Anspruchsvolle EU Regulatorik im Bereich KI und Maschinendaten

Von Dr. Oliver Meyer-van Raay, Prof. Dr. Marc Strittmatter, Vogel & Partner, Karlsruhe/Stuttgart

Dr. Oliver Meyer-van Raay

Dr. Oliver Meyer-van Raay, Fachanwalt für Informationstechnologierecht, berät Unternehmen im IT-, Daten- und Datenschutzrecht und unterstützt seine Mandanten regelmäßig bei ihren Softwareeinführungs-, Digitalisierungs- und KI-Projekten.

Prof. Dr. Marc Strittmatter

Prof. Dr. Marc Strittmatter berät als Of Counsel Unternehmen, die sich Technologie-Einführungsprojekte im Bereich ERP, Cloud, Outsourcing oder Unternehmensvernetzung und der regulatorischen Compliance, insbesondere im Datenschutz- und im Datenrecht vorgenommen haben.

Kontakt

Gegründet 2011, hat sich **Vogel & Partner** als bekannte Adresse für Technologie-, IP- und Medienrecht etabliert. Mit Standorten in Stuttgart, Karlsruhe und dem „Legal Lab" in Konstanz bietet die Kanzlei maßgeschneiderte Lösungen für innovative Unternehmen und ihre IT-, IP- und datenbezogenen rechtlichen Anforderungen.

Weitere Informationen zur Kanzlei in der Anzeige auf Seite 342

Die EU hat 2020 eine umfassende Datenstrategie beschlossen, die sie mit zahlreichen Rechtsakten umzusetzen gedenkt. Zukünftig werden der Data Act, der Data Governance Act, der Digital Services Act, der Digital Markets Act, der AI Act und die AI Liability Directive, die NIS2-Richtlinie sowie der Cyber Resilience Act, neben der Datenschutz-Grundverordnung (DSGVO), den Zugang, den Austausch und die Nutzung von Daten sowie die Erbringung von datenbasierten Diensten regeln.

Der Data Act befasst sich mit nicht-personenbezogenen Daten, die von vernetzten Produkten generiert werden. Statt einer Zuordnung über die Rechtsfigur des Dateneigentums sieht der Data Act Zugangs- und Nutzungsansprüche vor, welche die Basis eines neuen Datenwirtschaftsrechts bilden.

Neben dem Datenwirtschaftsrecht liegt ein zweiter Schwerpunkt der aktuellen EU-Gesetzgebung in der Regulierung von Künstlicher Intelligenz. Die EU-Kommission blickt mit einem gewissen Stolz darauf, der weltweit erste Gesetzgeber zu sein, der sich dieses Themas in dieser Regelungstiefe annimmt. (Pressemeldung der Kommission vom 09.12.2023 https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6473).

Zugang zu Daten statt Dateneigentum – ein neues Datenwirtschaftsrecht

Der Data Act trat am 11.01.24 in Kraft. Die Umsetzungsfrist läuft bis Mitte September 2025, d.h. bis dahin müssen die entsprechenden Vorgaben, z.B. Anpassungen der Produktdesigns (Data Access by Design), Datenzugangsrechte, Erstellung von Dateninformationen und die Überarbeitung und Ergänzung von Verträgen umgesetzt sein.

Der europäische Gesetzgeber hat sich spätestens durch die Verabschiedung des Data Act gegen das Konzept des Dateneigentums entschieden und damit die Diskussion beendet (Steinrötter, RDi, 2021, S. 483).

Neu regelt der Data Act nun das Recht der Nutzer auf Datenzugang und Datennutzung (Art. 3, 4 DA) der von ihnen generierten Daten, er verlangt den Abschluss von Datenlizenzverträgen und verbietet dabei die Verwendung unangemessener Vertragsklauseln (Art. 13 DA). Künftig haben Nutzer einen gesetzlichen Anspruch auf Zugang, Nutzung und Weitergabe (Art. 5, 6 DA) der von ihnen generierten Produkt- und Dienstdaten. Dies bezieht sich auf eine breite Palette von datengenerierenden Geräten wie vernetzte („smarte") Haushaltsgeräte, Fahrzeuge und Industriemaschinen sowie auf digitale Dienste, die mit angeboten werden. Gleichzeitig zwingt der Data Act Unternehmen dazu, ihre Daten technisch zugänglich zu machen, was wiederum Anpassungen in der Produktgestaltung (Data Access by Design) erforderlich macht.

Dass es bei der Verarbeitung von Daten mit Personenbezug zwischen unionsrechtlich verankerten Gedanken des „free flow of data" und dem Datenschutzrecht zu Spannungsverhältnissen kommen wird, liegt auf der Hand. Zwar gilt das Datenschutzrecht vorrangig, ebenso können zur Herausgabe verpflichtete Dateninhaber in eingeschränktem Umfang aber auch Geschäftsgeheimnisschutz einwenden. Diese Ausweichstrategien erfordern juristisches Fingerspitzengefühl. Schließlich benötigen Datenüberlassungsvereinbarungenn auch Regelungen zur Höhe der Vergütung, die Vorgabe heißt hier u.a. FRAND. Wie dies praktisch umgesetzt werden kann, ist aktuell aber noch gänzlich offen.

Ein weiterer zentraler Aspekt des Data Act betrifft das Cloud-Switching. Cloud-Anbieter sind künftig verpflichtet, in ihren Verträgen Bestimmungen zu verankern, die es ihren Kunden ermöglichen, innerhalb von maximal 30 Tagen zu vergleichbaren Diensten zu wechseln, Art. 25 Abs. 2 lit. d) DA. SaaS-Anbieter werden hierüber wenig erfreut sein, basiert ihre Erfolgsrechnung doch auf langfristiger Kundenbindung.

Regulierung zur Künstlichen Intelligenz – der „AI Act"

Das bereits vom Europäischen Parlament verabschiedete Gesetz über Künstliche Intelligenz (Artificial Intelligence Act, kurz AI Act) wurde am 12.07.24 veröffentlicht. Ab dem 01.08.24 wird der AI Act in Kraft treten, ab Februar 2025 müssen Unternehmen die ersten Bestimmungen umsetzen.

Die KI-Regulierung und die Einordung nach Risikoklassen

In Anlehnung an die Definition der OECD versteht der AI Act unter einem KI-System ein „maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können." Die Abgrenzung zu „normaler" Software verläuft also insbesondere entlang des Kriteriums des „Ableitens", welches einen gewissen Grad an Autonomie und typischerweise den Einsatz von Machine Learning Technologien voraussetzt.

Ein wesentliches Element des AI Act ist neben den sogenannten Totalverboten, die bestimmte Systeme und Einsatzzwecke mit inakzeptablem Risikopotenzial untersagen (wie z.B. KI-Systeme zur Ableitung von Emotionen einer natürlichen Person am Arbeitsplatz), die Regulierung von KI-Systemen, die als besonders risikobehaftet und damit als Hochrisiko-KI-Systeme eingestuft werden. Hierzu zählen laut Anhang III des AI Act z.B. KI-Systeme zur biometrischen Fernidentifizierung oder solche Systeme, die „bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen, insbesondere um gezielte Stellenanzeigen zu schalten, Bewerbungen zu sichten oder zu filtern und Bewerber zu bewerten". Für solche Hochrisiko-KI-Systeme gelten strenge Compliance-Vorgaben, z.B. in Bezug auf Datenqualität, Genauigkeit, Robustheit und Cybersicherheit. Allerdings sieht Art. 6 Abs. 3 des AI Act auch Einschränkungen vor, z.B. wenn das KI-System nur eine „eng gefasste Verfahrensaufgabe" oder eine „vorbereitende Aufgabe für eine Bewertung" durchführt; in solchen Fällen gelten die Systeme nicht (mehr) als hochriskant.

Die Regulierung von KI-Systemen im Rahmen des AI Act hängt aber nicht nur von der Risikoklasse des jeweiligen KI-Systems ab, sondern auch von der Rolle der handelnden Akteure (Provider bzw. Anbieter vs. Deployer bzw. Betreiber). Während die Anbieter von Hochrisiko-KI-Systemen das volle Pflichtenprogramm erfüllen müssen, ist die Regelungstiefe für Betreiber deutlich geringer. Allerdings können Betreiber ungewollt zu Anbietern werden, indem sie z.B. wesentliche Änderungen an einem durch einen Dritten entwickelten Hochrisiko-KI-System vornehmen. Aus Anwendersicht dürfte es daher in vielen Fällen darum gehen, diesen Rollenwechsel durch eine geeignete Ausgestaltung der Vertragsbeziehung zum Anbieter möglichst zu vermeiden.

Regulatorischer Rahmen von Data Act und AI Act

Der räumliche Anwendungsbereich von Data Act und AI Act ist weit: Alle Unternehmen, die auf dem EU-Markt tätig sind oder am Datenaustausch mit EU-Partnern teilnehmen, sind betroffen. Das in beiden Gesetzen verankerte Marktortprinzip erfasst somit auch nicht-europäische Unternehmen, die IoT-Produkte, verbundene Dienste oder KI-Systeme in der EU anbieten.

Die Durchsetzung des Data Act und die Überwachung seiner Einhaltung werden durch nationale Behörden in den jeweiligen Mitgliedstaaten sichergestellt. In Deutschland sollen hierfür die Datenschutzaufsichtsbehörden zuständig sein. Bei Verstößen gegen Vorschriften des Data Act drohen Sanktionen, die auf die DSGVO-Mechanismen verweisen (bis zu 20 Millionen € oder 4 % des weltweiten Jahresumsatzes).

Der AI Act verfolgt eine ähnliche Herangehensweise: Jeder EU-Mitgliedstaat muss eine nationale Aufsichtsbehörde benennen, welche die Umsetzung des AI Act überwacht. Der AI Act sieht ebenfalls einen Bußgeldrahmen vor: Verstöße gegen verbotene KI-Praktiken können mit bis zu 35 Millionen € oder 7 % des gesamten weltweiten Jahresumsatzes geahndet werden. Andere Verstöße können Bußgelder bis zu 15 Millionen € oder 3 % des gesamten weltweiten Jahresumsatzes nach sich ziehen.

Der Umgang mit Data Act und AI Act

Unternehmen müssen ihre Daten-Assets in Zukunft noch sorgfältiger als bisher ordnen: Welcher Bereich hat welche Daten, wie sind diese erfasst, geordnet, gesichert, strukturierbar und für Dritte ohne Verstöße gegen Datenschutz, Geschäftsgeheimnisschutz oder sonstige Vorgaben zugänglich?

Auf Basis einer solchen Data Governance Struktur wird es vielen Unternehmen gleichzeitig leichter fallen, die oben bereits angedeuteten Vermeidungsstrategien zu prüfen, z.B. in Bezug auf Datenzugangsansprüche aus dem Data Act durch entsprechende Ausgestaltung der vernetzten Produkte und Datenverarbeitungsvorgänge. Ähnliches gilt für Anbieter und Betreiber von KI-Systemen, die z.B. eine Einstufung als Hochrisiko-KI oder einen Wechsel in die Anbieter-Rolle vermeiden wollen. Hierfür, aber auch zur Ausschöpfung der mit den neuen Rechtsakten verbundenen Potentiale (z.B. Entwicklung neuer Geschäftsmodelle), gilt es, frühzeitig Juristen mit technischem Sachverstand an einen Tisch mit den Entwicklern und den Business Developern zu bringen, um gemeinsam entsprechende Konzepte, Geschäfts- und Vertragsmodelle zu entwickeln. ■

Impact Assessment: Relevanz für die eigene Organisation prüfen.

Zum Data Act Quick-Check:

Zum AI-Data Act Quick-Check:

KERNAUSSAGEN

- Der Data Act fordert eine Datenordnung von Unternehmen, die IoT-Daten oder -Dienste nutzen („Data Governance").
- Der Data Act ermöglicht durch das Recht auf Datenzugang neue Datengeschäftsmodelle z.B. für Start-ups, die bisher keinen Zugang zu proprietären Datenbeständen hatten.
- Die Vertragsparteien von Cloud-Verträgen müssen sich darauf einstellen, dass Cloud-Switching per Gesetz einfach und kurzfristig möglich sein wird und die Amortisation von Investitionen über vertragliche Mindestlaufzeiten schwieriger wird.
- Wer KI im Unternehmen einsetzt, muss sorgfältig abklären, in welche Risikoklasse sein System fällt und ob der Anbieter seinen Pflichten nachkommt.
- Wer KI von Dritten nutzt, kann ungewollt selbst zum Anbieter werden.
- Die EU setzt ihren Weg der Digitalregulierung mit unverminderter Intensität fort. Große Teile davon sind als Compliance-relevante Vorgaben zu verstehen und müssen organisatorisch und wie auch haftungsvermeidend entsprechend präzise umgesetzt werden.