängen kann.[17]

Das VCDPA wird vom Generalstaatsanwalt von Virginia durchgesetzt und sieht eine 30-tägige Nachbesserungsfrist vor.[18] Bei Nichteinhaltung kann jedoch eine zivilrechtliche Strafe von bis zu 7.500 US-Dollar pro Verstoß verhängt werden.[19]

3. Iowa

Nach Connecticut, Utah, Virginia, Colorado und Kalifornien war Iowa am 28. März 2023 der sechste Staat, der ein umfassendes Datenschutzgesetz verabschiedete. Das Gesetz wird am 1. Januar 2025 in Kraft treten, so dass Organisationen 21 Monate Zeit haben, die neuen Anforderungen zu erfüllen. Obwohl das Gesetz einige Ähnlichkeiten mit anderen staatlichen Datenschutzgesetzen aufweist, sollten Unternehmen auf die Unterschiede achten, wenn sie ihre Compliance-Bemühungen in den Vereinigten Staaten ausweiten.

Der Iowa Data Privacy Act (IDPA) gilt für Unternehmen, die in Iowa tätig sind oder sich mit ihren Produkten oder Dienstleistungen an Verbraucher in Iowa wenden und personenbezogene Daten von 100.000 oder mehr Verbrauchern in Iowa oder 25.000 oder

14 Spies: USA: Neues Datenschutzgesetz im US-Staat Virginia ZD-Aktuell 2021, 05047

15 Spies: USA: Neues Datenschutzgesetz im US-Staat Virginia ZD-Aktuell 2021, 05047

16 Spies: USA: Neues Datenschutzgesetz im US-Staat Virginia ZD-Aktuell 2021, 05047

17 Spies: USA: Neues Datenschutzgesetz im US-Staat Virginia ZD-Aktuell 2021, 05047

18 Spies: USA: Neues Datenschutzgesetz im US-Staat Virginia ZD-Aktuell 2021, 05047

19 Spies: USA: Neues Datenschutzgesetz im US-Staat Virginia ZD-Aktuell 2021, 05047

mehr Verbrauchern in Iowa kontrollieren oder verarbeiten und gleichzeitig mehr als 50 % ihrer Bruttoeinnahmen aus dem Verkauf dieser Daten erzielen. Die IDPA-Definition des Begriffs „Verbraucher" umfasst natürliche Personen mit Wohnsitz in Iowa, die in einem persönlichen (nichtkommerziellen und nichtbeschäftigten) Kontext handeln, und schließt Mitarbeiter und B2B-Kontakte aus.

Der IDPA erlegt den für die Datenverarbeitung Verantwortlichen Verpflichtungen auf. Dazu gehören beispielsweise die Beschränkung des Zwecks der Verarbeitung personenbezogener Daten, die Einführung angemessener Schutzmaßnahmen, den Verzicht auf Diskriminierung, transparente Datenschutzhinweise und die Sicherstellung, dass die Beziehungen zu den Auftragsverarbeitern vertraglich geregelt sind. Darüber hinaus erteilt es den Verbrauchern in Iowa das Recht auf Ablehnung, Löschung, Zugang, Widerspruch und Datenübertragbarkeit.

Zu den sensiblen personenbezogenen Daten gehören u. a. die rassische/ethnische Herkunft, religiöse Überzeugungen und Geolokalisierungsdaten. Die für die Verarbeitung Verantwortlichen müssen deutlich auf die Verarbeitung dieser Daten hinweisen und die Möglichkeit bieten, sich gegen eine Verarbeitung zu entscheiden. Der Generalstaatsanwalt von Iowa hat die ausschließliche Durchsetzungsbefugnis, und das Gesetz sieht kein privates Klagerecht vor.

4. Indiana

Mit der Unterzeichnung der Senate Bill No. 5 durch Gouverneur Eric Holcomb im Jahr 2023 wurde Indiana der siebte Staat, der ein umfassendes Datenschutzgesetz verabschiedet hat. Das Gesetz tritt am 1. Januar 2026 in Kraft. Es ähnelt anderen staatlichen Datenschutzgesetzen wie dem Virginia Consumer Data Protection Act.

Das Datenschutzgesetz von Indiana gilt für Organisationen, die personenbezogene Daten von mindestens 100.000 Einwohnern von Indiana oder 25.000 Einwohnern von Indiana verarbeiten und gleichzeitig mehr als 50 % ihrer Bruttoeinnahmen aus dem Verkauf personenbezogener Daten erzielen. Bestimmte Einrichtungen und Daten sind von dem Gesetz ausgenommen.

Das Gesetz verpflichtet die Unternehmen, den Verbrauchern klare und aussagekräftige Datenschutzhinweise zur Verfügung zu stellen und räumt den Verbrauchern ein Recht ein, ihre personenbezogenen Daten zu bestätigen, auf sie zuzugreifen, sie zu korrigieren, zu löschen und zu übertragen. Darüber hinaus können Verbraucher auch der Verarbeitung ihrer personenbezogenen Daten für gezielte Werbung, den Verkauf personenbezogener Daten oder die Profilerstellung, die erhebliche Auswirkungen hat, widersprechen.

Es gibt kein privates Klagerecht, und Unternehmen haben eine 30-tägige Frist zur Behebung angeblicher Verstöße.

5. Montana

Nachdem der Montana Consumer Data Privacy Act (MCDPA) beide Häuser der Legislative von Montana bereits passiert hat, fehlt nun lediglich noch die Unterschrift von Gouverneur Greg Gianforte. Der MCDPA ähnelt den Gesetzen in Connecticut und Virginia, was darauf hindeutet, dass diese Modelle zunehmend die Grundlage für andere staatliche Datenschutzgesetze darstellen.

Das Gesetz gilt für Unternehmen, die in Montana geschäftlich tätig sind, personenbezogene Daten von 50.000 oder mehr Verbrauchern in Montana oder von 25.000 oder mehr Verbrauchern in Montana kontrollieren oder verarbeiten und gleichzeitig mehr als 25 % ihrer Bruttoeinnahmen aus dem Verkauf dieser Daten erwirtschaften.

„Verbraucher" ist definiert als eine natürliche Person mit Wohnsitz in Montana, die in einem persönlichen Kontext handelt. Personenbezogene Daten werden als Informationen definiert, die mit einer identifizierten oder identifizierbaren Person verknüpft sind oder vernünftigerweise verknüpft werden können. Zu den sensiblen Daten gehören Informationen über die Rasse/ethnische Herkunft, die Religion, die Gesundheitsdiagnose, das Sexualleben, die sexuelle Orientierung, die Staatsbürgerschaft, den Einwanderungsstatus und genetische oder biometrische Informationen einer Person. Betroffene Unternehmen müssen den Verbrauchern eine Reihe von Standardrechten zugestehen, darunter das Recht auf Ablehnung des Verkaufs personenbezogener Daten, das Recht auf Löschung, Zugang, Berichtigung und Widerspruch, das Recht auf Einwilligung in Werbung und gezieltes Marketing für Personen zwischen 13 und 16 Jahren sowie das Recht auf Datenübertragbarkeit.

Sensible Daten dürfen nicht verarbeitet werden, ohne dass die Zustimmung des Verbrauchers eingeholt wurde oder, im Falle von Kindern, die COPPA-Bestimmungen eingehalten wurden.

Des Weiteren verpflichtet der MCDPA die für die Verarbeitung Verantwortlichen, den Zweck der Verarbeitung personenbezogener Daten auf das vernünftigerweise notwendige und verhältnismäßige Maß zu beschränken, Maßnahmen zu ergreifen, um angemessene Sicherheitsvorkehrungen für die von ihnen kontrollierten personenbezogenen Daten zu treffen, Verbraucher nicht zu diskriminieren, wenn sie ihre Rechte wahr-

nehmen, und in ihren Datenschutzhinweisen transparent zu sein. Der Generalstaatsanwalt von Montana hat die ausschließliche Durchsetzungsbefugnis, und es gibt kein privates Klagerecht.

6. Tennessee

Sobald Gouverneur Bill Lee zustimmt, wird sich Tennessee mit der Einführung des Tennessee Information Privacy Act (TIPA) bald den Staaten mit umfassenden Datenschutzgesetzen anschließen. Das TIPA folgt weitgehend dem Modell des kalifornischen CCPA, allerdings mit einer Ausnahme: Er gilt für Unternehmen, die in Tennessee tätig sind oder Produkte oder Dienstleistungen für Einwohner von Tennessee anbieten und personenbezogene Daten von mindestens 100.000 Verbrauchern oder 25.000 Verbrauchern verarbeiten und gleichzeitig mehr als 50 % ihrer Bruttoeinnahmen aus dem Verkauf von personenbezogenen Daten erzielen.

7. Vermont

Am 10. Mai 2024 hat der Gesetzgeber in Vermont eine umfassende Datenschutzgesetzgebung verabschiedet. Nun fehlt nur noch die Unterschrift des Gouverneurs. Dieses Gesetz umfasst den Vermont Data Privacy Act (VDPA), den Vermont Data Broker Security Breach Notice Act und den Vermont Age-Appropriate Design Code. Für Verbraucher bedeutet das, dass sie bei bestimmten Datenschutzverletzungen Klage erheben können.

Das Gesetz gilt für Unternehmer und Unternehmen, die in Vermont ihre Tätigkeit ausführen oder Produkte oder Dienstleistungen dort anbieten. Das Gesetz wird in verschiedenen Stufen je nach Unternehmensgröße angewendet. Unternehmen, die im vorangegangenen Kalenderjahr personenbezogene Daten von mindestens 25.000 Verbrauchern verarbeitet haben (ausgenommen sind Daten, die ausschließlich für Zahlungstransaktionen verarbeitet wurden) oder Daten von mindestens 12.500 Verbrauchern verarbeitet haben und mehr als 25 % ihres Umsatzes aus dem Verkauf dieser Daten erzielt haben, unterliegen dem VDPA bereits ab dem 1. Juli 2024. Diese Schwellenwerte werden schrittweise zum 1. Juli 2026 und 1. Juli 2027 halbiert, sowohl in Bezug auf die Anzahl der Verbraucher als auch auf den Umsatz (auf 20 %).

Der VDPA verlangt von Datenverarbeitern angemessene Sicherheitsstandards, Datenschutz-Folgenabschätzungen, die Einholung einer Einwilligung zur Verarbeitung sensibler Daten, Datensparsamkeit und detaillierte Datenschutzhinweise. In den Datenschutzhinweisen ist besonders ausführlich auf Dritte einzugehen, an die personenbezogene Daten weitergegeben werden. Datenverarbeiter müssen auch effektive Widerrufsmechanismen einführen und diese innerhalb von 15 Tagen umsetzen. Der Verkauf sensibler Daten ist unzulässig. Für Gesundheitsdaten gibt es verschiedene Weitergabebeschränkungen. Außerdem müssen Verantwortliche für Gesundheitsdaten virtuelle Schutzmaßnahmen einführen, um den rechtswidrigen Zugriff durch Dritte zu verhindern. Der Age-Appropriate Design Code schafft für Minderjährige spezielle Sicherheitsvorkehrungen, die den Grundsatz „Privacy by Design“ umsetzen.

Der VDPA gewährt Verbrauchern verschiedene Betroffenenrechte, einschließlich des Rechts auf Auskunft darüber, an welche Dritten personenbezogene Daten weitergegeben wurden. Datenverarbeiter müssen auf Anfragen von Betroffenen innerhalb von 45 Tagen antworten, wobei eine Verlängerung um weitere 45 Tage in Ausnahmefällen möglich ist.

Zuständig für die Durchsetzung des VDPA ist der Generalstaatsanwalt von Vermont. Ab dem 1. Januar 2027 bis zum 1. Januar 2029 können auch Verbraucher bei bestimmten Datenschutzverletzungen Klage erheben. Dies gilt für Fälle, in denen sensible Daten ohne Einwilligung verarbeitet wurden, für den Verkauf sensibler Daten oder für Verletzungen der Vorschriften zur Vertraulichkeit von Gesundheitsdaten.

D. EU-US Data Privacy Framework

Am 10. Juli 2023 hat die EU-Kommission eine neue Entscheidung getroffen, um den sicheren Datenverkehr zwischen der EU und den USA zu gewährleisten. Mit dem Trans-Atlantic-Data-Privacy-Framework (TADPF) wird nun der dritte Versuch unternommen, nach “Safe Harbor” und „Privacy Shield“ transatlantische Datentransfers möglichst unkompliziert zu gestalten. Mit dieser Vereinbarung können nun Daten von Unternehmen wie Google, Microsoft, Meta, AWS und anderen sicher von der EU in die USA übermittelt werden.[20]

Der Hintergrund des TADPF liegt in der Unwirksamkeit der vorherigen Regelungen Safe-Harbour und Privacy-Shield, die vom Europäischen Gerichtshof (EuGH) 2015 bzw. 2020 für ungültig erklärt wurden.[21] Seit dem 10. Juli 2023 gilt nun der lang erwartete neue Angemessenheitsbeschluss gemäß der Datenschutzgrundverordnung (DSGVO) zwischen der EU und den USA. Dieser Beschluss wurde getroffen, um eine sichere Übermittlung von Daten zwischen der EU und den USA zu gewährleisten. Das Trans-Atlantic Data Privacy

20 Hessel: Der neue Angemessenheitsbeschluss für Datenübermittlungen in die USA NJW 2023, 2969

21 Glocker: EU-US Data Privacy Framework: Update des Privacy Shield mit Augenmaß ZD 2023, 189

Framework ist ein Abkommen, das zwischen den 27 Mitgliedsstaaten der Europäischen Union und den Vereinigten Staaten geschlossen wurde.

I. Das Data Privacy Framework

Das TADPF ist ein Angemessenheitsbeschluss gemäß Art. 45 Abs. 1 DSGVO. Gemäß diesem Beschluss gelten die USA erneut als sicherer Drittstaat im Hinblick auf den Datenschutz. Daher sind für Datenexporte an Empfänger in den USA keine zusätzlichen Legitimationsinstrumente mehr erforderlich.[22] Allerdings hat das TADPF im Vergleich zu anderen Angemessenheitsbeschlüssen nur begrenzte Wirkung. Ähnlich wie beim vorherigen Privacy Shield gilt die privilegierte Wirkung des TADPF nur für Datenempfänger, die sich einem Selbstzertifizierungsmechanismus unterziehen und sich verpflichten, eine Reihe detaillierter Datenschutzverpflichtungen einzuhalten. Unternehmen, die gemäß den Kriterien des TADPF zertifiziert sind, werden voraussichtlich auf der Website www.dataprivacyframework.gov aufgeführt sein.

II. Was ist ein Angemessenheitsbeschluss?

Ein Angemessenheitsbeschluss gemäß der DSGVO, speziell Art. 45 Abs. 3 DSGVO, ist im Grunde genommen eine Entscheidung der Europäischen Kommission, die besagt, dass ein Drittland (ein Land außerhalb der EU/EWR) ein angemessenes Schutzniveau für personenbezogene Daten bietet. Dieser Beschluss bestätigt, dass das betreffende Drittland Datenschutzstandards eingeführt hat, die mit den Standards der EU vergleichbar sind und den Schutz personenbezogener Daten in ähnlicher Weise gewährleisten. Infolgedessen dürfen personenbezogene Daten ohne zusätzliche Schutzmaßnahmen in dieses Drittland übertragen werden.

Safe Harbour und Privacy Shield waren ebenfalls solche Angemessenheitsbeschlüsse. Wie bekannt, wurden beide von dem Europäischen Gerichtshof (EuGH) für ungültig erklärt. Einer der Hauptgründe dafür war, dass die USA faktisch kein Datenschutzniveau bieten konnten, das mit dem EU-Standard vergleichbar war. Insbesondere die nahezu uneingeschränkte Zugriffsmöglichkeit der US-Behörden, insbesondere der National Security Agency (NSA), auf personenbezogene Daten von EU-Bürgern spielte dabei eine Rolle. Dies galt sogar dann, wenn Unternehmen ihren Sitz in den USA hatten, aber ihre Dienstleistungen in der EU erbrachten.

III. Hintergrund: Executive Order vom 07. Oktober 2022

Um die Zugriffsmöglichkeiten der NSA auf personenbezogene Daten von EU-Bürgern einzuschränken, unterzeichnete US-Präsident Biden bereits am 07. Oktober 2022 die „Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities“. Diese Maßnahme sollte sicherstellen, dass zumindest der Grundsatz der Verhältnismäßigkeit gewahrt bleibt. Vor jedem Zugriff auf Daten von EU-Bürgern müssen die US-Geheimdienste nun überprüfen, ob der Zugriff auf die Daten verhältnismäßig ist. Darüber hinaus wurde ein Beschwerdeverfahren für EU-Bürger in den USA eingerichtet. EU-Bürger können sich daher beim Civil Liberties Protection Officer der US-Geheimdienste beschweren. Sollte eine solche Beschwerde nicht erfolgreich sein, haben EU-Bürger die Möglichkeit, vor einem neu geschaffenen Gericht, dem Civil Liberties Protection Officer, Klage zu erheben.

Diese Executive Order hat im Wesentlichen dazu geführt, dass die EU das TADPF beschlossen hat.

IV. Sichere Datenübermittlung zwischen EU und USA wieder möglich?

Solange der Europäische Gerichtshof (EuGH) das TADPF nicht erneut für ungültig erklärt, können sich EU-Unternehmen darauf verlassen, dass Unternehmen, die gemäß dem TADPF zertifiziert sind, die Datenschutzstandards einhalten. Im Gegensatz zu den Standardvertragsklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO, die vor der Einführung des TADPF hauptsächlich als Rechtsgrundlage für die Übermittlung personenbezogener Daten zwischen der EU und den USA verwendet wurden, entfällt beim TADPF die verpflichtende eigene Prüfung des Standards bei den jeweiligen US-Unternehmen.

E. Der American Privacy Rights Act

In den USA gibt es einen weiteren Anlauf für ein neues Datenschutzgesetz. Zwei ausschussvorsitzende Politiker der beiden Parteien haben hierfür am 07. April 2024 einen Entwurf vorgestellt. Der „American Privacy Rights Act“ (APRA) soll nationale Standards setzen und die steigende Zahl an Datenschutzgesetzen in den einzelnen Bundesstaaten eindämmen.

22 Glocker: EU-US Data Privacy Framework: Update des Privacy Shield mit Augenmaß ZD 2023, 189

Bisher gibt es in den USA kein einheitliches Datenschutzgesetz auf Bundesebene. In den vergangenen Jahren gab es einige Versuche, ein solches zu erschaffen, allerdings bislang ohne Erfolg. Hierzu gehört etwa der „American Data Privacy and Protection Act" (ADPPA) von 2022.

Die Republikanerin Cathy McMorris Rodgers und die Demokratin Maria Cantwell präsentierten den Entwurf für ein neues Datenschutzgesetz in den USA als eine vielversprechende Möglichkeit, einen einheitlichen Datenschutzstandard zu etablieren und den Bürgern mehr Kontrolle über ihre personenbezogenen Daten zu geben. Die Politikerinnen sehen laut ihrer Pressemitteilung die Erfolgschancen so hoch wie nie in den letzten Jahren, da beide Parteien den Vorschlag unterstützen.

Am 23. Mai 2024 wurde nun ein abgeänderter Vorschlag vom Energie- und Handelsausschuss des Repräsentantenhauses an den gesamten Ausschuss weitergeleitet.

I. Inhalt der Gesetzesinitiative

Ähnlich wie die europäische DSGVO knüpft der aktuelle Entwurf an personenbezogenen Daten an. Der APRA betont die Notwendigkeit einer bewussten und freiwilligen Einwilligung zur Datenverarbeitung. Auch existiert das Konzept der Datenminimierung. Besonders sensible Daten dürfen nur mit ausdrücklicher Zustimmung verarbeitet werden. Öffentlich zugängliche Informationen erhalten weitgehend keinen Schutz, dazu gehören etwa Informationen, die frei auf Webseiten einsehbar sind. In Anlehnung an das kürzlich in der EU verabschiedete Gesetz zur Festlegung harmonisierter Regeln für künstliche Intelligenz gibt es auch einige Passagen, die für Algorithmen gewisse Regeln vorsehen. Hierzu gehört etwa eine Risikoabschätzung oder das Recht auf eine Folgeentscheidung durch einen Menschen. Zur Durchsetzung der Regeln soll es zivilrechtliche Betroffenenrechte und besondere Befugnisse der Durchsetzungsbehörde für US-Wettbewerb und Verbraucherschutz, der Federal Trade Commission (FTC), geben. Auch soll es unter bestimmten Voraussetzungen die Pflicht zur Bestellung eines Datenschutzbeauftragten geben. Ein einzurichtender Entschädigungsfond soll Betroffenen bei Datenschutzverletzungen zugutekommen.

Im nun dem gesamten Ausschuss vorgelegten geänderten Entwurf existieren auch Regeln zu Privacy by Design, die Anbietern von Dienstleistungen und Produkten – vergleichbar mit Art. 25 DSGVO – vorschreiben, Datenschutz schon durch die jeweilige Technikgestaltung zu schaffen. Zudem soll es eine Ausnahme von dem Grundsatz der Datenminimierung für spezielle Forschungszwecke geben. Außerdem sollen Datenhändler einen Mechanismus implementieren, der es Betroffenen ermöglicht, die Löschung aller Daten zu verlangen, die der Verantwortliche nicht direkt vom Individuum erhalten hat.

II. Verhältnis zu Datenschutzgesetzen der Bundesstaaten

Da es Ziel des Gesetzesentwurfes ist, eine möglichst einheitliche Rechtslage zu schaffen, würde er viele bestehende Datenschutzgesetze der Bundesstaaten außer Kraft setzen. Bei dieser Vorrangigkeit von Bundesrecht handelt es sich um die sogenannte Pre-Emption. Gerade diese Regelung dürfte vielen Bundesstaatlern nicht passen. Deshalb listet der Entwurf verschiedene Regeln auf, die nicht von der Pre-Emption umfasst sind, wie etwa Verbraucherschutzgesetze oder Gesetze zum Schutz der Privatsphäre von Arbeitnehmern.

III. Bedeutung für den Angemessenheitsbeschluss

Zurzeit existiert zur Ermöglichung von Datenverkehr zwischen den USA und der EU ein im Juli 2023 erlassenes Privacy Framework. Ob dieses den Anforderungen an einen Angemessenheitsbeschluss genügt, wird aktuell in einem Verfahren vor dem EuGH thematisiert. Zumindest die letzten beiden Versuche, nämlich das Safe-Harbor-Abkommen und Privacy-Shield, sind vor dem EuGH gescheitert. Das neue Datenschutzgesetz würde bei Verabschiedung als Ausgangslage für die Beurteilung durch den EuGH herangezogen, falls das EuGH-Urteil nicht bereits davor fällt.

IV. Fazit

Die Einführung eines einheitlichen Datenschutzgesetzes auf Bundesebene könnte den Weg für eine klarere und konsistentere Datenschutzregulierung in den USA ebnen. Außerdem könnte dies endlich einen angemessenen Rechtsrahmen für den Datenaustausch mit Europa schaffen. Trotz vielversprechender Signale bleibt jedoch abzuwarten, was die Verhandlungen der nächsten Monate bringen und ob der APRA-Entwurf die notwendige Unterstützung findet.

F. Ausblick und Fazit

Die Datenschutzlandschaft in Nordamerika, insbesondere in den USA, präsentiert sich als ein komplexes Geflecht aus föderalen und bundesstaatlichen Regelun-

gen. Während auf föderaler Ebene bisher kein umfassendes Datenschutzgesetz existiert, bemühen sich einzelne Bundesstaaten zunehmend um eigene Regelungen, die den Schutz der Privatsphäre ihrer Bürger stärken sollen.

Diese föderale Zersplitterung bringt Herausforderungen sowohl für Unternehmen als auch für Verbraucher mit sich. Unternehmen müssen sich auf eine Vielzahl unterschiedlicher Regelungen einstellen, was den administrativen Aufwand und die Compliance-Kosten erheblich erhöht. Verbraucher hingegen können je nach Bundesstaat von unterschiedlichen Datenschutzstandards profitieren, was jedoch zu strukturellen Ungleichheiten im Datenschutz führt. Kritisch betrachtet ist die derzeitige Situation durch einen Mangel an Konsistenz und Effizienz geprägt. Die fragmentierte Gesetzgebung führt zu Unsicherheiten und zusätzlichen Belastungen, die vor allem kleine und mittlere Unternehmen überfordern können. Um diese Problematik zu lösen, sollten konkrete Schritte unternommen werden. Der aktuelle Entwurf für den bundesweiten APRA könnte hierfür einen geeigneten verbindlichen Mindeststandard für alle Bundesstaaten setzen. Es bleibt zu hoffen, dass der Vorschlag im Repräsentantenhaus weiterhin auf Zustimmung stoßen wird, um endlich geeignete einheitliche Datenschutzvorgaben für die USA zu schaffen.

Bis dahin wird es für Unternehmen entscheidend sein, flexibel zu bleiben und sich kontinuierlich an die sich entwickelnde Gesetzeslage anzupassen.

Insgesamt zeigt sich, dass der Datenschutz in den USA sich in einer dynamischen Entwicklungsphase befindet, die sowohl Risiken als auch Chancen für alle Beteiligten birgt. Eine engere Zusammenarbeit zwischen Bund und Ländern sowie ein verstärkter Austausch mit internationalen Datenschutzregelungen könnten hierbei den Weg zu einem effizienteren und gerechteren Datenschutz ebnen.

Rechtsanwalt **Dr. Kinast** ist Gründer und geschäftsführender Gesellschafter von KINAST Rechtsanwälte. Er ist externer Datenschutzbeauftragter zahlreicher nationaler und internationaler Großkonzerne, Banken und Versicherungen sowie Organisationen der Kirche und öffentlichen Hand. Weiterhin berät Herr Dr. Kinast als externer Compliancebeauftragter diverse Unternehmen der verschiedensten Branchen.