gungs- und Erstattungsklauseln in allgemeinen Geschäftsbedingungen nicht durchsetzbar oder gar rechtswidrig sein.

Aus diesen und weiteren Gründen sollten Unternehmen ihre internen Datenschutzan- 110
weisungen sowie ihre externen Datenschutzerklärungen, -bestimmungen und -verträge mit Betroffenen bewusst gestalten. In Datenschutzerklärungen, -bestimmungen und -verträgen können Unternehmen die Schwelle festlegen für eine einfache Datenoffenlegung (zB indem eine Einwilligung eingeholt oder eine vorherige Mitteilung bzgl. der Offenlegungspolitik des Unternehmens herausgegeben wird, wodurch Klagen von Nutzern gegen die Unternehmen oder im weiteren Sinne auch gegen die staatlichen Stellen wegen Datenschutzverletzung minimiert werden) oder für starken Widerstand gegen Anfragen staatlicher Stellen (zB indem strenge Anforderungen hinsichtlich der Offenlegung in Datenschutzerklärungen und -verträgen normiert werden, was wiederum Widerstand gegen Informationsanfragen staatlicher Stellen rechtfertigen kann). Darüber hinaus können Unternehmen innerhalb der Grenzen der Anforderungen an Datenvorhaltung und -löschung auch entscheiden, ob sie mehr oder weniger Daten für einen längeren oder kürzeren Zeitraum speichern. Dies können Unternehmen auf Grundlage der Erfahrung entscheiden, welche Anfragen von Behörden oder sonstigen staatlichen Stellen kommen, und danach, was die Unternehmen offenlegen möchten. Erwartet ein Unternehmen Informationsanfragen von staatlichen Stellen, die nach den Gesetzen eines anderen Landes problematisch sein könnten, kann das Unternehmen versuchen, einen engeren zeitlichen Rahmen zur Datenvorhaltung zu definieren. Bisweilen tendieren Gerichte und staatliche Stellen auch dazu, sich gegenseitig aus Höflichkeit (nicht aus Rechtspflicht) entgegenzukommen, insbes. dort, wo die angefragte Information im Ausland, zB von einer Tochtergesellschaft gespeichert ist. Jedoch haben die US-Gerichte bisher iRd prozessrelevanten Offenlegung grds. den Standpunkt vertreten, dass Informationen, die physisch auf US-Gebiet gespeichert oder für Leute auf US-Gebiet zugänglich sind, in Übereinstimmung mit dem US-Gesetz verarbeitet werden müssen, ohne große Rücksicht auf ausländisches Recht zu nehmen. Der Kongress hat diesen Grundsatz im CLOUD Act bestätigt. Viele andere Länder haben ähnliche Vorschriften, die es ihren Behörden erlauben, auf ihrem Hoheitsgebiet gespeicherte Daten zu beschlagnahmen oder den Zugang zu ihnen zu erzwingen, ohne sich an ausländische Gesetze zu halten.

Insbes. Unternehmen in der EU müssen sich auf Razzien in der Morgendämmerung 111
vorbereiten, die von Wettbewerbsbehörden, Steuerbehörden, Datenschutzbehörden und anderen staatlichen Einrichtungen häufig durchgeführt werden, um Mitarbeiter zu überraschen und vertrauliche Unterlagen mit personenbezogenen Daten und anderen Informationen zu beschlagnahmen. Das Personal, das die Empfangsbereiche bewacht, muss geschult werden, Zugang zu Notfallkontakten für juristische Unterstützung und kurze Richtlinien mit klaren Anweisungen (die so formuliert sind, dass sie den örtlichen Gesetzen entsprechen) über erste Reaktionen haben, wie das Recht, den Zugang zu verweigern, formell Einspruch zu erheben, gerichtliche Verfügungen zu verlangen und den Unternehmensanwalt zu kontaktieren.

Wenn ein Unternehmen zu dem Ergebnis gelangt, dass es ihm rechtlich verboten oder 112
dass es rechtlich nicht verpflichtet ist, auf eine bestimmte Anfrage einer öffentlichen Stelle zu antworten und aus Geschäftsgründen auch nicht antworten möchte, kann sich das Unternehmen im Rahmen seines Einwands gegen diese Anfrage auf das Datenschutzrecht und die Belange der betroffenen Person berufen. Das Unternehmen kann den Betroffenen auch über die Anfrage informieren und ihm so die Möglichkeit geben, selbst direkt dagegen vorzugehen. Unternehmen können jedoch idR nicht selbst ihre eigenen Datenschutzrechte geltend machen, da Unternehmen für gewöhnlich keinen Datenschutz genießen

In einigen Konstellationen können Unternehmen ihre Informationen ggf. dadurch 113
schützen, dass sie sich auf ihr Betriebsgeheimnis berufen oder sie können Informationsanfragen ggf. auch unter Berufung auf die unangemessene Belastung oder die Irrelevanz der angefragten Daten für den damit verfolgten Zweck anfechten.

114 Sieht sich ein Unternehmen regelmäßig Anfragen von staatlichen Behörden ausgesetzt, so sollte es – natürlich unter Berücksichtigung der Umstände des Einzelfalls – versuchen, eine einheitliche und konsequente Strategie gegenüber staatlichen Stellen zu verfolgen.

I. Internet of Everything, Vernetzte Geräte

115 Hersteller haben immer mehr ihrer Produkte mit Konnektivitätsfunktionen ausgestattet. Grund hierfür ist unter anderem, dass zellulare und drahtlose Kommunikationsverbindungen allgegenwärtig und wirtschaftlich rentabel geworden sind. Selbstfahrende Autos, Drohnen und andere Geräte können und müssen geortet werden und untereinander sowie mit Dritten (einschließlich Radfahrern und Fußgängern) zu Sicherheits- und Schadensverhütungszwecken kommunizieren. Das „Internet der Dinge", „Internet of Everything" oder „Machine-to-Machine" (M2M) Handel und Kommunikation erzeugen riesige Mengen an Daten über Geräte sowie deren Besitzer, Halter, Betreiber, Passagiere und Personen in der Nähe ihrer Sensoren. Bürger in aller Welt sind besorgt, dass nicht einmal die NSA die Daten sicher aufbewahren kann. Viele industrielle Systeme und Verbraucherprodukte sind weit weniger sicher und daher anfällig für Angriffe. Die US-amerikanische FTC hat gegen Unternehmen geklagt, die Geräte mit unzureichenden Datensicherheitsfunktionen verkauft haben. Darunter war ein Unternehmen, das Sicherheitskameras mit voreingestellten Passwörtern für den Online-Zugang geliefert hat, die die Verbraucher nicht geändert haben. Ferner wurde ein anderes Unternehmen verklagt, welches Software-Updates mit ihm bekannten Schwachstellen verkauft hat. Seit dem 1. Januar 2020 müssen Hersteller in Kalifornien vernetzte Geräte mit angemessenen Sicherheitsfunktionen ausstatten, die bestimmte gesetzliche Mindestanforderungen erfüllen. Bedenken hinsichtlich der Netzsicherheit gelten auch für Autos, Waffensysteme, Industrieanlagen, Energieerzeugungsanlagen, Flugzeuge und andere Maschinen, die von Hackern aus der Ferne gekapert werden könnten. Unternehmen sollten die Cybersicherheit bei der Entwicklung von Produkten und Systemen sowie bei der Planung von Räumlichkeiten sorgfältig berücksichtigen.

J. Jurisdiktion

116 Jedes Bestreben, Vorschriften einzuhalten, sowie jede rechtliche Haftungsanalyse beginnt mit zwei Fragen: (1) welche Gesetze sind anwendbar und (2) wie können die anwendbaren Gesetze durchgesetzt werden? Im Hinblick auf die Einhaltung datenschutzrechtlicher Bestimmungen, insbes. im internationalen Kontext, ist es notwendig, die einschlägigen Gesetze zu ermitteln und deren Einhaltung zu priorisieren.

117 *Anwendbares Gesetz:* Die Antwort auf die erste Frage – welches ausländische Datenschutzrecht findet Anwendung? – kann sehr lange sein. Nach Völkergewohnheitsrecht steht es jedem souveränen Land frei, je nach individuellem Bedarf Gesetze zu erlassen. IdR erklären die Länder ihr Datenschutzrecht für denjenigen anwendbar, der auf ihrem Hoheitsgebiet entweder Arbeitskräfte oder Arbeitsmittel einsetzt. Manche Länder gehen darüber hinaus und erklären ihr Datenschutzrecht auch für Unternehmen im Ausland anwendbar, wenn diese Unternehmen in dem jeweiligen Land Daten sammeln mittels lokaler Geschäftspartner, gezielter Webseiten (etwa gekennzeichnet durch Sprache, bestimmten Kontext, Währung, örtliche Telefonnummern und andere Einzelheiten) oder allein aufgrund der Tatsache, dass das ausländische Unternehmen Daten über Einwohner oder Staatsbürger des gesetzgebenden Landes sammelt. Deshalb stellen viele Unternehmen mit mehr oder weniger direktem Geschäftskontakt zu anderen Ländern bei näherem Hin-

sehen fest, dass tatsächlich das Datenschutzrecht eines anderen Landes auf ihre Auftragsverarbeitungsvorgänge Anwendung findet.

Das Recht der EU schränkt die Möglichkeiten ihrer Mitgliedstaaten ein, ihre nationalen 118
Datenschutzgesetze extraterritorial auf Unternehmen anzuwenden, die in anderen EWR-Mitgliedstaaten ansässig sind. Ein Verantwortlicher mit Sitz im EWR muss nur die Gesetze des EWR-Mitgliedstaats einhalten, in dem er eine Zweigstelle oder eine andere bedeutende physische Präsenz unterhält, selbst wenn er Daten aus anderen EWR-Mitgliedstaaten sammelt. Dieses Privileg gilt jedoch nicht für Unternehmen außerhalb des EWR. Daher muss ein in den USA ansässiges E-Commerce-Unternehmen, das Kunden im gesamten EWR hat, unter Umständen 30 verschiedene nationale Gesetze einhalten. Gründet das US-Unternehmen jedoch eine Tochtergesellschaft, bspw. in Irland (niedriger Körperschaftssteuersatz, Englisch als Amtssprache, hochqualifizierte Arbeitskräfte, vertrautes Rechtssystem, starke Rechtsstaatlichkeit, wirtschaftsfreundliche Regierung), um alleiniger Vertragspartner und Verantwortlicher für alle europäischen Kunden zu werden, dann müsste die neue Tochtergesellschaft nur die Datenschutzgesetze des Landes einhalten, in dem sie ihren Sitz hat.

Die Bedeutung dieses Vorteils hat sich durch die Harmonisierung iRd DS-GVO verrin- 119
gert, aber Unternehmen sollten diese Möglichkeit dennoch in Betracht ziehen, da viele nationale Datenschutzgesetze weiterhin in Kraft bleiben. Unternehmen in den USA können sich möglicherweise auf einen ähnlichen Schutz gemäß der Gewerbeklausel der US-Verfassung gegen staatliche Gesetze berufen, die den zwischenstaatlichen Handel diskriminieren oder unangemessen belasten.

Durchsetzbares Recht: Die Antwort auf die zweite Frage – wie kann Datenschutzrecht 120
insbes. über die Landesgrenzen hinweg durchgesetzt werden? – ist komplexer aber idR sehr hilfreich. Im Regelfall können Länder ihre Gesetze gegenüber Unternehmen, die in diesem Land weder physische Präsenz, Vermögenswerte noch Arbeitnehmer haben, nicht ohne Weiteres durchsetzen. Das internationale Gewohnheitsrecht verbietet es Ländern, ihre Staatsdiener und Beamten grenzüberschreitend in ein anderes Land zu entsenden, um Verwarnungen auszusprechen, Geldbußen einzutreiben oder Verhaftungen vorzunehmen. Es ist nicht einmal erlaubt, Verfügungen oder offizielle Briefe mit Verwarnungen oder Androhungen per Post oder E-Mail über die Grenzen des eigenen Landes hinaus zu verschicken, ohne die Einwilligung des Heimatlandes der betroffenen Person einzuholen. Einige Länder kooperieren sehr eng miteinander bei gewissen Themen (zB die EU-Staaten). Des Öfteren ist es jedoch äußerst schwierig und mühsam Vollstreckungsmaßnahmen gegenüber Unternehmen in anderen Ländern durchzusetzen. Privatklägern (zB die Betroffenen) wird es jedoch häufig gelingen, ein Gericht in ihrem Heimatland davon zu überzeugen, sich hinsichtlich eines ausländischen Unternehmens dennoch für zuständig zu erklären. Jedoch ist es schwierig oder gar unmöglich, in dem fremden Land ein daraus resultierendes Urteil grenzüberschreitend zu vollstrecken. Einstweilige Verfügungen, Strafen und andere Sanktionen können idR überhaupt nicht grenzüberschreitend vollstreckt werden. Zahlungstitel (zB ein titulierter Schadensersatzanspruch aus einem Zivilurteil) können einfacher durchgesetzt werden, solange sie jedenfalls nicht auch Straf- oder Sanktionscharakter haben oder sich auf Verfahrensgrundsätze beziehen, welche die öffentliche Ordnung beeinträchtigen. Dies erfasst jedoch nur Entschädigung für Vermögensschäden, die idR eher gering sind, weshalb sich eine Vollstreckung in Fällen mit Datenschutzbezug außer im Wege von Sammelklagen in den USA oft nicht lohnt. Deshalb und wegen weiterer praktischer Gründe (einschließlich der Kosten und Schwierigkeiten iRd Geltendmachung von Ansprüchen in einer anderen Rechtsordnung, einer anderen Sprache und einem anderen Rechtssystem) ist das praktische Risiko der Vollstreckung des ausländischen Datenschutzrechtes viel geringer als dessen theoretische Anwendbarkeit.

Es gibt dennoch mehrere beachtenswerte Ausnahmen: Unternehmen, die sich vertrag- 121
lich dazu verpflichtet haben, ausländisches Datenschutzrecht zu befolgen (zB durch Verwendung der EU-Standardvertragsklauseln oder formfreier Dienstverträge), können zur

Einhaltung von ihren ausländischen Geschäftspartnern gezwungen werden. Geschäftspartner haben die Mittel und die Motivation, diese auch durchzusetzen, weil sie zB wiederum direkt staatlichen Vollstreckungsmaßnahmen ausgesetzt sind oder die Einhaltung aus wirtschaftlichen Gesichtspunkten für sie wichtig ist. Darüber hinaus können sich Unternehmen auch der Anwendung ausländischen Rechts unterworfen und dazu eingewilligt haben, im Zusammenhang mit Erlaubnis- und Genehmigungsanträgen mit den ausländischen Datenschutzbehörden mehr oder weniger freiwillig zusammen zu arbeiten.

122 Aufgrund dieser Überlegungen können Unternehmen eine Prioritätenliste bzgl. der verschiedenen Gerichtszuständigkeiten dahingehend aufstellen, wessen Datenschutzrecht am ehesten angewendet und durchgesetzt wird. Innerhalb dieser Liste können die einzelnen Gerichtszuständigkeiten nach der Stärke des Zusammenhangs eingeordnet werden (physische Präsenz und Auftragsverarbeitungsmitarbeiter > gezielte Webseiten > ortsansässige Betroffene), danach ob das Unternehmen sich vertraglich oder auf andere Weise der Rechtsordnung und Gerichtszuständigkeit eines anderen Landes unterworfen hat (zB im Zusammenhang mit Erlaubnissen oder Genehmigungen) und danach, ob die Gerichte im Heimatland des Unternehmens mit einem fremden Land hinsichtlich der Vollstreckung datenschutzrechtlicher oder anderer Vorschriften zusammenarbeiten. Sollten die danach herausgefilterten relevanten Rechtsordnungen immer noch unüberschaubar zahlreich sein, können Unternehmen weiter priorisieren nach den Ländern, die erhebliche Einnahmen erwirtschaften bzw. versprechen oder für besonders hohe Anfälligkeiten bekannt sind, was ein Unternehmen negativ beeinträchtigen können (zB Deutschland), oder die besonders einschneidende Vollstreckungsmaßnahmen vorweisen können (zB astronomisch hohe Strafen in Frankreich und Spanien, öffentliche Festnahme eines US-Datenschutzbeauftragten in Italien).

K. Künstliche Intelligenz

123 Entwickler benötigen Daten, um selbstlernende Algorithmen, künstliche Intelligenz und andere Systeme trainieren zu können. So müssen Sie bspw. autonome Fahrzeugsysteme mit einer Vielzahl von Bildern, Videos, Tönen, Radar- und anderen Sensordaten versehen. Diese betreffen Straßen, Verkehrszeichen und -signale, Fußgänger, Radfahrer, Fahrer, Passanten und Verkehrssituationen. Ziel hierbei ist es, dass das System dazu in der Lage ist, Unfälle zu vermeiden und sonstige Risiken für Menschen zu verringern und sich diesbezüglich auch zu verbessern. Die Daten, die Sie benötigen, enthalten zwangsläufig Informationen über Kinder und sensible Daten, da Bilder von Personen auf öffentlichen Straßen unvermeidbar deren rassische und ethnische Herkunft, Gesundheitszustand (zB Brille oder Krücken) und Glaubensrichtungen (zB Kreuze, Hijabs, Slogans auf T-Shirts) zeigen. Nach der DS-GVO und dem CCPA müssen Unternehmen die Betroffenen über die automatisierte Entscheidungsfindung informieren, ihnen erklären, wie sich ihre Algorithmen auf den Einzelnen auswirken, und zudem Opt-Out-Möglichkeiten anbieten. Einige Unternehmen stellen sicher, dass Menschen die endgültigen Entscheidungen treffen, damit Offenlegungs- und Opt-Out-Anforderungen vermieden werden.

124 Organisationen ist die Erhebung und Weitergabe von Daten nach der DS-GVO, dem CCPA und anderen Gesetzen, die eine ausdrückliche Einwilligung erfordern oder den Betroffenen das Recht einräumen, dem Verkauf von Informationen zu widersprechen, untersagen oder stark einschränken.

125 Organisationen dürfen Daten nach der DS-GVO, dem CCPA und anderen Gesetzen, die eine ausdrückliche Einwilligung der Betroffenen erfordern oder diesen das Recht einräumen, dem Verkauf von Informationen zu widersprechen, nicht oder nur sehr stark eingeschränkt erheben und weitergeben. Folglich wird es für Entwickler immer schwieriger, die Daten zu beschaffen, die sie für maschinelles Lernen und andere Innovationen benöti-

gen. Lokale Behörden, Forschungseinrichtungen sowie kleinere Unternehmen können sich keine aufwändigen Datenerhebungsmaßnahmen leisten und sind vielmehr auf Informationslieferanten angewiesen. Darüber hinaus sind die Betroffenen durch mehrfache Datenerhebungsvorhaben stärker beeinträchtigt. Diese ergeben sich aus den zunehmenden Beschränkungen für einen effizienten Datenaustausch sowie aus der Bindung und der Zusammenarbeit zwischen Organisationen. Die Anforderungen an die Datenminimierung und die Beschränkung des Datenaustauschs wirken sich folglich negativ auf die Privatsphäre, die Innovation und den Wettbewerb aus. Zudem festigen sie die Wettbewerbsvorteile von Unternehmen, die bereits über eine große Menge an Daten verfügen. Unternehmen müssen diese Dynamik bei der Planung ihrer Vorhaben zur Datenerhebung, Kommerzialisierung und Entwicklung berücksichtigen, insbes. im Hinblick auf geografische Standorte und Gerichtsbarkeiten.

L. Landes-, Bundes- und Europarecht

Global agierende Unternehmen müssen sich nicht nur mit der internationalen Anwend- 126
barkeit von national geltenden Datenschutzgesetzen befassen. Darüber hinaus sind sie mit Regelungen verschiedener Gesetzgeber in einem Staat konfrontiert. In Deutschland erlassen zB sowohl die Länder als auch der Bund Datenschutzgesetze. Überdies gibt es Landes- und Bundesverfassungen, Verordnungen und Richtlinien der EU, die Grundrechtecharta der Union sowie die Europäische Menschenrechtskonvention (EMRK) und andere völkerrechtliche Regelungen, was die Rechtslage durchaus unübersichtlich machen kann.

Völkerrecht, Verfassungen und EU-Richtlinien haben in aller Regel keine unmittelbare 127
Wirkung zwischen Privaten (zB Unternehmen oder Einzelpersonen), sondern richten sich an den Staat – anders als nationale Gesetze und zB die DS-GVO. Unternehmen innerhalb und außerhalb des EWR müssen die DS-GVO einhalten, zB wenn Unternehmen außerhalb des EWR personenbezogene Daten mittels eines Onlinedienstes von Verbrauchern aus dem EWR oder mittels einer im EWR gelegenen Einrichtung sammeln. Die DS-GVO verlangt von Unternehmen insbes. das Folgende:

- Unternehmen müssen im Hinblick auf Maßnahmen eine Datenschutz-Folgenabschätzung vornehmen, die zu einem hohen Risiko für die betroffene Person führen können, zB die Erhebung von großen Mengen sensibler Daten. Des Weiteren müssen sie alle Datenverarbeitungstätigkeiten sowie die unternommenen Maßnahmen zur Einhaltung der Datenschutzgesetze in einem vorgegebenen Datensatzformular dokumentieren. Dabei sind insbes. die verschiedenen Kategorien von personenbezogenen Daten und Betroffenen, die Zwecke der Verarbeitung, die Empfänger, internationale Datentransfers sowie geeignete Garantien, Fristen für die Löschung und technische und organisatorische Sicherheitsmaßnahmen anzugeben (Art. 30, 35 DS-GVO).
- Unternehmensgruppen müssen idR für all ihre Niederlassungen einen Datenschutzbeauftragten benennen (die Benennung eines einzigen Datenschutzbeauftragten für alle Konzerngesellschaften ist ausreichend, sofern dieser sämtliche Niederlassungen des Unternehmens überwachen kann und sofern er von jeder Niederlassung aus leicht erreicht werden kann; Art. 37 DS-GVO).
- Unternehmen außerhalb des EWR müssen einen Vertreter innerhalb des EWR bestimmen (Art. 27 DS-GVO).
- Unternehmen müssen Datenvorhaltungs- und Datenlöschungsprogramme einführen, um die strengen Vorschriften hinsichtlich der Rechte der Betroffenen auf Auskunft, Berichtigung und Löschung erfüllen zu können (Art. 15–20 DS-GVO).
- Unternehmen müssen die Betroffenen detailliert über ihre Datenverarbeitungspraktiken belehren und dabei insbes. Folgendes mitteilen: den Namen und die Kontaktdaten des Verantwortlichen (sowie ggf. seines Vertreters im EWR, falls der Verantwortliche nicht

im EWR niedergelassen ist); die Kontaktdaten des Datenschutzbeauftragten; die Zwecke, für welche die personenbezogenen Daten verarbeitet werden sollen; die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden, wenn das die Rechtfertigung für die Verarbeitung darstellt; die Empfänger oder Kategorien von Empfängern; im Falle des internationalen Datentransfers, das Vorhandensein oder Fehlen eines Angemessenheitsbeschlusses der Kommission und ggf. einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind sowie viele weitere Details. Der Verantwortliche hat diese Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln (Art. 12, 13, 14 DS-GVO).

– Unternehmen müssen Maßnahmen einführen, um sicherzustellen, dass eine Verletzung des Schutzes personenbezogener Daten innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde gemeldet und die betroffene Person benachrichtigt wird (Art. 33, 34 DS-GVO).

128 Die DS-GVO geht grds. nationalen Datenschutzvorschriften vor und harmonisiert das Datenschutzrecht auf europäischer Ebene. Allerdings erlaubt oder verlangt die DS-GVO vielfach durch mehr als 50 Öffnungsklauseln den Erlass von Datenschutzvorschriften auf nationaler Ebene, sodass Unternehmen neben der DS-GVO auch weiterhin die nationalen, ggf. auch die strengeren Vorschriften beachten müssen. In Deutschland müssen Unternehmen insbes. das Bundesdatenschutzgesetz einhalten. Deutsche Landesdatenschutzgesetze richten sich vornehmlich an Landesbehörden, nicht Privatunternehmen.

129 In Österreich ergänzt das Datenschutzgesetz (DSG) die DS-GVO maßgeblich, welches als Bundesgesetz erlassen wurde. In der Schweiz haben Unternehmen künftig das neue Bundesgesetz über den Datenschutz (DSG), die Ausführungsbestimmungen in der neuen Datenschutzverordnung (DSV) und die neue Verordnung über Datenschutzzertifizierungen (VDSZ) einzuhalten, welche am 1. September 2023 in Kraft treten. Dadurch findet eine Annäherung an die DS-GVO statt.

M. Minderjährige

130 In den USA, wo regelmäßig weder die Einwilligung noch ein Vertrag nach Datenschutzrecht erforderlich ist, hat sich der Gesetzgeber für spezielle Gesetze entschieden, um Kinder vor Internetfirmen zu schützen. Nach dem Children Online Privacy Protection Act (COPPA) von 1998 müssen Webseitenbetreiber bestimmte Anforderungen erfüllen, wenn sie entweder wissend Daten von Kindern unter 13 Jahren sammeln oder ihre Webseite an Kinder unter 13 gerichtet ist. Die FTC hat kürzlich klargestellt, dass Unternehmen die Einwilligung der Eltern einholen müssen, selbst wenn sie Daten ohne Namen aber mit Identifizierungsmerkmalen, wie zB pseudonymer Nutzerkennung oder Cookies sammeln. Ob sich eine Seite an Kinder richtet, hängt von einer Gesamtbewertung der Themen und Graphiken der Webseite sowie des Durchschnittsalters der Nutzer und anderer Faktoren ab. Eine Klausel in den Nutzungsbedingungen der Webseite, nach der Nutzer 13 Jahre oder älter sein müssen, genügt nicht um die Anwendbarkeit des COPPA zu verhindern. Im Fall der Anwendbarkeit des COPPA muss der Webseitenbetreiber Datenschutzrichtlinien separat an Kinder und an deren Eltern richten und deren Einwilligung einholen. Für Webseitenbetreiber ist es schwierig, mit Sicherheit zu bestimmen, ob die zustimmende Person, die sich als Elternteil des Kindes registriert, tatsächlich der Vertretungsberechtigte ist (und nicht das Kind selbst unter einer anderen E-Mail-Adresse oder mit anderen Nutzerdaten). Wenn der Webseitenbetreiber Selbstregulierungs-Leitlinien befolgt, welche von der FTC gebilligt wurden, wird die Einhaltung der COPPA-Vorschriften durch den Webseitenbetreiber vermutet. Nach dem CCPA müssen Unternehmen die Einwilligung von

Kalifornien unter 16 Jahren und die Einwilligung der Eltern bei Kindern unter 13 Jahren einholen, bevor sie personenbezogene Daten von Kindern verkaufen. Für Unternehmen ist es viel schwieriger, sich zu vergewissern, dass sich ein Online-Dienst nicht an Kinder unter 16 Jahren richtet als an Kinder unter 13 Jahren. Denn Kinder, die sich ihrem 16. Geburtstag nähern, haben in vielen Bereichen eher ähnliche Interessen wie Erwachsene.

Nach der DS-GVO müssen Unternehmen die Einwilligung der Eltern einholen, bevor 131
sie personenbezogene Daten von Kindern unter 16 Jahren auf der Grundlage ihrer Einwilligung erheben, wobei einzelne EWR-Mitgliedstaaten das Schwellenalter wie in den USA auf 13 Jahre senken können. Dies führt zu einer gewissen Rechtsunsicherheit. So liegt zB in Deutschland die Altersgrenze bei 16 Jahren und in Österreich bei 14 Jahren. Ferner lässt die DS-GVO das allgemeine Vertragsrecht der Mitgliedstaaten unberührt, wie zB das wirksame Zustandekommen von Verträgen mit Minderjährigen. Damit können andere Altersgrenzen gelten, wenn die Datenverarbeitung hinsichtlich Minderjähriger auf andere Rechtsgrundlagen wie etwa die Erfüllung vertraglicher Pflichten oder berechtigte Interessen gestützt wird, zB bei der Verwendung von Internetdiensten im schulischen Kontext. Hier bezahlt der Minderjähre nicht mit seinen Daten, sodass nach deutschem Vertragsrecht (Altersgrenze 7 Jahre) die Willenserklärung zumindest nicht rechtlich nachteilig und damit eine Einwilligung der gesetzlichen Vertreter nicht erforderlich wäre. Im Ergebnis würde also die Altersgrenze davon abhängen, ob die Einwilligung nach dem jeweiligen Vertragsrecht erforderlich ist oder ob man sich auf die Einwilligung als Rechtsgrundlage stützt.

N. Nutzerprofile

Wenn natürliche Personen Datenverarbeitungs- und Kommunikationsgeräte benutzen, ge- 132
nerieren und übermitteln sie eine Unmenge an Daten. Viele dieser Daten werden nicht im Zusammenhang mit dem Namen einer bestimmten Person gespeichert, können aber ziemlich leicht mit einer bestimmten Person verbunden werden. Wenn man zB eine bestimmte Webseiten-Adresse in den Browser eingibt, sendet der Computer eine Anfrage mit bestimmten Informationen über den Computer sowie seine Soft- und Hardware an den Server, der die aufgerufene Webseite bereitstellt. Dieser Server verarbeitet die empfangenen Daten, um auf die Anfrage damit zu reagieren, was immer der Webseitenbetreiber den Besuchern zur Verfügung stellt – Bilder, Texte, für gewöhnlich auch Cookies, also kleine Softwaredateien, die auf dem Computer des Webseitenbesuchers platziert werden, um Informationen über den Besucher für den zukünftigen Zugriff auf diese Webseite zu speichern. Wenn der Webseitenbetreiber den Namen des Benutzers herausfindet (weil dieser sich für eine Dienstleistung registriert oder ein Produkt online zum Versand bestellt) kann der Webseitenbetreiber die aktiv übermittelten Daten (Name, Adresse) mit den passiv erfassten Daten (zuvor und danach besuchte Webseiten, auf einer bestimmten Seite verbrachte Zeit, Soft- und Hardware-Konfigurationen) verbinden. Viele dieser Daten werden auf die Initiative der betroffenen Person hin zu Kommunikations- und Informationsverschaffungszwecken gesammelt. Insoweit ist die Datenverarbeitung regelmäßig nach Datenschutzrecht erlaubt. Jedoch kann jede sekundäre Nutzung oder Sammlung der Daten, die nicht mehr allein dazu dient, vertragliche Pflichten gegenüber der betroffenen Person zu erfüllen, nach europäischem Recht der Einwilligung oder des berechtigten Interesses und in vielen anderen Ländern der Benachrichtigung und der Widerspruchs- bzw. Widerrufsmöglichkeit erfordern.

Cookies. Cookies und ähnliche Technologien werden zusammen mit dem Webinhalt als 133
Antwort auf Anfragen des Browsers gesendet. Viele Webseitenbetreiber erlauben es auch Dritten, deren Werbung sie auf ihrer Webseite anzeigen lassen, Cookies zu verschicken.

Cookies dienen dazu, bestimmte Informationen über den anfragenden Computer zu sammeln und zurückzumelden. Sie werden vor allem für folgende Zwecke verwendet:

1. Einige Cookies unterstützen die Funktionalität der Webseite. Cookies speichern zB, was ein Online-Käufer in seinen Einkaufswagen gelegt hat, bevor er sich mit seinem sicheren Konto anmeldet. Cookies können auch den Namen des Besuchers, Spracheinstellungen und andere Konfigurationen speichern. Sie können auch dazu verwendet werden, Informationen hinsichtlich der Webseiten zu sammeln, die der Besucher aufgerufen hat, bevor und nachdem er eine bestimmte Webseite besucht hat. Dadurch wird die Webseite verbessert, weiter individuell auf die Nutzer zugeschnitten und auch die Effektivität der Seite gemessen. Internetnutzer müssen über die Datenverarbeitung mittels derartiger Cookies informiert werden. Wenn und soweit die Cookies jedoch dazu erforderlich sind, der betroffenen Person die jeweiligen Dienste anzubieten, muss der Betreiber idR weder die ausdrückliche Einwilligung der betroffenen Person einholen noch Widerspruchs- bzw. Widerrufsmöglichkeiten bieten.
2. Einige Cookies unterstützen die Analyse des Webseiten-Verkehrs, Verbesserungen der Webseite und gezielte Werbung des Betreibers (sowohl auf seiner eigenen Seite als auch auf Seiten Dritter, um die Nutzer auf seine Seite zurückzuholen). Diese Cookies werden von dem Betreiber oder seinem Diensteanbieter platziert, um zu messen, wie viel Zeit der Nutzer auf einer bestimmten Seite verbracht, ob er Werbeseiten angeklickt oder Pop-up Fenster geschlossen hat. Durch diese Cookies werden regelmäßig keine personenbezogenen Daten an die Verantwortlichen übermittelt, weshalb solche Cookies oft als „Eigen-Cookies" bezeichnet werden (in Abgrenzung zu „Fremd-Cookies", welche im folgenden Abschnitt erläutert werden sollen). In vielen Ländern können „Eigen-Cookies", die nicht notwendig für die Dienstleistungserbringung sind, anhand einer einseitigen Mitteilung platziert werden (zB in der Datenschutzerklärung auf der Webseite). Nach europäischem Recht müssen Webseitenbetreiber vor Verwendung solcher Cookies deren Einwilligung einholen. Oft ist aber nicht klar, ob der Webseitenbetreiber (zB eine Internetzeitung) den Nutzern, die die Einwilligung versagen, dennoch die Nutzung seiner Dienste erlauben muss, weil es an der Freiwilligkeit der Einwilligung fehlen könnte. In diesem Zusammenhang gibt es drei Gestaltungsmöglichkeiten. (1) bei verweigerter Einwilligung, darf man die Webseite nicht nutzen; (2) bei erteilter Einwilligung darf man die Webseite mit Werbung nutzen; (3) bei Bezahlung darf man die Webseite werbefrei nutzen. Nach Ansicht der deutschen Datenschutzbehörden soll das Zusammenspiel aus (2) und (3) möglich sein, wenn erstens die Leistung im Bezahlmodell eine gleichwertige Alternative zur Leistung im Bezahlmodell darstelle und zweitens die Wirksamkeitsvoraussetzungen für eine Einwilligung nach der DS-GVO vorliegen, insbes. hinsichtlich der Granularität. Nach der DS-GVO müssen Unternehmen prüfen, ob der Druck zur Preisdifferenzierung dazu führt, dass die Einwilligung der Verbraucher oder Arbeitnehmer unfreiwillig ist. Unternehmen dürfen Kalifornier, die ihre Datenschutzrechte gemäß dem CCPA wahrnehmen, nicht diskriminieren. Dies umfasst das Recht, dem Verkauf ihrer persönlichen Daten oder der Weitergabe ihrer persönlichen Daten für kontextübergreifende verhaltensbezogene Werbung zu widersprechen.
3. Einige Cookies unterstützen gezielte Werbung und damit verbunden auch die Rückverfolgung durch werbetreibende Dritte. Betreiber, die verantwortlichen Dritten erlauben, Cookies zu platzieren, wenn der Nutzer die Webseite des Betreibers besucht, beteiligen sich damit nicht nur an der Datenübermittlung, sondern ermöglichen es auch der dritten Partei, Daten direkt zu sammeln. Die Betreiber haben nur wenig Kontrolle darüber und manchmal nicht einmal Kenntnis davon, welche Daten die dritte Partei überhaupt sammelt. Werbetreibende Dritte haben für gewöhnlich nicht die Möglichkeit, die Verbraucher zu unterrichten oder deren Einwilligung einzuholen, weshalb sie mit dem Betreiber zusammenarbeiten müssen, um sicherzustellen, dass die Einwilligung, soweit gesetzlich erforderlich, eingeholt wurde und dass alle erforderlichen Be-