Digital Services Act für Meta, X & Co.

Online-Riesen an der Leine

Die größten Plattformen und Suchmaschinen in Europa müssen sich seit Ende August den Regeln des Digital Services Act unterwerfen. Nutzer können seitdem beobachten, wie die US-Konzerne allmählich die Vorgaben zur Inhaltemoderation und Transparenz umsetzen.

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.

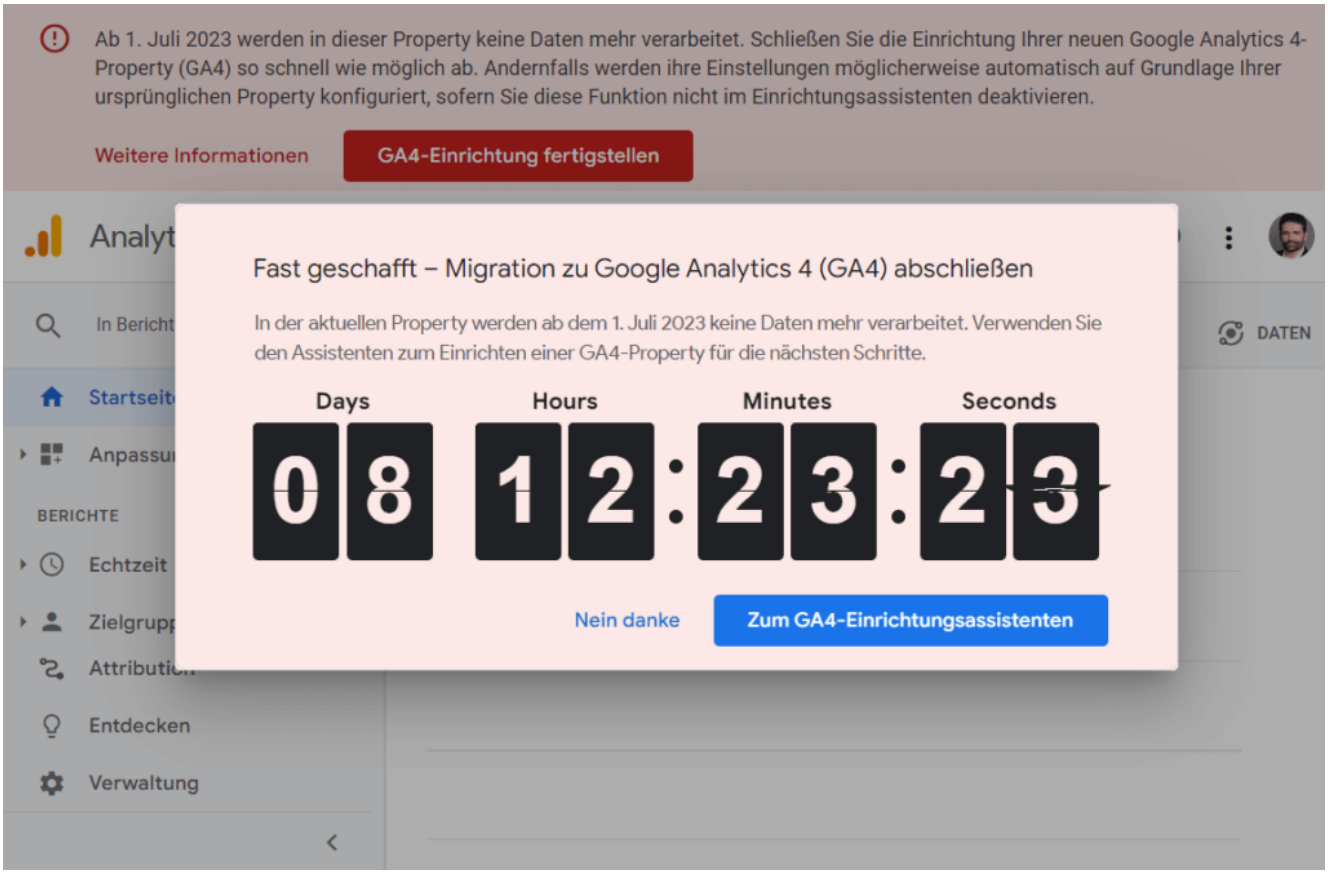
In diesem Beitrag erfahren Sie, was sich datenschutzrechtlich ändert, ob und wie Sie Google Analytics 4 einsetzen dürfen. Am Ende des Beitrags erhalten Sie eine Checkliste mit den wichtigsten Prüfpunkten vor dem Einsatz von Google Analytics 4.

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.

KI-Recht: ChatGPT, Bard und Co.

Über Risiken beim Einsatz von KI wird nicht erst seit ChatGPT diskutiert. Der geplante EU AI Act wird jedoch nicht alle Aspekte regeln.

Von Tobias Haar

-tract

- Die KI-Regulierung der EU soll noch 2023 kommen. Sie soll insbesondere Grundrechtsverletzungen bei Betroffenen verhindern, deren Daten unter KI-Einsatz verarbeitet werden.
- Der zugrunde liegende Ansatz ist risikobasiert und sieht für die verschiedenen Risikostufen daran angepasste Maßnahmen und Pflichten vor.
- Auch eine EU-Richtlinie für KI-Haftung ist in Vorbereitung. Sie soll Geschädigten die Beweislast erleichtern und sieht schon dann einen Anspruch auf Schadenersatz vor, wenn ein ursächlicher Zusammenhang des Schadens mit der KI nach vernünftigem Ermessen wahrscheinlich ist.

„Wir können also nicht wissen, ob uns die künstliche Intelligenz unendlich helfen wird, ob sie uns ignoriert und beiseiteschiebt oder ob sie uns möglicherweise zerstört.“ So äußerte sich bereits 2017 der berühmte Physiker Stephen Hawking. Der jüngste Hype um den Einsatz künstlicher Intelligenz als Chatbots in Suchmaschinen, namentlich ChatGPT in Microsofts Bing oder Bard bei Google, wirft ein Schlaglicht auf die aktuellen Entwicklungen im Bereich der KI. Zwar befindet sich die juristische Betrachtung dieser Phänomene noch am Anfang, erste Diskussionen werden aber bereits vehement geführt. Chatbots sind ein anschauliches Beispiel für den KI-Einsatz, um sich einigen wichtigen KI-Rechtsfragen zu nähern.

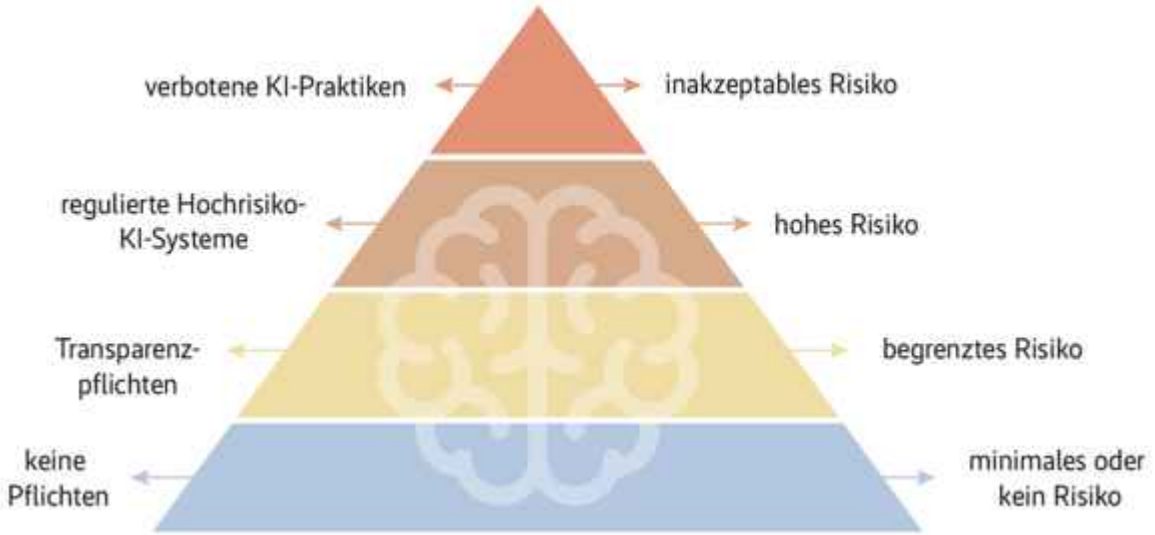
EU-Regulierung in den Startlöchern

Auf EU-Ebene wird derzeit am „Artificial Intelligence Act“, kurz AI Act, gearbeitet. Die Verordnung steht bereits kurz vor der abschließenden Abstimmung zwischen EU-Kommission, EU-Rat und EU-Parlament. Wie auch die Datenschutz-Grundverordnung wird sie nach Wirksamwerden in allen EU-Staaten unmittelbar

gelten, ohne dass es nationaler Umsetzungen bedarf. Mit einem Inkrafttreten ist noch 2023 zu rechnen, da den EU-Institutionen aufgrund der für 2024 anstehenden Europawahlen nicht mehr viel Zeit bleibt, ihre Agenda umzusetzen. Gelingt dies nicht, droht eine erhebliche Verzögerung der einheitlichen Regulierung von KI in der EU.

Die EU beschreibt das Spannungsfeld, in dem der AI Act regulierend eingreifen soll, wie folgt: „Der Ansatz der EU für künstliche Intelligenz konzentriert sich auf Exzellenz und Vertrauen, um die Forschungs- und Industriekapazitäten zu stärken und die Grundrechte zu gewährleisten.“ Seit zwei Jahren wird am Verordnungstext gefeilt. Über 3000 Änderungsanträge wurden eingereicht. Bereits die Definition von KI ist umstritten. Ein aktueller Vorschlag lautet, den Anwendungsbereich auf Systeme zu beschränken, „die durch maschinelle Lerntechniken und wissensbasierte Ansätze entwickelt wurden“.

Der AI Act wird einen risikobasierten Ansatz verfolgen. Das soll gewährleisten, „dass die auf dem EU-Markt in Verkehr gebrachten und in der Union verwendeten Systeme künstlicher Intelligenz (KI) sicher sind und die bestehenden Grundrechte und die Werte der Union wahren“. Verboten werden soll der KI-Einsatz bei der sozialen Bewertung von Personen. Für Hochrisikosysteme sind unter anderem Vorgaben im Bereich Datenqualität und Dokumentation vorgesehen. Daneben sind Transparenzvorgaben und weitere Schutzmaßnahmen zugunsten der Betroffenen geplant. Wie üblich sind schmerzhafte Bußgelder und behördliche Maßnahmen bei Nichteinhaltung vorgesehen.



Der risikobasierte Ansatz der KI-Regulierung soll verhindern, dass Grundrechte Betroffener und Werte der Europäischen Union verletzt werden. *Europäisches Parlament*

Mitten in den Diskussionen um den AI Act hat das Bundesverfassungsgericht Stellung zu einem der umstrittenen Themen genommen. Es geht darum, wie die Rechtsgrundlagen für die Datenauswertung mit KI durch die Polizei zur Gefahrenabwehr ausgestaltet sein müssen. Grundsätzlich ist eine automatisierte Datenauswertung nach Auffassung der Karlsruher Richter zulässig. Sie störten sich aber daran, dass die Polizeigesetze in Hamburg und Hessen nicht regeln, wann früher erhobene Daten für einen neuen Zweck ausgewertet werden dürfen.

Missbrauch von Datenverknüpfungen vermeiden

Insbesondere bei Daten, die aus einer Onlinedurchsuchung oder einer Wohnraumüberwachung stammen, müssen die Grundrechte der Betroffenen ausreichend gewahrt werden. Schafft KI durch die erstmalige Verknüpfung von Informationen gänzlich neues Wissen, gilt es, das allgemeine Persönlichkeitsrecht besonders zu berücksichtigen. Unter Fachleuten wird für die neu zu fassenden Regelungen in den Polizeigesetzen ähnlich dem AI-Act-Ansatz ein abgestufter Ansatz diskutiert. Je nach abzuwehrender Gefahr dürften danach bestimmte Analyseinstrumente zum Einsatz kommen. Zu berücksichtigen wäre

auch die zuvor angewandte Methode zur Erhebung der Daten.

Immer wenn von Daten die Rede ist, ist auch die Datenschutz-Grundverordnung (DSGVO) nicht weit. Sie gilt dann, wenn ein Chatbot personenbezogene Daten verarbeitet. Sie greift nur dann nicht, wenn es sich um nicht personenbezogene Daten handelt, also bei anonymen oder anonymisierten Daten. Wenn beim KI-Einsatz nur solche Daten verwendet werden, ist die juristische Compliance deutlich einfacher (siehe [1]).

Jede Form der Datenverarbeitung muss zulässig sein. Das ist sie, wenn die DSGVO oder eine informierte Einwilligung des Betroffenen dies erlauben. Wie in allen anderen Fällen kann der Betroffene bei KI-Einsatz Auskunfts-, Berichtigungs- und Löschungsrechte geltend machen. Wenn Unternehmen wie das hinter ChatGPT stehende OpenAI in Europa aber keine Niederlassung haben, wird die Rechtsdurchsetzung schwierig.

Von Bedeutung beim KI-Einsatz ist Artikel 22 der DSGVO. Er verbietet es, rechtlich erhebliche oder beeinträchtigende Entscheidungen über Menschen zu treffen, die ausschließlich einer automatisierten Datenverarbeitung entstammen. Ausdrücklich genannt wird in diesem Zusammenhang das Profiling. Ganz allgemein bedarf es einer DSGVO-konformen Datenschutzfolgenabschätzung, wenn risikobehaftete Datenverarbeitungen erfolgen. Dies ist insbesondere bei Gesundheitsdaten der Fall.

Bei Regelverletzungen droht Verbot

Jüngst hat die italienische Datenschutzaufsicht den Chatbot Replika verboten. Zur Begründung verwies sie auf die Verletzung von Transparenzvorschriften nach DSGVO und die unzulässige Verarbeitung von Daten Minderjähriger. Brisant an dem Chatbot ist, dass dieser auf Empathie aufbaut und beworben wird als „der KI-Begleiter, der sich kümmert“. Angeblich soll die App zudem Daten im Auftrag russischer Behörden sammeln. Künftig müssen sich solche KI-Anwendungen auch am AI Act

messen lassen.

Wer aber muss letztlich das Datenschutzrecht beim Einsatz von KI einhalten? Verantwortliche Stelle aus DSGVO-Sicht für Datenverarbeitungen ist, wer „allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“. Im Fall von ChatGPT wäre dies OpenAI, im Falle der Einbindung von Bard in Microsoft-Office-Applikationen wäre es Microsoft und so weiter. Wenn allerdings der Nutzer selbst KI-Systeme mit personenbezogenen Daten füttert, kommt auch er als Verantwortlicher in Betracht. Womöglich sind KI-Anbieter und -Nutzer auch als gemeinsam Verantwortliche in der Pflicht. Es kommt auf den Einzelfall an.

Und wer zahlt, wenn durch KI-Einsatz ein Schaden entstanden ist? Wenn einer Person ein Schaden entstanden ist und ein Vertrag zwischen Nutzer und Anbieter besteht, ergibt sich ein etwaiger Schadenersatzanspruch aus dem Vertrag. Nach hiesiger Rechtsordnung greifen ergänzend zu einem Vertrag die schuldrechtlichen Vorschriften im Bürgerlichen Gesetzbuch.

Erst 2022 hat der Gesetzgeber im BGB den Mängelbegriff im Kaufrecht und zahlreiche weitere Vorschriften ergänzt – unter anderem, um die zunehmende digitale Bereitstellung von Waren, aber auch rein digitale Dienstleistungen juristisch besser zu berücksichtigen. Auch auf mangelhafte KI-Leistungen sind diese Vorschriften anwendbar.

KI-Chatbots und das Urheberrecht

KI-gestützte Chatbots wie ChatGPT geben Texte aus. Aus juristischer Sicht ist das relevante Rechtsgebiet in diesem Zusammenhang das Urheberrecht. In dessen Zentrum steht das Grundverständnis, dass nur kreativ-schöpferische Leistungen eines Menschen urheberrechtlichen Schutz genießen können. Damit scheidet die KI selbst als urheberrechtsschöpfend von vornherein aus. Sie ist nur ein handwerkliches oder

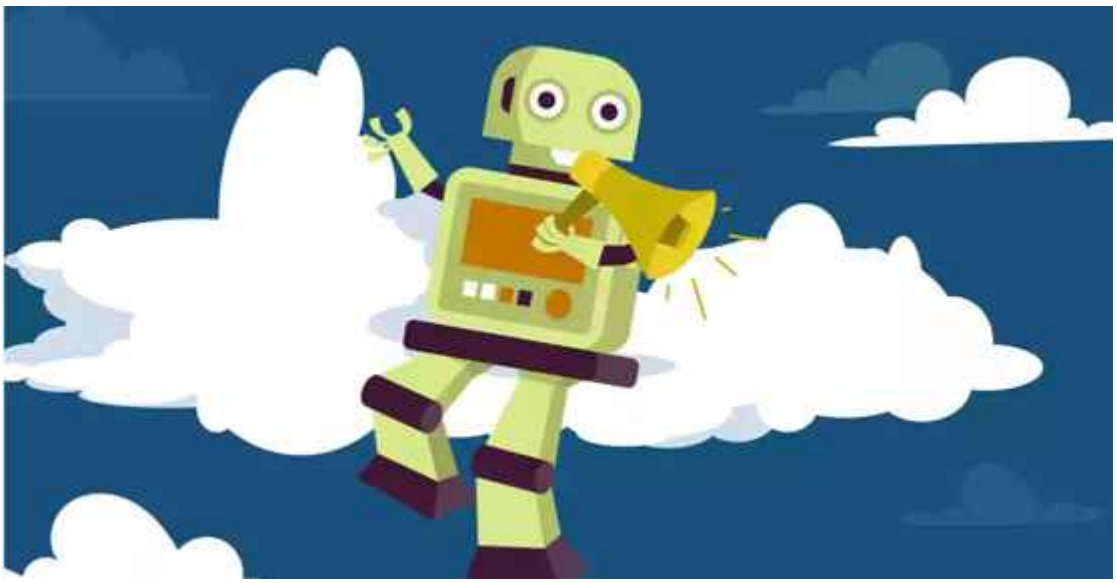
technisches Werkzeug eines dahinterstehenden Menschen. Ihre rein technische Leistung spielt aus urheberrechtlicher Sicht keine Rolle.

Auch der KI-Entwickler und -Betreiber hat an einem konkreten Ergebnis eines durch Nutzer eingesetzten KI-Chatbots keinen eigenen schöpferisch-kreativen Anteil. Er kann sich ebenfalls nicht auf das Urheberrecht stützen. Denkbar wäre allenfalls, dass der Gesetzgeber ein Leistungsschutzrecht für KI-generierte Inhalte schafft. Durch den Hype rund um ChatGPT und Co. könnte die bisher eher schwache Diskussion hierüber an Fahrt gewinnen. Ein Ergebnis ist derzeit nicht absehbar.

Ein KI-Entwickler kann sich allerdings auf den Urheberrechtsschutz für Computerprogramme oder das gesetzliche Leistungsschutzrecht für Datenbankhersteller berufen. Sie schützen ihn vor einer unerlaubten Übernahme der konkreten KI-Umsetzung. Daher kann er Geld für die Nutzung „seiner KI“ verlangen und ein entsprechendes Geschäftsmodell aufsetzen. OpenAI probiert dies derzeit mit ChatGPT aus. Eine Variante von ChatGPT wurde auch in die Microsoft-Suchmaschine Bing eingebunden, wofür Microsoft mehrere Milliarden US-Dollar gezahlt hat.

Wem gehören KI-generierte Inhalte?

Vorsicht ist aus urheberrechtlicher Sicht bei der Nutzung KI-generierter Inhalte geboten. Soweit diese auf urheberrechtlich geschützten Vorlagen beruhen und es sich nicht um gemeinfreie oder etwa auf Basis von Open-Source-Lizenzen für solche Zwecke nutzbare Werke handelt, kann man bei deren Nutzung durch etwaige Urheber in Anspruch genommen werden. OpenAI verweist darauf, dass ChatGPT ausschließlich Werke verwendet, bei denen keine Rechte Dritter entgegenstehen. Überprüfbar ist das im Einzelfall nicht. Den Nutzer eines urheberrechtsverletzenden Chatbot-Ergebnisses schützt seine Unwissenheit im Ernstfall nicht. Im Urheberrecht existiert kein Schutz des guten Glaubens.



Sind urheberrechtliche Inhalte nicht gemeinfrei oder frei nutzbar, stellt sich die Frage nach anderen Rechtfertigungen zur Verwendung von Werken im Rahmen des Text und Data Mining für KI-Zwecke. § 44 b des Urhebervertragsgesetzes (UrhG) versteht hierunter „die automatisierte Analyse von einzelnen oder mehreren digitalen oder digitalisierten Werken, um daraus Informationen über Muster, Trends und Korrelationen zu gewinnen“.

Eine Schranke des Urheberrechts enthält § 60 d des Urhebervertragsgesetzes für den Bereich des Text und Data Mining, sie erlaubt die automatisierte Auswertung – allerdings nur für die nicht kommerzielle wissenschaftliche Forschung. Dabei darf es auch keine beeinflussende Zusammenarbeit zwischen dem Forschungsinstitut und einem privaten Unternehmen geben.

§ 44 b UrhG besagt: „Zulässig sind Vervielfältigungen von rechtmäßig zugänglichen Werken für das Text und Data Mining.“ Dieser vermeintliche Freibrief gilt nicht unbeschränkt. Werke dürfen danach nur dann für Data Mining genutzt werden, „wenn der Rechtsinhaber sich diese nicht vorbehalten hat“. Bei online zugänglichen Werken muss ein solcher Nutzungsvorbehalt in maschinenlesbarer Form vorliegen.

Festlegen, was ein Webcrawler darf

Hier kommt der Robot Exclusion Standard ins Spiel. Ist im Stammverzeichnis einer Domain eine robot.txt-Datei hinterlegt, sollten Webcrawler diese zunächst auslesen. Der Domain-Inhaber kann darin festlegen, welche Suchmaschinen welche Inhalte unter einer Domain auslesen dürfen. Dieser Standard ist rechtlich möglicherweise als „Stand der Technik“ bindend. Er wird von den meisten Suchmaschinenbetreibern beachtet. Derzeit wird eine ähnliche Lösung mit dem Attribut „No AI“ diskutiert, um Webseiteninhalte vor der Nutzung durch KI-Systeme zu schützen.

Der Vollständigkeit halber stellt sich außerdem die Frage, ob dem KI-Nutzer nicht ein Urheberrechtsschutz an seinen Anweisungen an die KI zustehen kann. Es kommt beim sogenannten Prompt Engineering auf den Einzelfall an. Einfache Aufgabenstellungen fallen sicher nicht darunter, komplexe und individuelle Anweisungen möglicherweise schon. Urheberrechtlicher Schutz kann schließlich entstehen, wenn ein KI-Inhalt durch einen Menschen in ausreichender Schöpfungshöhe bearbeitet wird. Dann entsteht an den Bearbeitungen Urheberrechtsschutz.

Zwischen dem KI-Anbieter und dem KI-Nutzer besteht in der Regel ein Vertrag. Dieser enthält Regelungen über das Rechtsverhältnis zwischen beiden und auch im Hinblick auf die von der KI erzeugten Ergebnisse. An diesen erhält der KI-Nutzer meist sämtliche Rechte zur weiteren Nutzung. Ob daran ein Urheberrecht entsteht oder nicht, kann der Vertrag aber nicht regeln. Ein Urheberrecht entsteht kraft Gesetzes, nicht kraft eines Vertrages.

Wenn eine KI beispielsweise einen Artikel für die iX schreibt, hat niemand an dem Chatbot-generierten Text das Urheberrecht. Im Text können aber Werke Dritter verarbeitet worden sein, wodurch das Urheberrecht dieser Dritten tangiert wurde. Ist das nicht der Fall, ist der Text urheberrechtsfrei und kann

von jedermann genutzt werden. Einem Abdruck in der iX steht nichts im Wege.

Auch KI-Haftung soll reguliert werden

Unterdessen arbeitet die EU an einer Richtlinie zur KI-Haftung. Als Richtlinie ist sie nach ihrer Verabschiedung in nationales Recht umzusetzen. Sie soll Geschädigten die Beweislast erleichtern. So soll eine Kausalitätsvermutung greifen und ein Anspruch auf Schadenersatz schon dann bestehen, wenn eine Person für eine bestimmte für den Schaden relevante Verpflichtung verantwortlich war und „ein ursächlicher Zusammenhang mit der KI-Leistung nach vernünftigem Ermessen wahrscheinlich ist“.

Bei Hochrisiko-KI-Systemen sollen Richter zudem die Offenlegung von Informationen über solche Systeme anordnen können. Damit will man die verantwortlichen Personen ermitteln. Andererseits unterliegen offengelegte Informationen dem Geheimnisschutz. Auswirkungen auf den Bereich KI könnte auch die gleichfalls auf EU-Ebene diskutierte neue Produkthaftungsrichtlinie haben. Sie bietet Verbrauchern bei fehlerhaften Produkten eine verschuldensunabhängige Schadenshaftung. Mit ihr soll die seit 1985 EU-weit geregelte Produkthaftung an neue Technologien, etwa KI, angepasst werden.

Auf die KI-Anbieter kommen mehr und mehr regulatorische Pflichten und Complianceanforderungen zu. Deshalb müssen sie sich um ihre Haftungsrisiken Gedanken machen und entsprechende Vorkehrungen treffen. Das Trainieren von KI-Systemen auf Rechtskonformität ist eine der großen Herausforderungen beim Einsatz von KI. Dazu müssen aber zunächst einmal die gesetzlichen Vorgaben verfeinert werden. Sie werden aber auch nur den Rahmen festlegen. Die konkreten Ausgestaltungen hängen dann vom jeweiligen Einsatz von KI in der Praxis ab. Letztlich werden Gerichte darüber befinden, ob die Vorgaben in ausreichendem Maße eingehalten wurden oder nicht.

Auch KI-Nutzer müssen vor der Verwendung von KI-generierten Informationen juristische Aspekte beachten. Sie können sich im Bereich Datenschutz oder Urheberrecht in der Regel nicht auf ihre Unwissenheit berufen. Juristische Fallen entstehen, wenn Nutzer die Herkunft der durch KI verwendeten Datensätze nicht kennen und nicht kontrollieren können. Gleiches gilt für die eingesetzten Algorithmen. Zumindest bei KI-Anwendungen von Drittanbietern ist eine Kontrolle in den meisten Fällen nicht möglich.

Fazit

Künstliche Intelligenz fordert das Recht heraus. Je tiefer die KI in die verschiedenen Lebensbereiche eindringt, umso mehr müssen sich Gesetzgeber und Richter mit den daraus resultierenden Risiken befassen. Letztlich können davon zunächst fernliegende Rechtsbereiche betroffen sein, etwa das Schulrecht bei der Frage der Zulässigkeit KI-generierter Hausaufgaben. Es geht aber eben auch um komplexe Fragen im Haftungs-, Datenschutz- oder Urheberrecht (siehe Kasten „KI-Chatbots und das Urheberrecht“). Die EU plant mit dem AI Act einen risikobasierten Ansatz bei der KI-Regulierung bis hin zum Verbot einzelner KI-Ansätze. Auf Anbieter wie Nutzer kommen umfassende juristische Risiken zu. Das KI-Recht ist gekommen, um zu bleiben. (ur@ix.de)

ChatGPT im juristischen Einsatz

Künstliche Intelligenz ist nicht nur eine Herausforderung für die Juristerei. Sie kann ihr auch bei der Arbeitsbewältigung helfen. Richter, Staatsanwälte und Rechtsanwälte können von sprachmodellbasierten KI-Lösungen profitieren, die beispielsweise Urteile analysieren und Entscheidungsmuster aufzeigen. Hilfreich kann es auch sein zu wissen, wie ein bestimmtes Gericht in einem ähnlich gelagerten Verfahren entschieden hat. Das wäre ein großer Schritt hin zu einem „Predictive Decision-Making“, einem planbaren Ausgang eines Rechtsstreits.

Macht Chat-GPT Anwälte obsolet? Chatbots können dabei helfen, rechtssuchenden Bürgern den Gang zum Anwalt zu ersparen. Auch bisher war es möglich, zu Rechtsfragen zu „googeln“. Zukünftig könnte eine individuelle Rechtsberatung durch KI-Systeme hinzukommen. Sie wäre womöglich billiger als das Hinzuziehen eines Rechtsanwalts. Allerdings ist die Juristerei extrem komplex und jeder Einzelfall ist individuell zu betrachten. Dabei spielt der verfassungsrechtlich bei nahezu allen Rechtsfragen zu berücksichtigende Verhältnismäßigkeitsgrundsatz eine bedeutende Rolle. Er könnte eine KI – noch – an ihre Grenzen führen.

KI im juristischen Einsatz

Bereits heute werden KI-Systeme bei der Vertragsprüfung eingesetzt. Sie können Muster erkennen und beispielsweise auf Regelungslücken hinweisen. Derzeit werden solche Systeme etwa zur Prüfung von Vertraulichkeitsvereinbarungen eingesetzt. Auch an komplexere Verträge wagen sich die ersten Lösungen heran.

Weitere Anwendungsfelder für KI im Rechtsbereich gibt es bei Themen wie Contract Lifecycle Management. Im Bereich der DSGVO-Compliance können Webseiten auf die Einhaltung datenschutzrechtlicher Vorgaben etwa hinsichtlich der Datenschutzerklärung überprüft werden.

Welche weiteren Anwendungsfälle in Zukunft erlaubt sein werden, hängt von den regulatorischen Rahmenbedingungen ab. Denkbar sind KI-Systeme, die bei Gesetzesverstößen automatisch Sanktionen verhängen. Bei Parkzeitüberschreitungen ist das sicher eher akzeptabel als bei schwerwiegenden Straftaten. Hier dürfte Artikel 101 des Grundgesetzes eine Rolle spielen: „Niemand darf seinem gesetzlichen Richter entzogen werden.“ Dabei muss es sich (noch) um einen Menschen handeln.

1. Quellen

2. Tobias Haar; Nutzer unbekannt; Rechtsfragen der Pseudonymisierung und Anonymisierung; iX 5/2021, S. 86

Tobias Haar

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

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

DSGVO-Bußgelder um 50 Prozent gestiegen

DSGVO-Bußgelder um 50 Prozent gestiegen

Die Bußgelder für DSGVO-Verstöße zogen im letzten Jahr deutlich an. Dabei baten die europäischen Richter Meta für Verstöße bei Facebook, Instagram und WhatsApp zur Kasse – jedoch um 4 Milliarden zu wenig, wie Datenschutzaktivist Max Schrems meint.

Im Jahr 2022 ist die Zahl der Bußgelder in der EU wegen Verstößen gegen die Datenschutz-Grundverordnung stark angestiegen. Das belegt eine Studie der internationalen Anwaltskanzlei DLA Piper. Im Vergleich zum Vorjahr sind die Bußgelder um etwa 50 Prozent auf insgesamt 1,64 Milliarden Euro gestiegen. Dazu beigetragen haben insbesondere die Bußgelder gegen Facebook in Höhe von 210 Millionen Euro und Meta in Höhe von 180 Millionen Euro. Wegen dieser Verfahren führt die hierfür verantwortliche irische Datenschutzbehörde DPC das Ranking an. Im gleichen Zeitraum hat die Zahl der von Unternehmen gemeldeten Datenpannen signifikant abgenommen.

Der bekannte Datenschutzaktivist Max Schrems hat die irische Datenschutzbehörde für einen zu laxen Umgang mit Meta kritisiert. Seiner Meinung nach hätte das verhängte Bußgeld 4 Milliarden Euro höher ausfallen müssen – die Behörde legte sich jedoch auf 390 Millionen Euro wegen DSGVO-Verstößen fest. Der Vorwurf lautete, dass Facebook rechtswidrig die gezielte Werbung gegenüber Nutzern als vertragliche Leistung ausgegeben hat, für die keine Einwilligung erforderlich sei. Ebenso fehlte es an einer wirksamen Einwilligung für das Tracking des Nutzerverhaltens. Laut Schrems hätte die DPC bei der Bemessung des Bußgelds die zusätzlichen Werbeeinnahmen durch den Datenschutzverstoß angemessen berücksichtigen müssen.

Auch WhatsApp ist derzeit im Fokus der irischen Datenschutzaufsicht. Hier lautet der Vorwurf ebenfalls mangelnde Transparenz über die Verarbeitung von Nutzerdaten sowie fehlende Rechtsgrundlage für gezielte Werbung und Tracking. Auf ein bereits 2021 verhängtes Bußgeld in Höhe von 225 Millionen Euro folgte nun ein weiteres über 5,5 Millionen Euro. Aber nicht nur Meta steht am Pranger: Die französische Datenschutzaufsichtsbehörde CNIL hat gegen TikTok eine Strafzahlung von 5 Millionen Euro angeordnet. Ihrer Meinung nach ist es unzulässig, dass für Nutzer die Ablehnung von Cookies nicht so einfach wie die Zustimmung ist. Apple wurde schließlich für die Verwendung von Gerätedaten für personalisierte Werbung im App-Store durch die CNIL mit einem Bußgeld über 8 Millionen Euro belegt.

Unterdessen verhandelt der Europäische Gerichtshof im Bußgeldverfahren gegen die Deutsche Wohnen über Grundsatzfragen der Verhängung von Strafen nach der DSGVO. Konkret geht es darum, ob bei Datenschutzverstößen durch Unternehmen die hierfür verantwortlichen Personen namentlich ermittelt werden müssen oder ob es ausreicht, dass ein Verstoß begangen wurde. Die Richter prüfen zudem, ob Verstöße einer Leitungsperson zuordenbar sein müssen. Während dies nach deutschem Recht erforderlich ist, sieht die DSGVO diese Voraussetzungen nicht vor. Das Verfahren ist entscheidend für die künftige Bußgeldpraxis in Deutschland. *Tobias Haar* (pst@ix.de)

Internationale ISO-Norm 31700 zu Privacy by Design in Kraft getreten

Am 8. Februar 2023 ist die ISO 31700 in Kraft getreten. Sie beschreibt Datenschutzgrundsätze von Privacy by Design im Zyklus von Produkten und Dienstleistungen, die deren Anbieter künftig vom Beginn des Entwurfs über Entwicklung und Vermarktung berücksichtigen sollen. Der erste Teil des Standards beschreibt Prinzipien der datenschutzfreundlichen Produktgestaltung. Es geht dabei um Fragen des Designs von

Nutzerschnittstellen und Datenhaltung, der Kommunikation mit Verbrauchern, Risikoassessments oder Tests der Datenschutzeinstellungen.

Beispiele im zweiten Teil der Norm sollen das Verständnis für diese Standards und deren Umsetzung anschaulich verdeutlichen. Die Einhaltung des ISO-Standards 31700 ist nicht verpflichtend. Allerdings tragen solche Standards zur Weiterentwicklung des Standes der Technik insgesamt bei, der auch bei Datenschutzverstößen eine Rolle spielt. Der Download der Norm auf den Webseiten der internationalen Organisation für Normung ist gebührenpflichtig und kostet etwa 300 Euro. Der Standard konkretisiert Art. 25 DSGVO, der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen festschreibt. *Tobias Haar* (pst@ix.de)

BAG: Keine Pflicht zur Stechuhr im Homeoffice

Seit einem Beschluss des Bundesarbeitsgerichts zur Arbeitszeiterfassung durch den Arbeitgeber wird über dessen Auswirkungen auf Arbeitszeitmodelle wie Homeoffice diskutiert. Die Erfurter Richter hatten verbindlich festgestellt, dass Arbeitgeber verpflichtet sind, „Beginn und Ende der täglichen Arbeitszeit der Arbeitnehmer zu erfassen“. Die Präsidentin des Bundesarbeitsgerichts hat nun erklärt, dass das Urteil diese Vertrauensarbeitszeitmodelle nicht abschaffe. Unter anderem hatte der Branchenverband Bitkom zuvor Zweifel hieran geäußert.

Die BAG-Präsidentin Inken Gallner stellte zudem klar, dass durch die Gerichtsentscheidung keine Pflicht zur Einführung von Stechuhren entstanden sei. „Das Wie der Arbeitszeiterfassung liegt in den gestaltenden Händen des Gesetzgebers“, so Gallner. Flexible Arbeitszeitmodelle sollen durch den Beschluss nicht abgeschafft werden. Aber auch bei solchen müsse beispielsweise die elfstündige Ruhezeit eingehalten werden. Die grundsätzliche Pflicht zur Arbeitszeiterfassung besteht bereits. Zusätzlich kündigte das

Bundesarbeitsministerium an, Details der Zeiterfassung durch ein entsprechendes Gesetz regeln zu wollen. Wann dieses vorliegen und in Kraft treten wird, ist derzeit unklar. *Tobias Haar* (pst@ix.de)

EU untersucht Wettbewerbsverstöße durch Microsoft-Lizenzierungspraxis

Cispe lässt nicht locker: Die Vereinigung von Cloud-Infrastruktur-Anbietern in Europa hatte bereits im November 2022 eine Beschwerde bei der Generaldirektion Wettbewerb der EU-Kommission gegen Microsofts Bündelungspraxis von Softwareprodukten und Cloud-Services eingereicht. Jetzt legte der Verband noch einmal argumentativ nach.

Wissenschaftler der privaten Hochschulen Frankfurt School of Finance und European School of Management and Technology (ESMT) durchleuchteten im Auftrag von Cispe die ökonomischen Konsequenzen der Bündelung. In der 18-seitigen Untersuchung kommen sie zu dem Schluss, dass Preiserhöhungen, weniger Wahlmöglichkeit und geringere Innovationstätigkeit drohen.

Hintergrund ist der Verdacht, dass Microsoft die marktbeherrschende Stellung von zum Beispiel Windows oder Office als Hebel nutzen will, um sich im Cloud-Umfeld Vorteile zu verschaffen. Mittel zum Zweck sind die Lizenzbedingungen. Danach dürfen Kunden eine bereits erworbene Software auf Ressourcen externer Rechenzentren einsetzen, soweit diese von Microsoft als autorisierte Outsourcer zertifiziert sind – Amazon AWS, Google und Microsofts Azure selbst zählen nicht zu diesem erlauchten Kreis.

Allerdings offeriert der Konzern laut Studie diverse Optionen, bestehende Lizenzen auch ohne oder nur mit geringen Zusatzkosten in Azure zu nutzen. Diese Optionen stehen für AWS oder Google so nicht zur Verfügung. Ihr Einsatz wäre folglich die kostspieligere Alternative zur Microsoft-Cloud, da in der Regel neue Lizenzen zu erwerben sind. *Achim Born* (pst@ix.de)

EU-Studie deckt Rechtsverstöße durch Dark Patterns in Onlineshops auf

Eine groß angelegte Studie von EU-Kommission und Verbraucherschutzbehörden aus 23 Mitgliedstaaten sowie Norwegen und Island hat weitverbreitete Rechtsverstöße in Onlineshops dokumentiert. Demnach setzen deren Betreiber in fast 40 Prozent der Fälle manipulative Praktiken zum Täuschen von Nutzern ein. Insgesamt wurden knapp 1400 Onlineshops untersucht. Verbreitet setzten die Anbieter laut Studie falsche Countdown-Zähler mit Fristen für den Kauf bestimmter Produkte ein. Viele Shops versuchten, Kunden durch visuelle Gestaltung oder sprachliche Mittel zum Abschluss von Abonnements zu bewegen. Bei 70 Anbietern fehlten im Kaufprozess entscheidende Informationen oder diese wurden nur versteckt zur Verfügung gestellt. Bemängelt wurden auch Zwangsregistrierungen und „virtuelle Drängel- und Gängeleien“.

Die Behörden wollen die gerügten Shopbetreiber zunächst auffordern, die Rechtsverstöße kurzfristig abzustellen. Kommen sie dem nicht nach, drohen formale Verfahren und Bußgelder. Der Bundesverband Onlinehandel kritisiert, dass mit der Studie weniger als ein Prozent aller Onlineshops überprüft wurde. Auch fehlten große Plattformen und Marktplätze. Durch das im Digital Services Act verschärfte Verbot von Dark Patterns und ähnlichen Methoden dürfte der Fokus auf solche Praktiken weiter zunehmen. Verstöße können mit Bußgeldern von bis zu 6 Prozent des Jahresumsatzes sehr teuer werden. *Tobias Haar* (pst@ix.de)

USA und EU arbeiten an gemeinsamem KI-Rahmen

Eine Verwaltungsvereinbarung zwischen den USA und der EU soll die Kooperation im Bereich des Einsatzes von künstlicher Intelligenz fördern. Ziel sei es, bestimmte Prozesse per KI zu verbessern. Gemeint sind unter anderem die Katastrophenprävention durch Vorhersage von Extremwettersituationen, aber auch die Gesundheitsvorsorge

oder die Energieversorgung. Im Fokus steht dabei die gemeinsame Nutzung der vorhandenen sowie die Erschließung neuer Datenbestände im Einklang mit den geltenden datenschutzrechtlichen Bestimmungen. Ziel ist ein KI-Modell mit jeweils in der EU und den USA liegenden Daten zur gemeinsamen Nutzung. *Tobias Haar* (pst@ix.de)

Kurz notiert

Der Verbraucherzentrale Bundesverband hat neun **Telemedizin- und Arzttermin-Portale** wegen DSGVO-Verstößen abgemahnt. Die Datenverarbeitung sei intransparent und es fehlten Einwilligungen der Betroffenen.

Das Landesarbeitsgericht Köln sieht die Beweislast für den **Zugang einer E-Mail beim Absender.** Weder deren Absendung noch das Fehlen einer Unzustellbarkeitsnachricht begründen einen rechtlich relevanten Anschein für den Zugang einer E-Mail.

Die Schweiz hat zum Jahresanfang die **EU-Drohnenreglementierung** übernommen. Für Drohnen ab 250 Gramm gilt nun eine Registrierungspflicht. Piloten müssen zudem eine Onlineschulung nachweisen.

Der europäische Datenschutzausschuss EDSA sieht mögliche Rechtsverstöße bei **Cookie-Bannern.** Neben einem Akzeptieren-Button müsste es regelmäßig einen entsprechenden Ablehnen-Button geben, heißt es im Positionspapier. Auch die grafische Darstellung der Banner genügt oft nicht den Datenschutzvorgaben.

Markt + Trends | IT-Recht & Datenschutz

Gravierende Mängel beim Kündigungs-Button

Seit dem 1. Juli 2022 müssen in Deutschland tätige Unternehmen den sogenannten Kündigungs-Button auf ihren Webseiten anbieten. Die Verbraucherzentrale Bayern hatte systematisch Webseiten überprüft und bei der Mehrheit davon erhebliche rechtliche Mängel aufgedeckt. Ein Großteil bewegte sich überdies im Graubereich, teilt die Verbraucherzentrale Bayern mit.

Die Verbraucherverbände hätten insgesamt 152 Unternehmen abgemahnt. Lediglich auf 273 von 840 überprüften Websites fanden sich gesetzeskonforme Kündigungs-Buttons, heißt es aus Bayern weiter.

349 Webseiten ließen den vorgeschriebene Kündigungs-Button ganz vermissen. In 65 Fällen war er auf der Website versteckt, in 38 Fällen trug er eine unzulässige Beschriftung. Überdies wurden 339 weitere Verstöße im Zusammenhang mit der Bestätigungsseite und dem finalen Bestätigungs-Button festgestellt, teilen die Verbraucherschützer mit. Es hätten zum Beispiel Pflichtangaben gefehlt, oder es habe unzulässige Beschriftungen gegeben. Letztere müssen ebenfalls bestimmten Formalien genügen.

Bis Anfang November 2022 zeigten sich 86 Unternehmen einsichtig und unterschrieben die geforderte Unterlassungserklärung. In drei Fällen erwirkten die Verbraucherschützer eine einstweilige Verfügung, in 17 Fällen haben sie ein Klageverfahren vorbereitet oder bereits ein solches eingereicht.