IT-Recht 2023: Viele neue EU-Regeln

IT-Recht 2023: Viele neue EU-Regeln

Im kommenden Jahr muss sich die IT-Welt mit etlichen neuen rechtlichen Regulierungen auseinandersetzen, viele davon auf EU-Ebene. Unter anderem sollen die Internetgiganten stärker an die Leine genommen werden. Aber auch kleine Unternehmen müssen handeln.
Im kommenden Jahr muss sich die IT-Welt mit etlichen neuen rechtlichen Regulierungen auseinandersetzen, viele davon auf EU-Ebene. Unter anderem sollen die Internetgiganten stärker an die Leine genommen werden. Aber auch kleine Unternehmen müssen handeln.

Es gibt einen Grund, warum auf EU-Ebene derzeit viele Gesetzgebungsvorhaben im IT-Bereich forciert werden: die im Frühjahr 2024 anstehende Europawahl. Insbesondere die EU-Kommission möchte bis dahin möglichst alle ihre in der Agenda „Priorities 2019 – 2024 – A Europe fit for the digital age“

gesetzten Ziele erreichen. Die Amtszeit der derzeitigen Kommission endet mit der Legislaturperiode des Europäischen Parlaments. Anschließend wird eine neue EU-Kommission gebildet, die sich dann eine neue IT-Rechts-Agenda geben dürfte.

2023 werden zunächst zahlreiche EU-Gesetze in Kraft treten, die bereits im Jahr 2022 beschlossen wurden. Hierzu zählt der **Digital Markets Act (DMA),** der am 1. November 2022 in Kraft getreten und ab dem 2. Mai 2023 wirksam ist. Er sieht vor, dass es auf Plattformen der Gatekeeper im Internet fair zugeht, wie es auf einer Webseite der EU-Kommission heißt. Anhand objektiver Kriterien wird festgestellt, ob es sich bei einer Onlineplattform um einen solchen Gatekeeper handelt. Relevant sind dabei insbesondere die wirtschaftliche Position und die Nutzerzahlen.

Der DMA sieht vor, dass Gatekeeper künftig diskriminierungsfrei ihre Plattformen für den Absatz von Waren und Dienstleistungen durch Dritte zur Verfügung stellen müssen. Dies gilt auch für die dabei von Nutzern auf der Plattform hinterlassenen Daten. Eigene Waren und Dienstleistungen darf der Gatekeeper dabei nicht bevorzugen, auch darf er Nutzer nicht vom Deinstallieren von Apps abhalten. Außerhalb der Plattform darf er Nutzer nicht ohne deren Einwilligung bewerben. Die Bußgelder können bis zu 20 Prozent des weltweiten Jahresumsatzes betragen.

Länderübergreifende Dienste

Beim **Digital Services Act (DSA)** hat sich die EU auf eine längere Frist zwischen dem Inkrafttreten am 16. November 2022 und dem Wirksamwerden am 17. Februar 2024 verständigt. Hintergrund hierfür sind die zahlreichen und teils tiefgreifenden Vorgaben für sehr viele Unternehmen, die Leistungen rund um das oder im Internet anbieten. Im Wesentlichen geht es bei der Regulierung darum, Verbraucher und ihre Grundrechte besser zu schützen, einen einheitlichen

Rechtsrahmen zu schaffen und – vor allem auch für kleinere Serviceanbieter, KMU oder Start-ups – den Zugang zu EU-weiten Märkten zu vereinfachen. Nicht zuletzt liegt ein Schwerpunkt des DSA auf der Minderung systemimmanenter Risiken wie Manipulation oder Desinformation (siehe ix.de/zqe9).

Neben den üblichen Folgen bei Rechtsverstößen wie wettbewerbsrechtlichen Abmahnungen, einstweiligen Verfügungen und dergleichen sieht der DSA Bußgelder von bis zu sechs Prozent des weltweiten Jahresumsatzes des Anbieters vor. Betroffen vom DSA sind „vermittelnde Online-Dienste“. Hierzu zählen Vermittlungsdienste mit einem eigenen Infrastrukturnetz, etwa Internetanbieter, DNS-Registrierstellen und Hosting-Dienste im Bereich Cloud und Webhosting. Erfasst sind des Weiteren Onlineplattformen wie Onlinemarktplätze, App-Stores oder Social-Media-Plattformen. Der DSA sieht in den Regelungen zum Anwendungsbereich keine Ausnahmen für nicht kommerzielle Anbieter vor. Also dürften Mastodon und gegebenenfalls auch Wikipedia unter den Anwendungsbereich fallen.

Die betroffenen Unternehmen sind gut beraten, das Jahr 2023 zur Vorbereitung zu nutzen. Es gilt, die Compliance mit dem DSA zu schaffen, die AGB anzupassen und womöglich auch die angebotenen Leistungen selbst [1].

Der DSA wird in Fachkreisen auch als „Biest“ bezeichnet, denn die Vorgaben sind sehr weitreichend. Neben Tech-Giganten dürften beispielsweise auch einzelne geschäftliche WLAN-Betreiber betroffen sein. Mit Abmahnungen bei DSA-Verstößen ist ab Februar 2024 zu rechnen. Diese Abmahnwelle könnte deutlich größere Ausmaße annehmen als die derzeitige bei der Verwendung dynamischer Google-Fonts.

Kryptoregulierung verspätet sich

Eigentlich sollte die Verordnung **Markets in Crypto-Assets (MiCA)** bereits 2022 verabschiedet werden und in Kraft treten.

Überraschend vertagte das EU-Parlament die Beschlussfassung jedoch auf 2023. Inhaltlich bestand weitgehend Einigkeit zwischen EU-Rat, -Kommission und -Parlament. MiCA regelt die „digitale Darstellung eines Wertes oder eines Rechts, das elektronisch transferiert und gespeichert werden kann“, wenn dafür „die Distributed-Ledger-Technologie oder eine vergleichbare Technologie verwendet“ wird. Non-Fungible Tokens (NFT) sind nach derzeitigem Stand als Ergebnis längerer Diskussionen auf Gesetzgebungsebene nicht von der Verordnung betroffen. Die Verordnung ist Teil des EU-Pakets zur Digitalisierung des Finanzwesens.

Die MiCA-Verordnung soll EU-weit Krypto-Assets regulieren. Sie nimmt Emittenten und Dienstleister in den Fokus. Neben dem Anlegerschutz durch Transparenz- und Offenlegungspflichten stehen unter anderem die Verhinderung von Marktmissbrauch und Geldwäsche im Raum. Für zahlreiche Dienstleistungen wird zukünftig die Erlaubnis der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) erforderlich sein. Die Anforderungen ähneln denen an Finanzinstitute.

Kryptodienstleister müssen ihren Sitz und mindestens einen Geschäftsleiter in der EU haben. Sie müssen die BaFin über das Unternehmen sowie dessen Gesellschafter und Geschäftsleiter umfassend informieren. Die Geschäftsleiter müssen zudem fachlich geeignet und zuverlässig, die Geschäftsorganisation muss ordnungsgemäß und angemessen sein. Maßnahmen gegen Geldwäsche und die ausreichende Organisation der Compliance sind ebenso vorgeschrieben wie ein professionelles Beschwerdemanagement und die Pflicht, eigene Vermögenswerte von denen der Kunden zu trennen.

Sichere Standards für vernetzte Produkte

Am 15. September 2022 hat die EU-Kommission einen ersten Entwurf für einen **Cyber Resilience Act (CRA)** vorgestellt, der nun durch das Gesetzgebungsverfahren und die Abstimmungen zwischen EU-Kommission, -Rat und -Parlament läuft. Das Gesetz

soll gemeinsame Cybersicherheitsstandards für vernetzte Geräte und Dienste („Produkte mit digitalen Anteilen“) festlegen und damit spürbar zur Bekämpfung von Cyberkriminalität beitragen. Mit seiner Verabschiedung ist 2023 zu rechnen, 24 Monate nach Inkrafttreten wird es wirksam. Auf Hersteller solcher Produkte kommt aber bereits nach 12 Monaten eine Berichtspflicht zu, wenn in einem Produkt mit digitalen Elementen eine aktiv ausgenutzte Sicherheitslücke auftritt.

Die geplanten Regelungen reichen von der Pflicht von Herstellern und Dienstleistern, ein angemessenes Niveau an Cybersicherheit einzuhalten, bis hin zum Verkaufsverbot für Produkte mit bekannten Schwachstellen. Produkte sollen nur noch in Verkehr gebracht werden, wenn sie im Sinne von Security by Default konfiguriert sind. Zudem müssen Angriffsflächen und mögliche Auswirkungen von Attacken systemseitig begrenzt sein.

Für kritische Produkte sollen zwei Kategorien eingeführt werden. Die Anforderungen an die Compliance mit den CRA-Vorgaben sollen für Hersteller von Desktop- und Mobilgeräten, virtualisierten Betriebssystemen, Ausstellern digitaler Zertifikate, Allzweck-Mikroprozessoren, Kartenlesegeräten, Robotersensoren, intelligenten Zählern und IoT-Geräten jeglicher Art, Routern und Firewalls für den industriellen Einsatz deutlich höher sein als für andere Produkte mit digitalen Inhalten. Der CRA-Entwurf sieht Bußgelder bis 15 Millionen Euro beziehungsweise 2,5 Prozent des weltweiten Jahresumsatzes vor. In ersten Stellungnahmen warnen Branchenvertreter davor, kleine und mittlere Unternehmen durch allzu hohe und kostspielige Sicherheitsanforderungen vom Markt auszuschließen.

Auf Finanzunternehmen kommen bereits 2023 im Bereich Cybersicherheit zahlreiche Hausaufgaben zu. Am 10. November 2022 hat das EU-Parlament den **Digital Operational Resilience Act (DORA)** verabschiedet. Ziel ist es, bestehende Standards für die Cybersicherheit zu vereinheitlichen. Das soll die

digitale Betriebsstabilität von EU-Finanzunternehmen gewährleisten. Geplant ist ein detailliertes und umfassendes Rahmenwerk. DORA soll nach einer Umsetzungsfrist von zwei Jahren wirksam werden. Die Vorgaben gelten damit zum Jahreswechsel 2024/2025 (zu DORA siehe separaten Artikel ab Seite 92).

Lange erwartet: die NIS2-Richtlinie

Knapp zwei Jahre nach dem Kommissionsvorschlag hat ebenfalls im November 2022 das EU-Parlament der NIS2-Richtlinie zugestimmt. Die noch ausstehende Zustimmung durch die EU-Staaten gilt in Fachkreisen als Formsache. **NIS2** steht für die überarbeitete zweite Fassung der 2016 verabschiedeten **Directive on Security of Network and Information Systems.** Richtlinien sind anders als Verordnungen oder Acts durch die EU-Mitgliedsstaaten in nationales Recht umzusetzen. Ihr Ziel ist die Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

Geplant ist, durch NIS2 den Anwendungsbereich der bisherigen NIS1-Richtlinie drastisch auszuweiten. Unternehmen mit mehr als 50 Mitarbeitern und einem Jahresumsatz von mehr als 10 Millionen Euro sollen künftig unter NIS2 fallen, wenn sie in einem kritischen Sektor tätig sind. Auch die Auflistung, was als kritischer Sektor einzustufen ist, soll signifikant erweitert werden. Danach fallen künftig etwa auch Hersteller von Medizingeräten, Labore, Cloud-Provider, Rechenzentren und Content-Delivery-Netzwerke darunter. Zum etwas schwächer regulierten „wichtigen Sektor“ zählen künftig der gesamte industrielle Sektor, Hersteller von Computern sowie die Branchen Maschinenbau und Mobility.

Die von vielen lange ersehnte NIS2-Richtlinie weitet den Geltungsbereich ihres Vorgängers erheblich aus. Zahlreiche weitere Branchen gelten nun als „kritischer Sektor“.
Betroffene Unternehmen müssen Risikoanalyse- und Sicherheitskonzepte für die Informationssysteme, die Bewältigung von Zwischenfällen, die Offenlegung von Schwachstellen sowie die Gewährleistung der Sicherheit in der Lieferkette schaffen. Die Aufsichtsmaßnahmen und Durchsetzungsanforderungen der nationalen Behörden sollen strenger gefasst werden. Der Bußgeldrahmen soll 10 Millionen Euro oder bis zu zwei Prozent des weltweiten Jahresumsatzes umfassen.

Binnen 18 Monaten nach Inkrafttreten sollen die Mitgliedsstaaten die NIS2-Richtlinie umgesetzt haben. Betroffene Unternehmen müssen sich also auf erheblich verschärfte Vorgaben in puncto Cybersicherheit ab 2024 oder spätestens 2025 einstellen. Angesichts des Mangels an Fachkräften in diesem Bereich und des benötigten Vorlaufs für eine Compliance mit den NIS2-Vorgaben müssen sich die Verantwortlichen in Unternehmen spätestens ab 2023 mit der konkreten Umsetzung beschäftigen. Auf Betreiber kritischer Infrastrukturen kommt am 1. Mai 2023 auf jeden Fall eine bereits beschlossene Pflicht nach dem BSI-Gesetz zu. Sie sind

dann verpflichtet, Systeme zur Angriffserkennung zu verwenden.

Ein weiteres Großprojekt der EU ist der **Artificial Intelligence Act (AI Act).** Nachdem die EU-Kommission bereits im April 2021 einen ersten Gesetzentwurf vorgelegt hat, fand erst im Oktober 2022 die erste Plenarsitzung des EU-Parlaments dazu statt. Ein Grund für die lange Dauer des Verfahrens dürften die über 3000 Änderungsvorschläge sein, mit denen sich das Parlament bei der Regulierung des Einsatzes von künstlicher Intelligenz befassen muss. Die EU beabsichtigt mit dem AI Act einen einheitlichen Rechtsrahmen für vertrauenswürdige KI-Systeme zu schaffen sowie einheitliche Regeln für die Entwicklung, Vermarktung und Verwendung von KI innerhalb der EU im Einklang mit ihren Werten und den Grundrechten.

Schwieriges Ringen um Kompromisse

In Details ist der AI Act sehr umstritten. Der Anwendungsbereich, aber auch der Einsatz biometrischer Erkennungssysteme und ihr potenzieller Missbrauch stehen neben anderen Aspekten im Mittelpunkt der Diskussion. Ein Kompromissvorschlag sieht vor, Behörden in Drittstaaten vom AI Act auszunehmen, wenn sie künstliche Intelligenz im Rahmen von Vereinbarungen über internationale oder justizielle Zusammenarbeit verwenden und ein Angemessenheitsbeschluss der EU-Kommission nach der DSGVO vorliegt. Ausnahmen wird es sicher für die militärische Nutzung und womöglich auch für Forschung und Entwicklung geben. Der EU-Rat fordert zudem eine Beschränkung des Anwendungsbereichs auf maschinelles Lernen.

Angst vor kollektiver biometrischer Überwachung

Strittig ist, welche Ausnahmen es für das pauschale Verbot von Echtzeit-Fernerkennungssystemen zur biometrischen Identifizierung von Personen im öffentlichen Raum geben soll.

Einige EU-Parlamentarier haben Sorge, dass die Zulassung der Identifizierung von Entführungsopfern und Kriminellen sowie zur Abwehr von unmittelbar drohenden Terroranschlägen zur Überwachung der Gesellschaft quasi durch die Hintertür führen kann. Vereinzelte Forderungen sehen vor, das Verbot auch auf den privaten Bereich auszudehnen und auch durch Streichung des „Echtzeit-Erfordernisses“ eine nachträgliche Identifizierung zu untersagen.

Der AI Act wird einen risikobasierten Regelungsansatz verfolgen. KI-Systeme sollen in die vier Kategorien minimales, geringes, hohes oder unannehmbares Risiko eingestuft werden. Im unteren Bereich stehen Transparenzanforderungen und sektorale Regulierungen im Raum. Erfasst werden beispielsweise Systeme, die mit Menschen interagieren oder Emotionen anhand biometrischer Daten erkennen, sowie Systeme, die Inhalte erzeugen oder manipulieren. Unter Letzteres würden auch Deepfakes, also realistisch wirkende Medieninhalte fallen, die durch KI-Systeme geändert oder verfälscht wurden.

Für KI-Systeme mit hohem Risiko sind hohe Anforderungen an das Risikomanagement, die Datenqualität und die technische Dokumentation vorgesehen. Eine hochrangige Expertengruppe soll hierfür Mindestanforderungen gemäß definierten Ethik-Leitlinien festlegen. Diskutiert wird darüber hinaus eine Konformitätsbewertung, die vor Einsatz des betreffenden KI-Systems positiv ausfallen muss.

Als unannehmbar riskante KI-Systeme werden die genannten biometrischen Systeme zur Fernidentifizierung, aber auch Social Scoring durch Behörden (wie bereits in China praktiziert) sowie manipulative Systeme mittels Techniken der unterschwelligen Beeinflussung Schutzbedürftiger eingestuft. Für sie ist ein generelles Verbot vorgesehen. Verstöße gegen den AI Act sollen durch beträchtliche Bußgelder geahndet werden. Diskutiert wird über einen Rahmen von bis zu 30 Millionen Euro oder sechs Prozent des weltweiten Jahresumsatzes.

US-EU-Datenschutz, die Dritte!

Was noch? Spannend wird sein, ob die EU-Kommission aller Kritik zum Trotz im Frühjahr 2023 einen sogenannten Angemessenheitsbeschluss gemäß Artikel 45 der Datenschutz-Grundverordnung fassen wird, der dem Datenschutz in den USA „ein angemessenes Schutzniveau“ bescheinigt. Seit der Europäische Gerichtshof in seinem viel beachteten Schrems-II-Urteil den **EU-US Privacy Shield** kassiert hat, ist die Übermittlung personenbezogener Daten aus der EU in die USA deutlich erschwert.

Im Oktober 2022 hatte US-Präsident Biden eine Executive Order unterzeichnet, mit der ein angemessenes Datenschutzniveau aus EU-Sicht geschaffen werden soll. Zahlreiche Datenschützer wie der scheidende Landesdatenschutzbeauftragte Baden-Württembergs Stefan Brink, aber auch der Datenschutzaktivist Max Schrems zweifeln daran, dass die Executive Order ausreicht. Der EuGH dürfte erneut mit der Rechtslage befasst werden. Ein Ende der Gemengelage ist nicht absehbar.

Ungeachtet dessen dürften die von Unternehmen getroffenen Maßnahmen und Verträge auch weiterhin nicht den Bestimmungen der DSVGO entsprechen. Seit Ende 2022 gelten neue Vorgaben für die Standardvertragsklauseln. Sie sind derzeit eine der wenigen Möglichkeiten, den Datentransfer in die USA rechtskonform auszugestalten. Die Datenschutzbehörden dürften 2023 mit einer Durchsetzung der Änderungen beginnen und gegebenenfalls signifikante Bußgelder verhängen.

Um die in den letzten Jahren heftig diskutierte **E-Privacy-Verordnung** ist es zuletzt sehr ruhig geworden. Sie soll die DSGVO ergänzen und weiter gehende Rahmenbedingungen für den Umgang mit personenbezogenen Daten im Bereich der elektronischen Kommunikation schaffen. In erster Linie soll es Regelungen etwa zu Cookies oder Trackern geben. Diskutiert werden auch Vorgaben für Direktmarketing und Teilnehmerverzeichnisse. Ob die Verordnung nun endlich 2023

das Licht der Welt erblicken wird, ist allerdings mehr als fraglich. Aber selbst wenn, dürfte sie nicht vor 2025 wirksam werden.

Weniger wegwerfen, mehr reparieren

Mitte November 2022 haben sich die EU-Mitgliedsstaaten und die EU-Kommission auf neue **Ecodesign-Vorgaben** geeinigt. Sie sollen 2023 formal verabschiedet und nach einer Umsetzungsfrist von 21 Monaten wirksam werden. Eingeführt werden soll ein **Recht auf Reparatur.** Hersteller von Smartphones, Tablets und Co. müssen danach Reparaturanleitungen und für die Dauer von sieben Jahren bestimmte Ersatzteile wie Displays und Batterien verfügbar halten. Software-Updates müssen fünf Jahre lang bereitgestellt werden. Sie dürfen die Geräteperformance nicht beeinträchtigen. Schließlich sollen die Rechte von Dienstleistern gestärkt werden, die Gerätereparaturen anbieten.

2023 dürfte die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) eine neue Fassung ihres Rundschreibens **Mindestanforderungen an das Risikomanagement (MaRisk)** veröffentlichen. Es wird die derzeit gültige Fassung dieses Rundschreibens vom August 2021 ersetzen. Aus IT-Sicht interessant sind die Diskussionen rund um IT-Sicherheit und IT-Zugang zu Handelsplattformen aus dem Homeoffice. Infolge der Coronapandemie haben zahlreiche Finanzdienstleister gefordert, den strengen Ansatz aufzuweichen, dass beispielsweise ihr Aktienhandel nur „in Geschäftsräumen“ stattfinden darf. Letztlich haben Änderungen in der MaRisk zahlreiche Auswirkungen auf die im Finanzwesen eingesetzten IT-Systeme. Relevant ist hier auch das 2021 überarbeitete Rundschreiben **Bankaufsichtsrechtliche Anforderungen an die IT,** kurz **BAIT,** das die MaRisk konkretisiert. Womöglich steht auch dieses 2023 zur Überarbeitung an.

Weitergehen dürfte es 2023 auch mit den Vorbereitungen für einen **European Chips Act,** der die Wettbewerbsfähigkeit und

Resilienz der Chipindustrie in der EU signifikant stärken soll. Am 24. September 2023 wird zudem der **Data Governance Act (DGA)** wirksam, der am 23. September 2022 in Kraft trat. Sein Ziel ist die Schaffung eines erleichterten Rahmens für die gemeinsame Nutzung von Daten. Ein europäisches Datenaustauschmodell soll zur Förderung der künstlichen Intelligenz einen Datenaustausch zwischen verschiedenen Branchen über Ländergrenzen hinweg ermöglichen. Bürger sollen ihre personenbezogenen Daten für bestimmte Zwecke spenden können. Zudem soll der Zugang zu Daten der öffentlichen Hand erleichtert werden. Datenvermittlungsdienste müssen in einem Register aufgeführt sein, damit interessierte Bürger sich von deren Vertrauenswürdigkeit überzeugen können.

Weiter voranschreiten dürfte 2023 auch die CSAM-Verordnung, die die EU-Kommission im Mai 2022 vorgelegt hat. **CSAM** steht für **Child Sexual Abuse Material,** also Kinderpornografie. Hosting- und Kommunikationsanbieter sollen danach Risikoeinschätzungen vornehmen und Maßnahmen zur Risikoreduzierung treffen. Sie werden dabei überwacht durch nationale Aufsichtsbehörden, denen besondere Befugnisse etwa in Bezug auf die Sicherstellung und Sperrung entsprechender Inhalte zustehen sollen.

Zu erwartende Neuerungen im IT-Recht 2023			
Kürzel	Name	in Kraft ab/seit	wirksam ab
AI Act	Artificial Intelligence Act	voraussichtlich 2023, spätestens 2024 (auch ein Scheitern ist nicht auszuschließen)	voraussichtlich nicht vor 2025, nach aktuellem Stand 24 Monate nach Inkrafttreten

Zu erwartende Neuerungen im IT-Recht 2023			
Kürzel	Name	in Kraft ab/seit	wirksam ab
CRA	Cyber Resilience Act	2023	24 Monate nach Inkrafttreten; einige erste Pflichten jedoch bereits 12 Monate nach Inkrafttreten
CSAM	„Child Sexual Abuse Material“-Verordnung	voraussichtlich 2023	voraussichtlich 6 Monate Umsetzungsfrist ab Inkrafttreten
DGA	Data Governance Act	23. September 2022	24. September 2024
DMA	Digital Markets Act	1. November 2022	2. Mai 2023
DORA	Digital Operational Resilience Act	verabschiedet am 10. November 2022; Inkrafttreten 20 Tage nach Veröffentlichung im EU-Amtsblatt	Jahreswechsel 2024/2025
DSA	Digital Services Act	16. November 2022	17. Februar 2024
	Ecodesign-Vorgaben, „Recht auf Reparatur“	2023	21 Monate Umsetzungsfrist ab Inkrafttreten
ECA	European Chips Act	voraussichtlich 2023	noch in Diskussion
ePVO	E-Privacy-Verordnung	eventuell 2023	nicht vor 2025

Zu erwartende Neuerungen im IT-Recht 2023			
Kürzel	Name	in Kraft ab/seit	wirksam ab
	EU-US Privacy Shield 2.0	eventuell 2023	
LksG	Lieferkettengesetz	1. Januar 2023	mit Inkrafttreten
MaRisk; BAIT	Mindestanforderungen an das Risikomanagement; Bankaufsichtsrechtliche Anforderungen an die IT	voraussichtlich 2023	
MiCA	Markets in Crypto-Assets	2023	18 Monate nach Inkrafttreten; voraussichtlich 2024
NIS2	Directive on Security of Network and Information Systems	voraussichtlich 2023, benötigt noch Zustimmung der EU-Staaten	voraussichtlich 2024, spätestens 2025

Abuse-Material: finden, löschen, berichten

Verfahren und Techniken zum Aufspüren kinderpornografischer Inhalte sollen bestimmten Vorgaben entsprechen, so datenschutzfreundlich und so wenig fehleranfällig wie möglich sein. Weitere Vorgaben soll ein noch zu schaffendes EU Centre on Child Sexual Abuse (EU Centre) veröffentlichen. Zusätzlich gibt es für die verantwortlichen Unternehmen Berichtspflichten. Sie müssen entsprechende Inhalte löschen oder den Zugang zu ihnen effektiv unterbinden, wenn die Inhalte außerhalb der EU gehostet werden. Die Aufsichtsbehörden können Anordnungen treffen, denen unverzüglich Folge zu leisten ist.

App-Stores werden verpflichtet, den Download von Apps zu verhindern, die Kinder „einem hohen Risiko der Anwerbung […] aussetzen können“. Das EU Centre steht dabei den Dienstanbietern, den einzelstaatlichen Ermittlungsbehörden sowie Europol, den EU-Mitgliedsstaaten und den Opfern beratend und unterstützend zur Seite. Wann die CSAM-Richtlinie verabschiedet werden wird, ist offen. Zuletzt hatten sich der Europäische Datenschutzbeauftragte und der Europäische Datenschutzausschuss kritisch geäußert. Sie werten die geplanten Regelungen als nicht vereinbar mit der Datenschutz-Grundverordnung und den freiheitlichen Grundrechten. Die emotionale Diskussion wird 2023 fortgesetzt werden.

Ab 1. Januar 2023 gilt das **Lieferkettengesetz,** zunächst für Unternehmen mit mehr als 3000 und ab 2024 auch für Unternehmen mit weniger als 1000 Beschäftigten. Es gilt zwar nicht ausschließlich für die IT-Branche, allerdings versprechen sich Marktbeobachter dort ein Umsatzwachstum, geht es doch um Automatisierung, Platform as a Service, Supply-Chain-Management sowie Blockchain-Technologien. Ungeachtet der gesetzlichen Vorgaben dürfte die Diskussion um Diversifizierung der Beschaffung von Produkten, Rohstoffen und dergleichen auch 2023 anhalten.

Fazit

Aus IT-rechtlicher Sicht wird es das Jahr 2023 in sich haben. Die EU ist sehr umtriebig und wird zahlreiche Gesetzesvorhaben umsetzen. Auf Unternehmen aller Branchen kommen zahlreiche neue Vorgaben zu, etwa bei der Cybersicherheit. Einige der Gesetzeswerke werden erst in den Jahren 2024 oder 2025 greifen. Zur Vorbereitung bleibt Unternehmen dennoch wenig Zeit. Denn ab Wirksamwerden der verschärften Vorgaben greifen signifikante Bußgelder nach dem Vorbild der Datenschutz-Grundverordnung. In manchen Fällen drohen auch Abmahnungen durch Verbände und Konkurrenten.

Ein Neujahrswunsch vieler betroffener Unternehmen für 2023

dürfte allerdings nicht in Erfüllung gehen: Es steht nicht zu erwarten, dass es vor der Europawahl 2024 noch zu einer Überarbeitung und Änderung der Datenschutz-Grundverordnung kommen wird. Hoffen darf man aber auf einen EU-US Privacy Shield 2.0 für die rechtssichere Übermittlung personenbezogener Daten in die USA. Hierzu wie auch in anderen Bereichen wird es auch im kommenden Jahr interessante und bedeutsame Gerichtsurteile geben, nicht zuletzt des Europäischen Gerichtshofs. Prosit 2023! (ur@ix.de)

1. Quellen
2. Tobias Haar; EU will digitale Märkte regulieren; iX 9/2022, S. 80
3. Die im Text angesprochenen Gesetzesvorhaben sind über ix.de/zqe9 zu finden.

Tobias Haar

ist Rechtsanwalt mit Schwerpunkt IT-Recht bei Vogel & Partner in Karlsruhe. Er hat zudem Rechtsinformatik studiert und hält einen MBA.