

Regulierungsflut im Rahmen

Datenverkehr. Im Februar 2020 hat die EU-Kommission ihre Digitalstrategie „Gestaltung der digitalen Zukunft Europas“ veröffentlicht. Umfassende wertebasierte Digitalreformen in einem einheitlichen Rechtsrahmen sollen die EU fit für den globalen Wettbewerb machen. Dieses ehrgeizige Vorhaben bringt eine Vielzahl von neuen Regulierungen mit sich. Die Wichtigsten sollen in diesem Artikel von Rechtsanwalt Georg Huber von der Kanzlei Greiter, Pegger, Kofler & Partner kurz vorgestellt werden.



Die Digitalwirtschaft unterlag bislang nur relativ wenigen regulatorischen Vorgaben. Die EU will nun einen einheitlichen Rahmen für einen europäischen Datenmarkt und Datenaustausch zur breiteren Nutzung von Daten schaffen und so die Wertschöpfung erhöhen. Gleichzeitig sollen Verbraucherrechte gestärkt und die Marktmacht der großen Konzerne wie Google, Amazon oder Facebook begrenzt werden.

Die DSGVO soll weitgehend unberührt bleiben, wenngleich sich in der Praxis zahlreiche Überschneidungen und (ungelöste) Abgrenzungsfragen ergeben werden.

Angesicht der Vielzahl und der Komplexität der neuen Vorschriften verliert man leicht den Überblick. Vor allem für KMUs wird es vermutlich schwierig, künftig rechtskonform zu agieren.

Im Folgenden werden überblicksartig die wichtigsten neuen Rechtsakte vorgestellt.

1. Digital Market Act (DMA)

Der DMA soll die Marktmacht der großen digitalen Plattformen wie Google, Amazon, Facebook oder Apple („Gatekeeper“) beschränken.

Gatekeepern werden verschiedene Verpflichtungen und Verbote auferlegt. Amazon darf zB eigene Produkte und Dienstleistungen auf seinem Marketplace nicht mehr bevorzugen und muss Händlern den Zugriff auf jene Daten ermöglichen, die sie auf der Plattform generieren.

Verstöße können Bußgelder bis zu 10% des Jahresumsatzes (im Wiederholungsfall 20%) oder tägliche Zwangsgelder in Höhe von 5% des durchschnittlichen Tagesumsatzes nach sich ziehen.

Der DMA wurde am 5. Juli 2022 vom EU-Parla-

ment verabschiedet. Vermutlich noch im Herbst wird auch der Rat formell zustimmen.

2. Digital Services Act (DSA)

Mit dem DSA soll der Onlinehandel neu geregelt werden. Einheitliche Regeln für digitale Vermittlungsdienste (wie etwa Online-Plattformen) sollen zu einem sicheren, vorhersehbaren und vertrauenswürdigen Online-Umfeld beitragen.

Der DSA unterscheidet dabei nach Größe: Kleinunternehmen unterliegen etwa im Vergleich zu großen Online-Plattformen nur geringen Verpflichtungen.

Online-Vermittler müssen illegale Inhalte wie hate speech oder Gewaltaufrufe, feststellen und beseitigen (Sperrung oder dauerhafte oder vorübergehende Sperre eines Nutzer-Accounts, etc) oder einfache Beschwerdemodelle für Nutzer

der EU-Digitalstrategie

einrichten. Sehr große Plattformen müssen dafür auch ein Risikomanagement betreiben, um „systemische Risiken“ zu minimieren und verhindern (z.B. die Gefährdung demokratischer Prozesse).

Bei Online-Werbung muss erkennbar sein, dass es sich um Werbung handelt, in wessen Namen sie angezeigt wird und nach welchen Kriterien jene Nutzer ausgewählt werden, denen die Werbung angezeigt wird.

Zur Durchsetzung der Ansprüche haben die Mitgliedsstaaten Koordinationsstellen einzurichten und Bußgelder bis zu 6% des Jahresumsatzes sowie Zwangsgelder bis zu 5% des durchschnittlichen Tagesumsatzes vorzusehen.

Der DSA wurde ebenso wie der DMA am 5. Juli 2022 vom EU-Parlament verabschiedet und tritt nach Zustimmung durch den Rat vermutlich noch im Herbst in Kraft.

3. Data Act (DA)

Das Herzstück der Digitalstrategie stellt wohl der Data Act dar. Er soll 2024 in Kraft treten und gilt für alle Branchen und Wirtschaftsbereiche.

Hintergrund des DA ist der Umstand, dass eine Vielzahl maschinengenerierter Daten (Stichwort: internet of things), wirtschaftlich weitgehend ungenutzt sind. Dieser „Datenschatz“ soll gehoben werden.

Derzeit haben oft nur Hersteller Zugang zu Daten, die über ihre Produkte generiert werden. Der Data Act soll für eine gerechtere Verteilung der Wertschöpfung bei der Verwertung von nicht personenbezogenen Daten sorgen. Private und gewerbliche Nutzer sollen daher ein Recht auf Zugang zu und Weitergabe von solchen Daten erhalten.

Der Data Act trifft nach derzeitigem Stand folgende wesentlichen Grundaussagen (Auswahl):

- Der Dateninhaber (also in der Regel der Hersteller) darf vom Nutzer generierte maschinenbezogene Daten nur mit dessen Einwilligung nutzen.
- Dem Nutzer sind die von ihm generierten Daten in Echtzeit zur Verfügung zu stellen.
- Dritten darf die Nutzung nur erlaubt werden, wenn der Nutzer zustimmt.
- Öffentliche Stellen dürfen bei außergewöhnlichen Ereignissen (z.B. Pandemie) auf die Daten zugreifen.
- Unfaire Klauseln in Lizenzverträgen über die Nutzung der Daten sind unzulässig.

Der Data Act wirft viele Fragen auf, etwa wie Geschäftsgeheimnisse geschützt sind und wie er sich zur DSGVO hin abgrenzt. Nach der DSGVO dürfen nämlich personenbezogene Daten nicht ohne weiteres Dritten zur Verfügung gestellt

werden. Die Abgrenzung, welche Daten personenbezogen sind und welche nicht, ist aber äußerst komplex. Die Lösung dieser Frage könnte für Unternehmen eine Wahl zwischen Cholerea und Pest bedeuten, da sowohl Verstöße nach der DSGVO als auch dem Data Act mit Bußgeldern bis zu 20 Millionen Euro oder 4% des weltweiten Unternehmensumsatzes sanktioniert werden. Es bleibt zu hoffen, dass im weiteren Diskussionsprozess Anpassungen und Entschärfungen vorgenommen werden.

4. Data Governance Act (DGA)

Begleitend zum Data Act soll der DGA Grundlagen für den Datenaustausch über verschiedene Branchen sowie über Ländergrenzen hinweg fördern. Er ist am 24. Juni 2022 in Kraft getreten und gilt ab 23. September 2023.

Er zielt darauf ab, die Verfügbarkeit von Daten zur wirtschaftlichen Nutzung, gemeinsamen Verwendung und für Forschungszwecke zu erhöhen, um datengestützte Innovationen, zB künstliche Intelligenz, zu fördern und dadurch die Wettbewerbsfähigkeit der europäischen Datenwirtschaft zu stärken. Ein echter europäischer Markt für Daten soll entstehen.

Der DGA regelt vor diesem Hintergrund, dass öffentliche Stellen bestimmte Kategorien von Daten zur Weiterverwendung, zB für Forschungszwecke im Gesundheitsbereich, freigeben können.

Allerdings soll die DSGVO Vorrang genießen, wenn personenbezogene Daten betroffen sind. Die Privatsphäre darf daher nicht beeinträchtigt werden, wenn der öffentliche Sektor Daten freigibt. Bei einer Freigabe werden daher vor allem technische Lösungen wie eine Anonymisierung erforderlich sein.

Ein weiterer zentraler Regelungspunkt des DGA sind Datenvermittler. Da Daten für die Weiterverwendung bereitgestellt werden sollen, werden viele Unternehmen Datenmissbrauch befürchten. Für Datenvermittler werden daher besondere Regeln, etwa eine Anmeldepflicht und eine Überwachung durch Behörden, eingeführt.

Der dritte Eckpfeiler des DGA sind sogenannte „Datenspenden“ (Datenaltruismus). Dabei geht es darum, dass Daten für nicht kommerzielle Zwecke unentgeltlich zur Verfügung gestellt werden, damit sie der Gesellschaft zu Gute kommen. Bürger könnten etwa mit eigenen Sensoren erhobene Daten über Lärm, Luftverschmutzung etc. der Allgemeinheit zur Verfügung stellen.

Der DGA will die Verfügbarkeit von Daten in der EU erhöhen sowie vertrauenswürdige Strukturen auf dem Datenmarkt schaffen. Der Data Act hingegen soll das wirtschaftliche Potential von Daten für Wirtschaftstreibende nutzbar machen.

Aus beiden lässt sich das Bestreben herauslesen, Datenmonopolen gegenzusteuern und einen offenen und fairen Zugang zum Datenmarkt zu gewährleisten.

5. Artificial Intelligence Act (AI Act)

Die im April 2021 präsentierte AI Act verfolgt das Ziel, einen gesetzlichen Rahmen für den transparenten und sicheren Einsatz von künstlicher Intelligenz zu schaffen. Man könnte ihn als eine Art „Produktsicherheitsgesetz“ für künstliche Intelligenz betrachten.

Der AI Act verfolgt einen risikobasierten Ansatz, das heißt, er unterscheidet zwischen verschiedenen Risikostufen von KI-Systemen. Der AI Act verbietet zB generell den Einsatz von KI-Systemen bei „unannehbaren Risiken“.

Verboten ist etwa der Einsatz von KI im Zusammenhang mit staatlichen Praktiken der Bewertung sozialen Verhaltens (social scoring) oder für Techniken, die das Bewusstsein unterschwellig beeinflussen.

KI-Systeme mit hohem (aber nicht unannehmbarem) Risiko müssen für die Marktzulassung strenge Anforderungen erfüllen, während bei geringem Risiko in der Regel nur Transparenzpflichten zu erfüllen sind (z.B. Information des Nutzers, dass er über einen Bot mit einem KI-System kommuniziert).

Bei Verstößen sieht der Entwurf des AI Acts Bußgelder von bis zu 30 Millionen Euro bzw. 6% des weltweiten Jahresumsatzes vor.

7. Cyber Resilience Act

Mit dem Mitte September 2022 präsentieren Cyber Resilience Act sollen neue Sicherheitsanforderungen für vernetzte Hard- und Softwareprodukte etabliert werden. Hersteller müssen dafür sorgen, dass Produkte mit digitalen Elementen Anforderungen zur Cybersicherheit erfüllen.

Die Pflichten beinhalten etwa die Berücksichtigung der Cybersicherheit bereits beim Design und der Entwicklung, Dokumentations- und Meldepflichten und die Bereitstellung von Sicherheits-Updates.

Der Entwurf der Kommission wird in einem nächsten Schritt vom Rat und dem EU-Parlament geprüft.

Zum Autor:

Dr. Georg Huber, LL.M., CIPP/E
ist Rechtsanwalt bei Greiter Pegger Kofler & Partner in Innsbruck.



Nähere Infos unter www.lawfirm.at