Deutsches Whistleblower-Gesetz tritt in Kraft

Ein neues Gesetz soll Hinweisgeber vor Repressalien und Vergeltungsmaßnahmen schützen. Es verpflichtet außerdem Unternehmen, technische Systeme und Prozesse für solche Hinweise einzuführen.

Mehr lesen …

KI-Regulierung nimmt international Konturen an

Die Grundlagen des europäischen KI-Gesetzes stehen, in Einzelfragen dürften die verantwortlichen EU-Gremien in nächster Zeit noch nachjustieren.

Mehr lesen …

Einheitsstrafen DSGVO

Neue europäische Regeln für DSGVO-Bußgelder

Erstmals haben sich die europäischen Datenschutzbehörden auf gemeinsame Grundsätze geeinigt, nach denen Bußgelder zu verhängen sind. Diese lassen den Behörden in den einzelnen Ländern aber nach wie vor große Spielräume.

Von Joerg Heidrich

Link zu den EDSA-Guidelines: ct.de/yfyw

Mehr lesen …

Google Analytics 4 & DSGVO: Ihre Datenschutz-Checkliste für die Umstellung am 1. Juli 2023

Ab dem 1. Juli 2023 stellt Google seinen Dienst Google Analytics dauerhaft auf die neue Version "Google Analytics 4" (kurz "GA4") um. Mit dieser Änderung kommen nicht nur technische, sondern auch rechtliche Veränderungen auf Nutzer von Google Analytics zu.

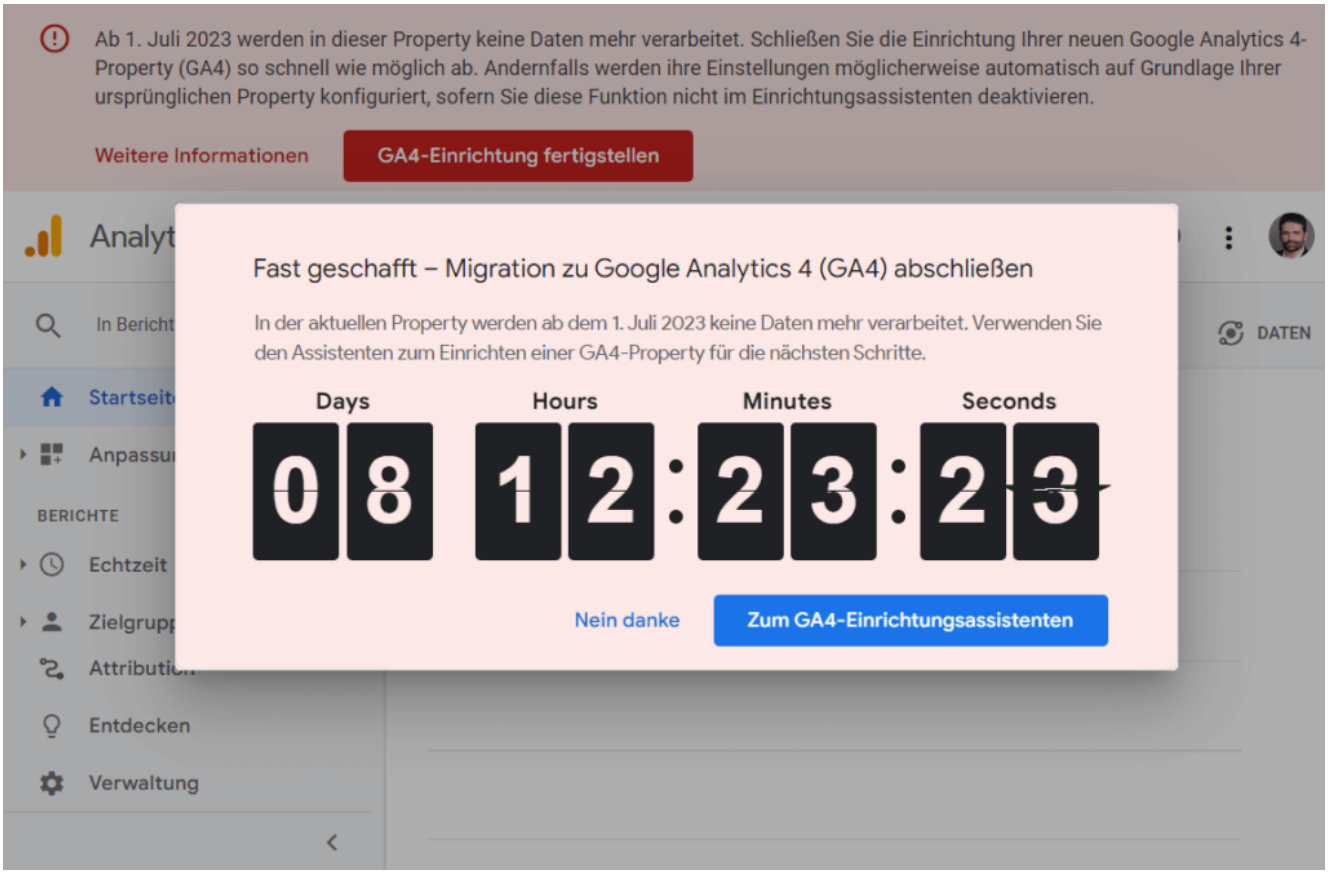
In diesem Beitrag erfahren Sie, was sich datenschutzrechtlich ändert, ob und wie Sie Google Analytics 4 einsetzen dürfen. Am Ende des Beitrags erhalten Sie eine Checkliste mit den wichtigsten Prüfpunkten vor dem Einsatz von Google Analytics 4.

Wie erfolgt die Umstellung auf Google Analytics 4?

Sollten Sie bisher noch keine eigenen Schritte zur Umstellung unternommen haben, so hat Google bereits im März 2023 automatisch Google Analytics 4 für Sie eingerichtet, basierend auf Ihren bisherigen Einstellungen und Zielen für Universal

Analytics.

Bis Ende Juni 2023 haben Sie noch die Möglichkeit, Daten in der alten Version (Universal Analytics) zu sammeln und zu nutzen. Danach beginnt eine Übergangszeit von sechs Monaten, in der Sie auf alte Daten zugreifen können. Ab dann müssen Sie Google Analytics 4 einsetzen.



Was ist technisch neu an Google Analytics 4?

Universal Analytics und Analytics 4 sind beide Versionen von Googles Analysetool, jedoch mit technischen Unterschieden.

Universal Analytics fokussiert sich auf Sitzungen und Nutzerinteraktionen auf einzelnen Geräten. Im Gegensatz dazu konzentriert sich Analytics 4 auf die Nachverfolgung von Nutzern über verschiedene Geräte hinweg und ermöglicht eine detailliertere Erfassung des Nutzerverhaltens durch sogenannte “Events”, was tiefergehende Einblicke in ihr Verhalten bietet.

Kurzum, Analytics 4 ist die neuere Version, die detailliertere und geräteübergreifende Daten liefert. Umgekehrt hat Google aber auch die Datenschutzaspekte verbessert.

Versionsbezeichnung: In der Praxis verwendet man die Versionsbezeichnungen selten, sondern spricht schlicht von “Google Analytics”. Ab Juli 2023 ist damit automatisch Google Analytics 4 gemeint.

Ist Google Analytics 4 datenschutzrechtlich sicherer?

Google Analytics 4 erleichtert zwar die Nachverfolgung des Nutzerverhaltens, bietet aber zugleich neue Datenschutzfunktionen:

- **Cookie-los:** Mit Google Analytics 4 können Tracking-Verfahren eingerichtet werden, die ohne Cookies auskommen.
- **Serverseitiges Tracking:** Nutzerdaten können auf dem eigenen Server pseudonymisiert werden, bevor sie an Google übermittelt werden.
- **Standort EU:** Google zufolge werden alle Daten von Endgeräten in der EU auf Servern innerhalb der EU gespeichert und verarbeitet.
- **IP-Kürzung in der EU:** Im Gegensatz zu Universal Analytics erfolgt die Kürzung der IP-Adressen der Nutzer auf EU-Servern von Google. Das bedeutet, dass ein entsprechend pseudonymer Datensatz in die USA übermittelt wird.
- **Kürzere Aufbewahrungsfristen:** Im Gegensatz zur bisherigen Standardlöschfrist von 26 Monaten bei Universal Analytics erlaubt GA4 keine längere Aufbewahrung als 14 Monate für Daten.
- **Google Signals:** Durch die Deaktivierung von Google Signals kann die Verknüpfung mit einem Google-Konto

verhindert werden.
- **Geo- und Geräteinformationen:** Die Genauigkeit der gesammelten Geo- und Geräteinformationen kann angepasst werden.

Die genannten Maßnahmen tragen zur Verbesserung des Datenschutzniveaus bei der Verwendung von Google Analytics 4 bei. Beachten Sie jedoch, dass die Nutzung von Google Analytics damit nicht automatisch zulässig und rechtssicher wird.

EU-Vorschriften zu mehr Cybersicherheit

Die Europäische Union bringt im Rahmen ihrer Digitalstrategie zwei wichtige Gesetze auf den Weg: den Cyber Resilience Act (CRA) sowie die sogenannte NIS2-Richtlinie.Da wir immer digitaler werden, muss auch immer mehr Wert auf Onlinesicherheit, oder wie es auf Neudeutsch heißt, Cybersecurity, gelegt werden.

Die EU-Kommission hat am 15. September 2022 einen Entwurf des CRA vorgeschlagen, der noch vom europäischen Parlament und vom Rat angenommen werden muss.

Recht auf Updates durch den CRA

Mit dem CRA werden erhöhte Sicherheitspflichten auf Hersteller, Vertreiber, Importeure und Händler von IT-Produkten zukommen. Dazu zählen insbesondere geplante Meldepflicht für aktiv ausgenutzte Schwachstellen und Sicherheitsvorfälle. Durch die Vorgaben des CRA sollen

sicherere Hardware- und Softwareprodukte gewährleistet werden.

Zu den dabei erfassten Produkten zählt jedes Software- oder Hardwareprodukt sowie seine Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die separat in Verkehr gebracht werden. Er ist anwendbar auf „Produkte mit digitalen Elementen“, also auf solche Produkte, die ohne ihre digitalen Elemente nicht sinnvoll genutzt werden können (z. B. Smartphones). Der CRA teilt die Produkte mit digitalen Elementen in drei Kategorien ein:

- Standardkategorie
- kritische Klasse I
- kritische Klasse II

In die Standardkategorie fallen voraussichtlich gut 90 Prozent aller Produkte, wie z. B. Textverarbeitung, Fotobearbeitung oder Festplatten. Zum CRA gehören verschiedene Anhänge. Darin, nämlich in Anhang III, werden die kritischen Produkte mit digitalen Elementen der Klassen I und II aufgeführt. Zur kritischen Klasse I zählen u. a. Software für Identitätsmanagementsysteme, Browser, Passwortmanager, Antivirensoftware, VPN-Lösungen, Netzwerkmanagementsysteme, Werkzeuge zur Verwaltung der Netzwerkkonfiguration, Systeme zur Überwachung des Netzwerkverkehrs, Verwaltung von Netzwerkressourcen, Systeme zur Verwaltung von Sicherheitsinformationen und -ereignissen (SIEM), Update-/Patch-Verwaltung (einschließlich Bootmanager), Systeme zur Verwaltung der Anwenderkonfiguration, Software zur Verwaltung mobiler Geräte, Firewalls, Router/Modems, Anwenderspezifische integrierte Schaltungen (ASIC) oder auch Industrielle Automatisierungs- und Steuerungssysteme (IACS). Zur kritischen Klasse II zählen hingegen insbesondere Betriebssysteme für Server, Desktops und mobile Geräte, Infrastrukturen für öffentliche Schlüssel und Aussteller digitaler Zertifikate, Hardwaresicherheitsmodule (HSM), sichere Kryptoprozessoren,

Smartcards, Smartcard-Lesegeräte und Token oder auch Geräte des industriellen Internets der Dinge.

Folgende Pflichten sollen zukünftig auf die vom Anwendungsbereich des CRA erfassten Unternehmen zukommen:

- Berücksichtigung der Cybersicherheit schon in der Planungs-, Entwurfs- und Entwicklungsphase sowie auch in der Produktions-, Liefer- und Wartungsphase („Security by Design“)
- umfangreiche Dokumentationspflichten in Bezug auf Cybersicherheitsrisiken
- Meldepflicht für aktiv ausgenutzte Schwachstellen und Vorfälle
- Überwachungs- und Beseitigungspflichten von Schwachstellen während der erwarteten Produktlebensdauer (max. fünf Jahre)
- Pflicht zur Lieferung von klaren und verständlichen Gebrauchsanweisungen
- Pflicht zur Bereitstellung von bestimmten Pflichtinformationen (u. a. Name, Anschrift und Kontaktdaten des Herstellers, Typen-, Chargen-, Versions- bzw. Seriennummer, Verwendungszweck, Art der technischen Sicherheitsunterstützung, die der Hersteller anbietet, sowie der Zeitpunkt, bis zu dem sie geleistet wird)
- Pflicht zur Bereitstellung von Sicherheitsupdates für jedenfalls fünf Jahre

Ganz konkret und unabhängig von der jeweiligen Kategorie müssen Produkte mit digitalen Elementen zudem immer einer Risikobewertung unterzogen werden.

Unter die Produkte mit digitalen Elementen im Sinne des CRA fallen jedoch weder „Produkte mit digitalen Inhalten“ noch „digitale Produkte“. Die Erstgenannten zeichnen sich dadurch aus, dass der digitale Teil des Produkts für dessen

Funktionsfähigkeit nicht von zentraler Bedeutung ist (z. B. Kühlschrank mit Bestellfunktion via App). Bei den „digitalen Produkten“ handelt es sich um rein digitale Produkte (z. B. Apps oder Musikdateien). Der CRA hat folglich einen sehr weit gefassten Anwendungsbereich, von dem nur ein paar spezifische Produktkategorien ausgenommen werden, wie beispielsweise Medizinprodukte. Software, die als Dienstleistung angeboten wird, also Software-as-a-Service-bzw. Cloudleistungen, wird ebenfalls gesondert geregelt.

Sichere Infrastrukturen durch NIS2

Speziell auf den Bereich der sogenannten kritischen Infrastruktur (KRITIS) zielt die NIS2-Richtlinie ab. Es geht also um den besseren Schutz von Stromversorgung, Wasserwerken oder Telekommunikationsleitungen. Es soll ein Höchstmaß an Ausfallsicherheit gewährleistet werden, um beispielweise Strom-Blackouts oder Störungen der Trinkwasserversorgung für die Bevölkerung möglichst zu vermeiden oder jedenfalls so schnell und gut wie möglich auf derartige Störungen reagieren zu können.

In Deutschland ist mit Blick auf den KRITIS-Sektor bereits 2015 das IT-Sicherheitsgesetz (IT-SiG) in Kraft getreten. Darin war auch eine Änderung des damaligen § 13 Telemediengesetz (TMG) enthalten, der in einem Absatz 7 die Pflicht für alle Websitebetreiber zur Absicherung ihrer Websites mit sich brachte (z. B. durch Verschlüsselung nach dem Stand der Technik per SSL-/TLS-Zertifikat). Diese Norm findet sich nach der letzten Änderung des TMG nun in § 19 Abs. 4 des Telekommunikations-Telemedien-Datenschutz-Gesetzes (TTDSG). Seit Mai 2021 ist nunmehr das zweite IT-Sicherheitsgesetz (IT-SiG2) in Kraft, welches sowohl den Adressatenkreis als auch den Pflichtenkatalog der KRITIS-Betreiber merklich erweitert hat.

Aber auch auf EU-Ebene tut sich einiges. 2016 ist die

Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (kurz: NIS-Richtlinie) in Kraft getreten. Sie ist der europäische Rahmen für Cybersecurity im KRITIS-Bereich und soll ein hohes Sicherheitsniveau für Netzwerke und Informationssysteme sicherstellen.

Seit dem Jahr 2021 wird die NIS-Richtlinie überarbeitet. Ihr Nachfolger, die sogenannte NIS2-Richtlinie, soll den bestehenden Rechtsrahmen modernisieren, um die Herausforderungen des zunehmenden Grades an Digitalisierung und der stetig wachsenden Bedrohungen für die Cybersicherheit meistern zu können. Nach Inkrafttreten der NIS2-Richtlinie muss diese noch in das jeweilige nationale Recht der EU-Mitgliedsstaaten umgesetzt werden. In NIS2 wird zwischen kritischen und wichtigen Einrichtungen unterschieden:

- *Kritische Einrichtungen:* Energie (Strom, Fernwärme und Fernkälte, Erdöl, Erdgas und Wasserstoff); Verkehr (Luft, Schiene, Wasser und Straße); Bankenwesen; Finanzmarktinfrastrukturen; Gesundheitswesen; Herstellung pharmazeutischer Erzeugnisse (einschließlich Impfstoffe und kritischer Medizinprodukte); Trinkwasserversorgung; Abwasserwirtschaft; digitale Infrastrukturen (Internetknoten, DNS-Anbieter, Anbieter von Clouddienstleistungen, Anbieter von Rechenzentrumsdiensten, Netze zur Bereitstellung von Inhalten, öffentliche elektronische Kommunikationsnetze und elektronische Kommunikationsdienste,…); öffentliche Verwaltung; Weltraum.
- *Wichtige Einrichtungen:* Post- und Kurierdienste; Abfallwirtschaft; Chemikalien; Lebensmittel; Herstellung anderer Medizinprodukte, von Computern, Elektronik und Kraftfahrzeugen sowie Maschinenbau; Anbieter digitaler Dienste (Onlinemarktplätze, Onlinesuchmaschinen und

Plattformen der sozialen Netzwerke).

Sowohl die kritischen als auch die wichtigen Einrichtungen müssen u. a. folgende Cybersecurity-Maßnahmen treffen:

- Erlass und Umsetzung von Richtlinien für Risiken und Informationssicherheit
- Umsetzung von Maßnahmen zur Prävention, Detektion und Bewältigung von Cybersecurity-Vorfällen (Sicherheitspannen)
- Ergreifen von Maßnahmen zum Business Continuity Management (BCM) inkl. Backup- bzw. Krisenmanagement
- Gewährleistung der Sicherheit bei der Beschaffung von IT- und Netzwerksystemen
- Beachtung von Vorgaben für Kryptografie bzw. Verschlüsselung
- Umsetzung angemessener Maßnahmen zur Zugangskontrolle
- Einsatz sicherer Sprach-, Video- und Textkommunikation
- Einsatz gesicherter Notfallkommunikationssysteme

Durch die NIS2-Richtlinie wird der Aspekt der Cybersecurity zukünftig in der gesamten Lieferkette zu berücksichtigen sein. Außerdem sollen die Aufsicht und die Zusammenarbeit zwischen den Behörden und den von NIS2 betroffenen Betreibern innerhalb der EU vertieft werden. Die Sanktionen bei Verstößen gegen die NIS2-Vorgaben sollen durch die einzelnen EU-Mitgliedsstaaten selbst geregelt werden. Allerdings wird von Seiten des EU-Gesetzgebers bestimmt, dass die Sanktionen wirksam, verhältnismäßig und abschreckend sein müssen. Gegen kritische Einrichtungen sollen Geldbußen mit einem Höchstbetrag von mindestens 10 Mio. Euro oder von mindestens 2 Prozent des gesamten weltweit erzielten Vorjahresumsatzes verhängt werden können. Bei Sanktionen gegen wichtige Einrichtungen soll der Höchstbetrag mindestens 7 Mio. Euro oder 1,4 Prozent des Vorjahresumsatzes betragen.

Praxistipp

Neben dem CRA und NIS2 beinhaltet die Strategie der EU noch weitere Gesetze, die den Umgang mit digitalen Daten regeln sollen. Dazu zählen insbesondere der Data Governance Act (DGA) zur Förderung der Weiterverwendung von Daten des öffentlichen Sektors, der Digital Markets Act (DMA) und der Digital Services Act (DSA) zur Regulierung großer Onlineplattformen, der Artificial Intelligence Act (AIA) zur Regulierung von Künstlicher Intelligenz (KI) oder auch der Data Act (DA) zur besseren Weiterverwendung von Unternehmensdaten. Bei diesen Rechtsakten handelt es sich nicht um bloße Zukunftsmusik, denn der DMA ist bereits seit dem 1. November 2022 in Kraft. Der DGA wird ab dem 24. September 2023 anwendbar sein, der DSA bereits ab dem 2. Mai 2023.

Michael Rohrlich hat als Rechtsanwalt und Fachautor seinen Kanzleisitz in Würselen, Nähe Aachen. Seine beruflichen Schwerpunkte liegen auf dem Gebiet des Onlinerechts sowie des gewerblichen Rechtsschutzes. Weitere Infos zu den Themen aus den Rechtsbeiträgen sowie Gesetze und Gerichtsentscheidungen bietet er unter www.rechtssicher.info an.

DSGVO Neuigkeiten vom 09.04.2023

Das Landgericht Leipzig macht Quad9 zum Täter von Urheberrechtsverletzungen. Müssen DNS-Betreiber jetzt mit hohen Geld- oder Haftstrafen rechnen?

Markt + Trends | IT-Recht & Datenschutz

DNS-Server lösen Namen zu IP-Adressen auf und sind essenziell fürs Surfen. Wer nicht die Standard-Server der Provider nutzt, surft schneller und ohne Blockaden.

Durchsetzung der DSGVO soll EU-weit harmonisiert werden

Die EU-Kommission strebt eine verbesserte Rechtsdurchsetzung der Datenschutz-Grundverordnung an. Hierzu sollen die Verfahrensvorschriften zur DSGVO-Durchsetzung harmonisiert werden. Konkret soll es dabei um eine Verbesserung der Zusammenarbeit zwischen den Datenschutzbehörden der verschiedenen EU-Staaten gehen. Hinzukommen sollen die Festlegung von Verfahrensfristen, die Bereitstellung von Instrumenten und die Anforderungen an den Informationsaustausch. Zu guter Letzt sollen die Position der

Beschwerdeführer und der Betroffenen gestärkt werden.

Die geplanten Änderungen gehen unter anderem darauf zurück, dass die irische Datenschutzbehörde in der Kritik der anderen EU-Datenschutzbehörden steht. Der Vorwurf lautet auf einen zu nachgiebigen Umgang mit in Irland ansässigen internationalen Unternehmen, darunter Meta, Alphabet und Facebook. Die Beschwerden über zu niedrige Bußgelder oder eine zu lange Verfahrensdauer mehren sich. *Tobias Haar* (fo@ix.de)

Europäischer Datenschutzausschuss gibt grünes Licht für EU-US Data Privacy Framework

Mit Spannung wurde die Stellungnahme des Europäischen Datenschutzausschusses (EDSA) zum geplanten EU-US Data Privacy Framework erwartet. Doch sie fiel anders aus als von vielen Beobachtern erwartet: Zwar kritisiert der EDSA Einzelaspekte des Rahmens für die DSGVO-konforme Übermittlung von personenbezogenen Daten in die USA, die erwartete völlige Ablehnung blieb jedoch aus.

Eine formale Verabschiedung des Frameworks dürfte damit nur noch eine Frage der Zeit sein. Die Chancen auf dessen Bestand auch bei sich anschließenden Gerichtsverfahren sind damit ebenfalls gestiegen.

In seiner Stellungnahme betont der EDSA deutliche Verbesserungen unter anderem im Bereich der Rechtsbehelfe gegen Verstöße der US-amerikanischen Zusagen beim Datenschutz. Zu diesen Zusagen äußert sich beispielsweise der Bundesdatenschutzbeauftragte Ulrich Kelber: „Wir sehen den Willen, ein angemessenes Schutzniveau für Betroffene, deren personenbezogenen Daten an Unternehmen in die USA übermittelt werden, zu schaffen.“

Allerdings kommt es nach Auffassung des hamburgischen

Datenschutzbeauftragten Thomas Fuchs darauf an, wie diese Vorgaben sich in der Praxis bewähren. „Ob und inwiefern tatsächlich Geheimdienstaktivitäten auf ein verhältnismäßiges Maß reduziert werden und wirksamer Rechtsschutz gewährleistet ist, kann nur die Umsetzung in der Praxis zeigen“, so Fuchs. *Tobias Haar* (fo@ix.de)

Fragen des Urheberrechtsschutzes für KI-generierte Bilder

Unter Einsatz von künstlicher Intelligenz durch einen Computer generierte Bilder genießen keinen Schutz nach den Urheberrechtsgesetzen: Darauf hat das United States Copyright Office hingewiesen. In ihrer Einschätzung folgt die Behörde den urheberrechtlichen Vorschriften, die nur schöpferische Leistungen von Menschen erfassen. Auch hierzulande fallen nur „persönliche geistige Schöpfungen“ unter das Urheberrecht. Ob und wie KI-generierte Inhalte zukünftig geschützt werden sollen, diskutieren Juristen derzeit weltweit.

Andererseits können Bilder von KI-gestützten Generatoren urheberrechtlich geschützte Werke enthalten. Zu diesem Ergebnis kam eine Studie der Alphabet-Töchter Google und DeepMind, der University of California in Berkeley, der ETH Zürich sowie der Princeton University. Mit bestimmten Prompts konnten sie Kopien bestehender Werke als KI-Output erzeugen. Deren Nutzung könnte folglich zu einem Urheberrechtsverstoß führen. Denkbar ist dies auch bei textlichen oder sonstigen Ergebnissen von KI-Generatoren wie ChatGPT. *Tobias Haar* (fo@ix.de)

Onlinezugangsgesetz 2.0: Kritik an Gesetzesentwurf der Bundesregierung

Die Bundesregierung will die Digitalisierung der Verwaltung beschleunigen und hat einen Entwurf für eine Überarbeitung des

Onlinezugangsgesetzes vorgelegt. Ziel ist eine einfache, moderne und digitale Verfahrensabwicklung. Geplant sind etwa die Bereitstellung von zentralen Basisdiensten durch den Bund, wodurch landeseigene Entwicklungen für Bürgerkonto und Postfächer entfallen. Zudem soll der Ersatz der Schriftform durch elektronische Signaturen vorangetrieben werden. Auch auf Nutzerfreundlichkeit und Barrierefreiheit soll geachtet werden.

Der Gesetzesentwurf ist vielfach auf Kritik gestoßen. Der Bundesverband der Deutschen Industrie vermisst die Setzung von Standards und Schnittstellen für die digitale Verwaltung. Er fordert zudem eine „Ende-zu-Ende-Digitalisierungspflicht“, also eine rein digitale Verarbeitung von online gestellten Anträgen in den Behörden. Gefordert werden auch vom Bund zentral bereitgestellte Infrastrukturen wie Cloud-Betriebsplattformen oder Bezahlfunktionen. Kritisiert wird zudem, dass keine Umsetzungsfristen, sondern nun nur noch eine begleitende Evaluierung vorgesehen ist. *Tobias Haar* (fo@ix.de)

Kurz notiert

Das Gesetz zum **Schutz von Whistleblowern** ist vorerst gescheitert. Der Bundesrat hat das vom Bundestag im Dezember beschlossene Gesetz abgelehnt. Gegen Deutschland läuft ein Verfahren der EU-Kommission wegen der verspäteten Umsetzung der Whistleblower-Richtlinie.

Der Bundesdatenschutzbeauftragte hat der Bundesregierung den **Betrieb einer Facebook-Fanpage** untersagt. Nach derzeitiger Rechtslage ist die damit verbundene Datenübermittlung an Meta rechtswidrig, so die Begründung.

Ob **Cheat-Software für Computerspiele** gegen das Urheberrecht verstößt, soll nun der Europäische Gerichtshof klären. Der Bundesgerichtshof hat die für die Games-Branche wichtige Frage zur Entscheidung den EU-Kollegen vorgelegt.

Wer wegen Wettbewerbsverstößen zur Unterlassung bestimmter Inhalte auf Webseiten verpflichtet ist, ist nicht für Altversionen von **Webseiten in der Wayback Machine** verantwortlich. Das hat das Landgericht Karlsruhe entschieden.

Das Landgericht Ravensburg hat die **Entsperrung eines Mobiltelefons** per Fingerabdruck gegen den Willen eines Verdächtigen als rechtmäßig eingestuft.

Der in Kraft getretene **EU Digital Services Act** sieht eine Finanzierung der Aufsicht über sehr große Plattformen über Gebühren vor. Facebook und Co. werden dafür künftig mit bis zu 0,05 Prozent ihres weltweiten Jahresumsatzes zur Kasse gebeten.

DNS-Resolver Quad9 wegen Urheberrechtsverletzung verurteilt

Das Landgericht Leipzig macht Quad9 zum Täter von Urheberrechtsverletzungen. Müssen DNS-Betreiber jetzt mit hohen Geld- oder Haftstrafen rechnen?

Markt + Trends | IT-Recht & Datenschutz

DNS-Server lösen Namen zu IP-Adressen auf und sind essenziell fürs Surfen. Wer nicht die Standard-Server der Provider nutzt, surft schneller und ohne Blockaden.
Durch eine viel beachtete Entscheidung des Landgerichts Leipzig hat der nicht kommerzielle DNS-Resolver Quad9 erneut eine juristische Niederlage erlitten. Das Urteil erging auf eine Klage von Sony auf Sperrung des Zugangs zu Webseiten, auf denen sich urheberrechtswidrige Downloads befinden. Das Brisante an dem Urteil ist, dass Quad9 als Täter und nicht lediglich als Störer in die Verantwortung genommen wurde. Quad9 hat mit Unterstützung der Gesellschaft für Freiheitsrechte (GFF) Berufung gegen die Entscheidung angekündigt.

Der Rechtsstreit zwischen Sony und Quad9 läuft bereits seit 2021 und hatte seinen Anfang in einem einstweiligen

Verfügungsverfahren vor dem Landgericht Hamburg. Dort unterlag Quad9 in erster Instanz. Das Berufungsverfahren vor dem Hanseatischen Oberlandesgericht ist noch nicht abgeschlossen. Das jetzige Urteil des Landgerichts Leipzig erging im Hauptsacheverfahren. Dreh- und Angelpunkt der Rechtsstreitigkeiten ist, ob sich ein DNS-Resolver auf die Haftungsprivilegierungen für Zugangsprovider berufen kann.

Die Leipziger Richter lehnten es ab, Quad9 überhaupt als Zugangsprovider einzustufen. Daher griffen die allgemeinen urheberrechtlichen Bestimmungen. Durch die Auflösung von Namen in IP-Adressen greift damit eine Haftung als Täter, wenn sich hinter den IP-Adressen urheberrechtswidrige Inhalte zum Download befinden, so die Richter. Ein Rechtsgutachten der Bayreuther Juraprofessorin Ruth Janal kommt zu einem anderen Ergebnis. Danach sei ein offener DNS-Resolver von einer Urheberrechtsverletzung weiter entfernt als ein Zugangsprovider.

Das Urteil stößt auf Kritik und dürfte die Gerichte noch über Jahre hinweg beschäftigen. Moniert wird, dass damit die urheberrechtliche Haftung völlig neutraler Infrastrukturdienste wie Quad9 sogar strenger als die sozialer Netzwerke wäre. Zudem gelte nach dem jüngst in Kraft getretenen Digital Services Act die Haftungsprivilegierung für Internetzugangsanbieter eindeutig auch für DNS-Resolver. Quad9 will das Urteil anfechten. *Tobias Haar* (fo@ix.de)

NIS-2-Richtlinie

NIS-2-Richtlinie: Auftrag für KRITIS-Schutz

Mit den überarbeiteten Vorgaben an kritische Einrichtungen im Bereich der Cybersicherheit hat die EU auf die geänderte Gefahrenlage reagiert. Bis 2024 müssen die EU-Staaten ihr nationales Recht anpassen.

Von Tobias Haar

-tract

- Die NIS-2-Richtlinie löst ihre Vorgängerin ab, EU-Mitgliedsstaaten müssen sie bis 2024 in nationales Recht umsetzen.
- Die neue Richtlinie hat zwei Schwerpunkte: das Erschaffen nationaler Cybersicherheitsstrategien samt den dafür nötigen Institutionen sowie die verbesserte Kommunikation zwischen den Mitgliedsstaaten und den Sicherheitsbehörden.
- Die NIS-2-Richtlinie erweitert den Anwendungsbereich auf zusätzliche Sektoren und Unternehmen.
- Hierzulande dürfte die Umsetzung im Rahmen eines überarbeiteten IT-Sicherheitsgesetzes, dann in Version 3.0, erfolgen. Dies hatte der Koalitionsvertrag der Bundesregierung ohnehin vorgesehen.

Das Ziel der NIS-2-Richtlinie zum Schutz von Netzwerk- und Informationssystemen ist die Verbesserung der Resilienz und Reaktionsfähigkeit im Bereich der Cybersicherheit der öffentlichen und privaten Sektoren sowie der EU insgesamt. Sie löst die Vorgängerregelung NIS-1-Richtlinie aus dem Jahr 2016 ab. Im Text der NIS-2-Richtlinie wird der Vorgängerin eine große Rolle bei der Stärkung der Cyberresilienz bescheinigt, zudem habe sie in diesem Bereich ein „erhebliches Umdenken

bewirkt“. Zwischenzeitlich hätten sich allerdings „inhärente Mängel ergeben, die ein wirksames Vorgehen gegen aktuelle und neue Herausforderungen im Bereich Cybersicherheit verhindern“.

Bis zum 17. Oktober 2024 müssen EU-Mitgliedsstaaten die NIS-2-Richtlinie in nationales Recht umsetzen. So sieht es die „Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union … (NIS-2-Richtlinie)“ vor. Verordnungen, beispielsweise die Datenschutz-Grundverordnung (DSGVO), gelten im Gegensatz dazu unmittelbar nach Inkrafttreten für jeden Einzelnen und sind rechtlich verbindlich.

Artikel 1 der neuen NIS-2-Richtlinie beschreibt deren Ziele. In erster Linie gehe es darum, „nationale Cybersicherheitsstrategien zu verabschieden sowie zuständige nationale Behörden, Behörden für das Cyberkrisenmanagement, zentrale Anlaufstellen für Cybersicherheit und Computer-Notfallteams (CSIRT) zu benennen oder einzurichten“. Außerdem beschäftigt sie sich mit Regelungen zum Cybersicherheitsmanagement, einschließlich entsprechender Berichtspflichten, dem Austausch von Cybersicherheitsinformationen zwischen den EU-Staaten sowie mit der Art und Weise der Aufsicht in den einzelnen Mitgliedsstaaten. Sektorspezifische Spezialgesetze gehen ebenfalls aus der NIS-2-Richtlinie hervor.

Mehr Sektoren und Unternehmen betroffen

Die NIS-2-Richtlinie erweitert den Anwendungsbereich auf zusätzliche Sektoren und Unternehmen (siehe Abbildung). In Anhang I zur Richtlinie finden sich Auflistungen von „Sektoren mit hoher Kritikalität“ sowie „sonstige kritische Sektoren“. Zu ersteren zählen Unternehmen im Bereich Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, Verwaltung von IKT-Diensten, öffentliche Verwaltung und Weltraum. Zur zweiten

Gruppe zählen die Sektoren Post- und Kurierdienste, Abfallbewirtschaftung, Produktion, Umgang und Handel mit chemischen Stoffen oder Lebensmitteln, bestimmte Unternehmen im Bereich des verarbeitenden Gewerbes, Anbieter digitaler Dienste sowie Forschung.

Die NIS-2-Richtlinie weitet den Geltungsbereich ihrer Vorgängerin erheblich aus und deckt nun ebenfalls die rechts dargestellten Bereiche mit ab.
Unternehmen, die in mindestens einen der genannten Sektoren fallen, sind von der Richtlinie erfasst, wenn sie als „mittleres Unternehmen“ einzustufen sind. Das gilt für Firmen mit weniger als 250 Mitarbeitern und einem Jahresumsatz von unter 50 Millionen Euro beziehungsweise einer Jahresbilanz von unter 43 Millionen Euro. Ungeachtet ihrer Einstufung sind Anbieter öffentlicher Kommunikationsnetze und -dienste sowie Vertrauensdiensteanbieter und Namensregister der obersten Domäne einschließlich DNS-Diensteanbieter stets erfasst. Die Richtlinie führt weitere Kriterien für die Einstufung von Unternehmen als kritisch ein und erlaubt es den Mitgliedsstaaten, diese weiter zu verschärfen. So strebt sie für die gesamte EU eine „Mindestharmonisierung“ an.

Kapitel 2 der Richtlinie legt Vorgaben für einen „Koordinierten Rahmen für die Cybersicherheit“ fest. Dazu

zählt in erster Linie, dass sich jeder EU-Staat eine nationale Cybersicherheitsstrategie geben muss. Diese muss beispielsweise „die Bestimmung von Maßnahmen zur Gewährleistung der Vorsorge, Reaktionsfähigkeit und Wiederherstellung bei Sicherheitsvorfällen, einschließlich der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor“ umfassen.

Ein Schwerpunkt in dieser nationalen Cybersicherheitsstrategie liegt auf IKT-Produkten und -Diensten. Ein weiterer auf „der allgemeinen Verfügbarkeit, Integrität und Vertraulichkeit des öffentlichen Kerns des offenen Internets“. Risikomanagementmaßnahmen sollen stets weiterentwickelt und auf dem neuesten Stand eingesetzt werden.

Die EU-Staaten müssen für die Cybersicherheit zuständige Behörden schaffen und dies der EU-Kommission mitteilen. Über sie sollen grenzüberschreitende Abstimmungen erfolgen. Sie sollen über „angemessene Ressourcen“ verfügen, um ihre Aufgaben wirksam und effizient wahrnehmen zu können, um die Ziele der NIS-2-Richtlinie zu erreichen.

Nationale Notfallteams

Die NIS-2-Richtlinie sieht außerdem die Schaffung von Computer-Notfallteams (CSIRTs) vor und beschreibt ausführlich, welchen Anforderungen diese genügen müssen. Sie müssen über eine hohe Erreichbarkeit verfügen und dafür redundante Kommunikationskanäle unterhalten. Sie sind an sicheren Standorten einzurichten, ihre Datenverarbeitung muss sicher und ihre Bereitschaft jederzeit gewährleistet sein. Zu ihren Aufgaben zählen die Überwachung und Analyse von Cyberbedrohungen, die Ausgabe von Frühwarnungen und Alarmmeldungen sowie die Information über Cyberbedrohungen, die Reaktion auf Sicherheitsvorfälle, Lagebeurteilungen und Schwachstellenscans. Zudem soll es darüber im Rahmen des CSIRT-Netzwerks einen regelmäßigen Austausch geben.

Ein weiteres Ziel der Richtlinie ist es, die Zusammenarbeit zwischen den EU-Staaten im Bereich Cybersicherheit zu stärken. Eine Kooperationsgruppe soll beispielsweise Orientierungshilfen für die zuständigen Behörden ausarbeiten, den Austausch von Best Practices fördern, die EU-Kommission im Bereich der Cybersicherheit beraten oder den jeweils aktuellen Stand „in Bezug auf Cyberbedrohungen oder Sicherheitsvorfälle wie Ransomware“ beschreiben.

Die Abstimmung zwischen den EU-Staaten und ihren Behörden bildet einen klaren weiteren Schwerpunkt der NIS-2-Richtlinie. Zur Förderung einer raschen und wirksamen operativen Zusammenarbeit zwischen den CSIRTs soll ein Netzwerk entstehen. Darin geht es um Informationsaustausch, Technologietransfers und die gegenseitige Unterstützung. Über die Fortschritte beim Erreichen dieser Ziele sollen die Staaten regelmäßig berichten.

Des Weiteren werden die Aufgaben des Europäischen Netzwerks der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) weiter konkretisiert. Es koordiniert künftig Maßnahmen bei „Cybersicherheitsvorfällen großen Ausmaßes und Krisen auf operativer Ebene und zur Gewährleistung eines regelmäßigen Austauschs relevanter Informationen zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union“. Auch hier soll eine regelmäßige Evaluierung der geleisteten Arbeit erfolgen.

Die Richtlinie beschreibt schließlich Grundsätze der internationalen Zusammenarbeit im Bereich der Cybersicherheit, die Erstellung zweijährlicher Berichte über den Stand der Cybersicherheit in der EU und Peer-Reviews innerhalb des CSIRT-Netzwerks.

Vorgaben beim Risikomanagement

Umfassende Vorgaben ergeben sich aus der NIS-2-Richtlinie an die jeweiligen nationalen Gesetzgeber im Bereich der

Risikomanagementmaßnahmen. Dies beginnt mit Grundsätzen im Bereich der Governance. Leitungsorgane kritischer Einrichtungen müssen die ergriffenen Maßnahmen billigen, deren Umsetzung überwachen und für Verstöße verantwortlich gemacht werden können. Sie selbst müssen und ihre Mitarbeiter sollen regelmäßig an Schulungen teilnehmen, „um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben“.

Die Risikomanagementsysteme müssen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen umfassen. Damit möchte man die Risiken für die genutzten Netz- und Informationssysteme bei Sicherheitsvorfällen verhindern oder zumindest minimieren. Dabei sind der Stand der Technik sowie geltende Vorschriften einzuhalten und ein „gefahrenübergreifender Ansatz“ zu wählen (siehe Kasten).

Risikomanagementmaßnahmen

Folgende Punkte müssen Risikomanagementsysteme nach der NIS-2-Richtlinie im Bereich der Cybersicherheit nach Artikel 21 Absatz 2 umfassen:

a. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;
b. Bewältigung von Sicherheitsvorfällen;
c. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;
d. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;
e. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung

von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

f. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;
g. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
h. Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;
i. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und das Management von Anlagen;
j. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Bis 17. Oktober 2024 wird die EU-Kommission technische und methodische Anforderungen für die aufgelisteten Risikomanagementmaßnahmen erlassen. Diese gelten dann für „DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten, Anbieter von Onlinemarktplätzen, Onlinesuchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter“.

Die Richtlinie schlägt den EU-Staaten vor, erfassten Unternehmen und Behörden bei eigenentwickelten und -genutzten IKT-Produkten und -Diensten eine Zertifizierung gemäß den Schemata für Cybersicherheitszertifizierungen vorzuschreiben. Bei der Sicherheit von Netz- und Informationssystemen sollen zudem internationale Normen und technische Spezifikationen gefördert werden. Nicht in der EU ansässige von der NIS-2-Richtlinie erfasste Unternehmen müssen einen Vertreter innerhalb der EU benennen.

ENISA erstellt Register betroffener Einrichtungen

Die European Union Agency for Cybersecurity (ENISA) übernimmt die Aufgabe, ein EU-weites Register aller von der NIS-2-Richtlinie erfassten Einrichtungen im Bereich digitale Infrastruktur zu schaffen und zu pflegen, einschließlich Cloud-Anbieter, aber auch sozialer Netzwerke. Auf die Betreiber von TDL-Namensregistern und DNS-Registrierungsdienste sollen zusätzliche Pflichten zukommen. Sie müssen „genaue und vollständige Domänennamen-Registrierungsdaten in einer eigenen Datenbank im Einklang mit dem Datenschutzrecht der Union in Bezug auf personenbezogene Daten mit der gebotenen Sorgfalt sammeln und pflegen“.

Nationale Gesetze sollen es zusätzlich auch nicht von der Richtlinie erfassten Einrichtungen ermöglichen, „Informationen über Cyberbedrohungen, Beinahe-Vorfälle, Schwachstellen, Techniken und Verfahren, Kompromittierungsindikatoren, gegnerische Taktiken, bedrohungsspezifische Informationen, Cybersicherheitswarnungen und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten zur Aufdeckung von Cyberangriffen“ auszutauschen. Aus kartellrechtlichen Gründen soll dies aber nur gelten, wenn es für das Management von Sicherheitsvorfällen erforderlich ist und der Informationsaustausch das Cybersicherheitsniveau erhöht.

Schließlich umfasst die NIS-2-Richtlinie Anweisungen zur Aufsicht und Durchsetzung der Vorgaben. Der Katalog an Kompetenzen für die zuständigen Behörden ist lang. Er reicht von Vor-Ort-Kontrollen bei den betroffenen Einrichtungen über Sicherheitsscans bis hin zu Vorgaben für die Nachweise zur Umsetzung der Cybersicherheitskonzepte. Die betroffenen Einrichtungen sind zur umfassenden Mitwirkung zu verpflichten. Bei Rechtsverstößen sollen Warnungen und Handlungs- oder Unterlassungsanweisungen einschließlich Fristsetzungen möglich sein.

Bußgelder für Verstöße gegen die Vorgaben sollen „wirksam, verhältnismäßig und abschreckend“ sein. Bei Verstößen gegen die Pflichten im Bereich des Risikomanagements sollen Bußgelder für wesentliche Einrichtungen bei mindestens 10 Millionen Euro oder 2 Prozent des weltweiten Vorjahresumsatzes gedeckelt sein. Bei wichtigen Einrichtungen liegt die Grenze bei 7 Millionen Euro beziehungsweise 1,4 Prozent des weltweiten Vorjahresumsatzes.

EU-Maßnahmen-Portfolio

Die NIS-2-Richtlinie fügt sich in eine ganze Reihe von gesetzgeberischen Maßnahmen der EU ein. Sie ist Teil der „Gestaltung der digitalen Agenda Europas“, die sich die EU-Kommission 2020 als Vorhaben in ihrer Amtszeit bis zur Europawahl im Jahr 2024 gesetzt hat. Dazu gehören auch der derzeit diskutierte AI Act zur Regulierung des Einsatzes von künstlicher Intelligenz, der Cyber Resilience Act, der Digital Operational Resilience Act und weitere. Wegen der anstehenden Europawahl befinden sich zahlreiche Gesetzeswerke im Jahr 2023 auf der Zielgeraden (siehe „IT-Recht 2023: Viele neue EU-Regeln“ in iX 1/2023, S. 86).

Die NIS-2-Richtlinie adressiert die EU-Staaten, die die Vorgaben nun umsetzen müssen. Zahlreiche Regelungen beinhalten daher Aufforderungen wie „Die Mitgliedsstaaten stellen sicher …“ oder „Die Mitgliedstaaten können …“. In Deutschland dürfte es zu einer Überarbeitung des 2021 in Kraft getretenen IT-Sicherheitsgesetzes 2.0 kommen. Dies passt auch zur Vereinbarung im Koalitionsvertrag der Bundesregierung. Dort heißt es: „Die Cybersicherheitsstrategie und das IT-Sicherheitsrecht werden weiterentwickelt.“ Dort ist auch von „ehrgeiziger Cybersicherheitspolitik“ die Rede. Die Cybersicherheit bezeichnet der Koalitionsvertrag als „digitale Schlüsseltechnologie“.

Fazit

Mit der Umsetzung der NIS-2-Richtlinie will die EU ein hohes gemeinsames Cybersicherheitsniveau sicherstellen, „um so das Funktionieren des Binnenmarkts zu verbessern“. So lautet das übergreifende Ziel. Um das zu erreichen, hat die EU den Anwendungsbereich der Richtlinie und die Aufgaben der zuständigen Behörden wesentlich erweitert und neue Behörden geschaffen. Die Mitgliedsstaaten sollen sich zudem besser austauschen und die Überwachung verschärfen.

Die ausdrücklichen Regelungen zur persönlichen Verantwortlichkeit der Leitungsorgane und die gleichzeitig signifikant erhöhten Bußgeldrahmen dürften für Zündstoff sorgen. Die EU unterstreicht damit die große Bedeutung der Cybersicherheit und reagiert auf steigende Risiken. Das Thema bleibt spannend und ein Dauerbrenner. In der EU sind nun erst einmal wieder die einzelnen EU-Staaten an der Reihe. Von der Richtlinie erfasste Unternehmen tun aber gut daran, den Gesetzgebungsprozess zu beobachten und zu begleiten. Sich früh auf anstehende Änderungen einzustellen ist für sie eine kluge Strategie. (jvo@ix.de)

1. Quellen
2. Tobias Haar; IT-Recht 2023: Viele neue EU-Regeln; iX 1/2023, S. 86
3. NIS-2-Richtlinie online verfügbar unter ix.de/z3zm

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.

Kündigungsbutton: zahlreiche Abmahnungen

Kündigungsbutton: zahlreiche Abmahnungen

Seit Juli 2022 besteht eine Pflicht, Verbrauchern das Kündigen online abgeschlossener Verträge zu erleichtern. Die Verbraucherzentrale Bayern hat 840 Webseiten daraufhin untersucht und erhebliche Mängel festgestellt, die zu 154 Abmahnungen wegen Rechtsverstößen geführt haben. In einigen Fällen wird es zu Gerichtsverfahren kommen.

In zahlreichen Fällen war der vorgeschriebene Kündigungsbutton gar nicht vorhanden, in anderen Fällen war er versteckt und nicht wie gesetzlich gefordert „gut auffindbar“. Verstöße lagen auch gegen die Pflicht vor, eine gut lesbare Schaltfläche mit der Aufschrift „jetzt kündigen“ oder einer gleichwertigen Bezeichnung vorzuhalten. *Tobias Haar* (ur@ix.de)