www.compliance-berater.de

Compliance Berater

CB

12 / 2024

Betriebs-Berater Compliance

21.11.2024 | 12.Jg
Seiten 461–508

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

CB-BEITRAG

Dr. Thorsten Ammann, Florian Achnitz, LL. M., und Ludwig Lauer

Passierschein A38? – Die Zuständigkeitsregelungen des AI Acts im nationalen und supranationalen Behördendschungel

Der EU AI Act (zu Deutsch: „KI-Verordnung") – das weltweit erste Gesetz zur Regulierung Künstlicher Intelligenz – ist am 2.8.2024 in Kraft getreten.[1] Ziel der nach Art. 288 AEUV unmittelbar in allen 27 Mitgliedstaaten geltenden Verordnung ist es, durch harmonisierte Vorschriften einen – am Grundrechtsschutz natürlicher Personen ausgerichteten – vertrauenswürdigen und sicheren Einsatz von KI-Systemen im Gebiet der Europäischen Union zu gewährleisten. Nachdem wir mit unserem Beitrag „Künstliche Intelligenz – ein Compliance-Thema" in CB 2024, 317, einen ersten Überblick über die Compliance-rechtlichen Implikationen der KI-Verordnung aus unternehmerischer Sicht gegeben haben, möchten wir uns im Folgenden mit der Frage beschäftigen, welche Behörden auf supranationaler und nationaler Ebene für welche Fragen und Anliegen rund um Künstliche Intelligenz (im Folgenden „KI") kompetente und zuständige Stellen sind.

I. Warum diese ganze Regulierung?

Um den Hintergrund des KI-Regulierungsansatzes etwas greifbarer zu machen, lassen Sie uns auf eine Zeitreise gehen. Zurück ins alte Rom müssen wir dafür nicht, jedoch zurück in das Jahr 1886, das Jahr, in dem Carl Benz sein „Fahrzeug mit Motorenbetrieb" zum Patent anmeldete. Das Automobil war geboren – und damit eine für die damalige Zeit neue Technologie mit seinerzeit unvorstellbarem sozioökonomischem und disruptivem Potenzial. Doch es dauerte, bis das Kfz zu jenem zuverlässigen und sicheren Verkehrsmittel heranreifte, wie wir es heute kennen. Nicht zuletzt auch dafür verantwortlich ist der rechtliche Ordnungsrahmen, der im Laufe der Zeit immer weitere Konturierung erfahren hat. Angefangen von Kfz-Zulassungsbehörden, die über die Verkehrssicherheit des Fahrzeuges wachen, über die StVO, die Verhaltensregelungen bei dessen Bewegung im öffentlichen Raum aufstellen, bis hin zu verpflichtenden regelmäßigen technischen Kontrollen durch den Technischen Überwachungsverein (TÜV), die gewährleisten sollen, dass das Fahrzeug auch nach Inverkehrbringen verkehrssicher bleibt.

Die damalige Situation um das Automobil ist mit der heutigen Situation um KI durchaus vergleichbar. Auch mit KI handelt es sich um eine neue Technologie mit erheblichem sozioökonomischem Potenzial, die Innovationsförderung verdient. Gleichzeitig bedarf es, wie beim Automobil auch, vertrauensbildender Maßnahmen in die neue Technologie, da sie ihr soziökonomisches Potenzial nicht wird entfalten können, wenn niemand bereit ist, sie zu nutzen. Um dies zu erreichen, bedarf es eines dem Kfz vergleichbaren Ordnungsrahmens, in dessen Realisierung die KI-Verordnung jedoch einen komplexen mehrstufigen Ansatz verfolgt, der Durchsetzungsbefugnisse sowohl auf nationaler als auch auf europäischer Ebene vorsieht.

Anders ausgedrückt: Es könnte wahr werden, das „Haus, das Verrückte macht" und bislang nur eingefleischten Asterix-Lesern aus „Asterix erobert Rom" ein Begriff sein möge. Im „Haus, das Verrückte macht" sollen *Asterix* und *Obelix* den Passierschein A38 besorgen, eine Aufgabe von mehreren, die nicht mit Menschenverstand, sondern nur mit übernatürlichen Kräften und damit von Göttern lösbar sein soll.[2] Der vorliegende Beitrag soll in einer ersten Annäherung untersuchen, ob und inwieweit der mehrstufige Ansatz der KI-Verordnung mit Durchsetzungsbefugnissen auf nationaler und supranationaler Ebene schon unter Anwendung vernünftigen Menschenverstands zu praktikablen Ergebnissen führt oder den Ruf nach übernatürlichen Kräften verlangt.

II. Mehrstufiges Governance-Konzept

Um die Systematik hinter dem mehrstufigen gesetzlichen KI-Governance-Konzept zu verstehen, hilft ein Blick auf den Kommissionsentwurf der KI-Verordnung aus dem Jahr 2021.[3] Dieser ging unter

1 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401689 (letzter Abruf: 17.10.2024).

2 *Goscinny/Uderzo,* Asterix erobert Rom, Köln, 2016.

3 COM(2021) 206 final, abrufbar unter https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0019.02/DOC_1&format=PDF (letzter Abruf: 17.10.2024).

Berücksichtigung des in Art. 5 Abs. 3 AEUV niedergelegten Subsidiaritätsgrundsatzes und Art. 291 AEUV, wonach die Verfahrens- und Vollzugsautonomie bei den Mitgliedstatten liegt, von einer Schlüsselrolle der Mitgliedstaaten bei der Um- und Durchsetzung der KI-Verordnung aus. Vor diesem Hintergrund waren für die nationalen Behörden weitreichende Kompetenzen, insbesondere hinsichtlich Notifizierung und Marktüberwachung von KI-Systemen, vorgesehen.[4] Durchsetzungsbefugnisse auf europäischer Ebene fanden sich in dem seinerzeitigen Kommissionsentwurf noch nicht.[5]

Dies änderte sich erst mit dem Ende 2022 als sogenanntem „Large Language Model" konzipierten und gelaunchten Chatbot „ChatGPT" des US-amerikanischen Softwareunternehmens OpenAI.[6] In Abkehr von der bisherigen gesetzgeberischen Vorstellung, dass KI-Systeme spätestens ab dem Zeitpunkt ihres Inverkehrbringens oder ihrer Inbetriebnahme einen klar definierten Zweck verfolgen würden, sollte fortan dem Umstand Rechnung getragen werden, dass es daneben solche KI-Modelle gibt, deren Zweckbestimmung auch nach ihrem Inverkehrbringen nutzerzentriert variieren kann, sich also für eine Vielzahl von Verwendungszwecken eignen (sog. „KI-Modelle mit allgemeinem Verwendungszweck" bzw. „General Purpose AI" – im Folgenden GPAI-Modelle).

Als regulatorische Antwort entstand die Idee eines „AI Office" (zu Deutsch: „Büro für Künstliche Intelligenz") auf europäischer Ebene. Diese per Kommissionsbeschluss[7] vom 24.1.2024 errichtete und organisatorisch in die Generaldirektion „Kommunikationsnetze, Inhalte und Technologien" der Europäischen Kommission eingebettete Institution tritt nach dem finalen Verordnungstext[8] ergänzend neben den nationalen Governance-Rahmen.

III. Kompetenzen auf Unionsebene

1. AI Office

Wirft man einen Blick auf die Legaldefinition aus Art. 3 Nr. 47 KI-Verordnung, so wird das AI Office als „die Aufgabe der Kommission, zur Umsetzung, Beobachtung und Überwachung von KI-Systemen und KI-Modellen mit allgemeinem Verwendungszweck" definiert.[9] Wenngleich die Definition sprachlich vor dem Hintergrund etwas missglückt erscheint, als dass das AI Office freilich lediglich die den in Art. 3 Nr. 47 KI-Verordnung genannten Aufgaben zugewiesene Institution (und nicht die Aufgabe selbst) darstellt, wird ihr Errichtungszweck schnell klar: Zentrale Aufgabe des AI Office ist die kohärente Umsetzung und Durchsetzung der KI-Verordnung innerhalb der Europäischen Union für GPAI-Modelle. Daneben weist die Verordnung dem AI Office weitere Aufgabenfelder zu – dazu später mehr.[10]

Gemäß Art. 88 Abs. 1 KI-Verordnung kommt dem AI Office die ausschließliche Befugnis zur Beaufsichtigung und Durchsetzung von GPAI zu. Zur Wahrnehmung dieser Aufgabe kann es nach Art. 89 Abs. 1 KI-Verordnung die „erforderlichen Maßnahmen" ergreifen. Diese zunächst sehr offen gefasste Norm erfährt durch die Befugnisnormen der Art. 91–93 KI-Verordnung nähere Konturierung.

Zu den konkreten Kompetenzen des AI Office zählt zum einen nach Art. 91 Abs. 1 KI-Verordnung die Befugnis, sämtliche Dokumentation und Informationen beim Anbieter des betreffenden GPAI-Modells anzufordern, um zu prüfen, ob die insoweit geltenden Anforderungen der Verordnung eingehalten sind. Ferner hat es nach Art. 92 Abs. 1 KI-Verordnung die Befugnis, Bewertungen durchzuführen – insbesondere zur Ermittlung inhärenter systemischer Risiken in GPAI-Modellen. Solche systemischen Risiken sind nach Art. 51 KI-Verordnung anzunehmen, sofern das betreffende GPAI-Modell über einen besonders hohen Wirkungsgrad verfügt, verbunden mit der Gefahr negativer Folgen für die öffentliche Gesundheit, die öffentliche Sicherheit oder Grundrechte.[11] Ein hoher Wirkungsgrad wird dabei nach Art. 51 Abs. 2 KI-Verordnung fingiert, wenn die kumulierte Menge der für sein Training verwendeten Berechnungen – gemessen in Gleitkommaoperationen – mehr als 10^{25} beträgt. Kommt das AI Office nach seiner Bewertung zu der Einschätzung, dass die Kriterien für ein systemisches Risiko vorliegen, ist das GPAI-Modell zu einem GPAI-Modell mit systemischem Risiko hochzustufen, was gesteigerte Compliance-Anforderungen nach sich zieht.

Weitere Befugnisse des AI Office sind in Art. 93 KI-Verordnung zu finden. Soweit erforderlich und angemessen, kann das AI Office hiernach Anbieter zu geeigneten Maßnahmen auffordern, wie etwa zur Vornahme von Risikominderungsmaßnahmen. Derartige Aufforderungen können – wie etwa aus gefahrenabwehrrechtlichen Kfz-bezogenen Maßnahmen bekannt – sogar darin bestehen, die Bereitstellung eines GPAI-Modells vollständig einzuschränken, es zurückzunehmen oder zurückzurufen.[12] Soweit einer solchen Aufforderung (mindestens in fahrlässiger Weise) nicht nachgekommen wird, greifen die empfindlichen Bußgelder aus Art. 101 Abs. 1 KI-Verordnung mit Geldbußen von bis zu 3% des weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr oder 15 Mio. EUR, je nachdem, welcher Betrag der höhere ist.

Bei der Festsetzung der Höhe der Geldbuße oder des Zwangsgelds ist nach Art. 101 Abs. 2 KI-Verordnung Art, Schwere und Dauer des Verstoßes sowie den Grundsätzen der Verhältnismäßigkeit und der Angemessenheit Rechnung zu tragen. Zudem hat das AI Office dem potenziellen Bußgeldadressaten gem. Art. 101 Abs. 2 KI-Verordnung vor Festsetzung einer Entscheidung seine vorläufige Beurteilung mitzuteilen und – vergleichbar der verwaltungsbehördlichen Anhörung bei belastenden Verwaltungsakten – dem Adressaten Gelegenheit zur Stellungnahme zu geben, auf dessen Grundlage das AI Office seine Entscheidung gegebenenfalls korrigieren kann.

2. Beratende Gremien

Dem AI Office stehen auf europäischer Ebene drei Institutionen beratend zur Seite, denen jedoch keine Durchsetzungskompetenzen zukommen (Umkehrschluss aus Art. 88 Abs. 1 KI-Verordnung):

---

4 Vgl. *Bomhard/Merkle*, RDI 2021, 276, 282.

5 Stattdessen fand sich mit dem „European Artificial Intelligence Board" in den Art. 56 ff. COM (2021) 206 final ein Vorläufer des AI Office, dessen Funktion sich weitgehend in Beratung und Unterstützung der Kommission erschöpfen sollte.

6 Es handelt sich bei einem „Large-Language-Modell" um ein computerlinguistisches Wahrscheinlichkeitsmodell, das statistische Wort- und Satzfolge-Beziehungen aus einer Vielzahl von Textdokumenten durch einen rechenintensiven Trainingsprozess erlernt hat und damit in der Lage ist, auf eine Vielzahl von Sprachbefehlen hin individuell antworten zu können. Vertiefend nachzulesen unter https://cdn.openai.com/better-language-models/language_models_are_unsupervised_multitask_learners.pdf (letzter Abruf: 17.10.2024).

7 Gründungsbeschluss der Kommission vom 24. Januar 2024 zur Einrichtung des Europäischen Amts für künstliche Intelligenz (C/2024/1459), abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:C_202401459 (letzter Abruf: 17.10.2024).

8 Siehe hierzu Fn. 1.

9 Vgl. auch ErwG 148 KI-Verordnung.

10 Hierzu im Einzelnen Gliederungspunkt III.3.

11 S. hierzu Art. 3 Nr. 65 KI-Verordnung sowie ErwG 110 KI-Verordnung.

12 Siehe hierzu Art. 93 Abs. 1 c) KI-Verordnung.

a) Wissenschaftliches Gremium

Zunächst steht dem AI Office ein Wissenschaftliches Gremium[13] zur Seite, das durch einen Durchführungsrechtsakt zu errichten ist (Art. 68 KI-Verordnung). Das Wissenschaftliche Gremium setzt sich aus von der Kommission ausgewählten unabhängigen Sachverständigen zusammen und steht somit für die notwendige technische Expertise. Nach Art. 90 Abs. 1 KI-Verordnung kann das Wissenschaftliche Gremium dem AI Office etwa qualifizierte Warnungen – das heißt unter Nennung einschlägiger Fakten und relevanter Informationen – übermitteln, wenn es Grund zu der Annahme hat, dass ein GPAI-Modell ein konkretes, identifizierbares Risiko auf Unionsebene birgt. Die Warnung kann ferner dazu dienen, darauf hinzuweisen, dass das GPAI-Modell ein systemisches Risiko darstellt. Untechnisch gesprochen kann man die Warnungen auch als „Handlungsimpulse" des AI Office verstehen.

b) KI-Gremium

Nachdem eine qualifizierte Warnung durch das Wissenschaftliche Gremium an das AI Office erfolgt ist, hat das AI Office das sog. KI-Gremium zu unterrichten. Dem KI-Gremium gehören – anders als dem Wissenschaftlichen Gremium – hochrangige Vertreter der Mitgliedstaaten und der Europäische Datenschutzbeauftragte (EDSB) an. Als wichtiges Beratungsgremium soll das KI-Gremium Orientierungshilfen zu allen Fragen im Zusammenhang mit KI-bezogener Politik erarbeiten, insbesondere zu KI-Regulierung, KI-bezogener Innovations- und Exzellenzpolitik und internationaler Zusammenarbeit. Das KI-Gremium spielt eine zentrale Rolle bei der reibungslosen, wirksamen und einheitlichen Durchführung der KI-Verordnung. Es soll als Forum fungieren, in dem die KI-Regulierungsbehörden – also AI Office, nationale Behörden und EDSB – eine einheitliche Durchführung der KI-Verordnung koordinieren können.[14]

c) Beratungsforum

Neben dem Wissenschaftlichen Gremium und dem KI-Gremium existiert mit dem Beratungsforum[15] (Art. 67 KI-Verordnung) eine dritte beratende Institution bestehend aus verschiedenen Interessenträgern, darunter der Industrie, Start-up-Unternehmen, kleinen und mittleren Unternehmen (KMU), der Zivilgesellschaft und Wissenschaft. Kernaufgabe des Beratungsforums ist es, auf Ersuchen des KI-Gremiums oder der Europäischen Kommission Empfehlungen, Gutachten sowie schriftliche Stellungnahmen zu erarbeiten. Eigene Durchsetzungsbefugnisse des Beratungsforums sieht die KI-Verordnung indes nicht vor.

3. Weitere Kompetenzen des AI Office

Zusätzlich zu den oben unter III.1. beschriebenen Durchsetzungsbefugnissen kommen dem AI Office einige weitere Kompetenzen zu. So soll das AI Office etwa eine zentrale Rolle in Forschungs-, Entwicklungs-, und gesellschaftspolitischen Fragen im Zusammenhang mit der Entwicklung und Anwendung künstlich intelligenter Lösungen einnehmen. Einen ersten Überblick über die konkreten Aufgabenfelder gibt die von der Europäischen Kommission hierzu herausgegebene Pressemeldung über den organisatorischen Aufbau des AI Office, der insgesamt folgende zu errichtende Referate innerhalb der Generaldirektion „Kommunikationsnetze, Inhalte und Technologien" vorsieht[16]:

- *Regulierung und Compliance* – insb. Überwachung von GPAI-Modellen auf Unionsebene
- *KI-Sicherheit* – Ermittlung systemischer Risiken von GPAI-Modellen und Risikominderungsmaßnahmen,
- *Exzellenz im Bereich KI und Robotik* – Forschungs- und Entwicklungsmaßnahmen im Bereich von KI,
- *KI für das Gemeinwohl* – Europäische KI-Initiativen in zentralen gesellschaftspolitischen Fragen, etwa zur Krebsdiagnostik sowie
- *KI-Innovation und Politikkoordinierung* – Überwachung der KI-Strategie und -Investitionen, Einrichtung von KI-Reallaboren.

Eine weitere Aufgabe des AI Office wird es sein, sog. „Verhaltenskodizes"[17] zu entwickeln (Art. 95 KI-Verordnung). Für KI-Systeme, die keiner bestimmten Risiko-Kategorie der KI-Verordnung unterfallen – etwa intelligente Spam-Filter oder einfache Chat-Bots – besteht die Möglichkeit, sich im Sinne einer „Best-Practice" nach Art. 95 KI-Verordnung freiwillig dem vom AI Office auszuarbeitenden Verhaltenskodex zu unterwerfen. Hierdurch soll sich mittel- bis langfristig ein gewisser „KI-Goldstandard" entwickeln, eine Idee, die man in ähnlicher Form schon im Zusammenhang mit der Datenschutzgrundverordnung kennt.

Last but not least soll das AI Office die Europäische Kommission bei der Ausarbeitung von Leitlinien, Durchführungsrechtsakten und delegierten Rechtsakten zur Umsetzung der KI-Verordnung unterstützen. Während die Leitlinien (Art. 96 KI-Verordnung) rechtsunverbindlich dazu dienen sollen, die Umsetzung der Anforderungen der KI-Verordnung in der täglichen Praxis zu erleichtern – etwa durch adressatenbezogene Handlungsempfehlungen zur Umsetzung der aus der Verordnung resultierenden Pflichten – bieten delegierte Rechtsakte der Kommission die Möglichkeit, ausgewählte Regelungsbereiche der KI-Verordnung im Nachgang und Bedarfsfall anzupassen und zu ergänzen – etwa zur nachträglichen Einstufung eines neu in Verkehr gebrachten KI-Systems als „hochrisikoreich", um mit dem technologischen Fortschritt auch in rechtlicher Hinsicht Schritt halten zu können. Durchführungsrechtsakte der Kommission präzisieren hingegen bereits durch die KI-Verordnung geregelte Bereiche.

4. KI-Pakt

Keine durch die KI-Verordnung geregelte Institution, gleichwohl existent und daher erwähnenswert, ist der sogenannte KI-Pakt. Unter dieser Bezeichnung haben sich Unternehmen verschiedenster Größe und Branchen freiwillig zusammengeschlossen, um mit der Umsetzung der Anforderungen der KI-Verordnung unter Federführung des AI Office schon vor Ablauf der gesetzlichen Umsetzungsfristen zu beginnen.[18] Idee des KI-Pakts ist es, interessierten Unternehmen eine Plattform zum gegenseitigen Austausch zu bieten und diese zu motivieren, frühzeitig Maßnahmen zur Umsetzung der Anforderungen der KI-Verordnung anzugehen.

Die von Unternehmen, die sich dem KI-Pakt anschließen, zu unterzeichnenden Beitrittserklärungen enthalten unter anderem die Verpflichtung zur Umsetzung der folgenden drei Kernmaßnahmen:

- Annahme einer KI-Governance-Strategie, um die Einführung von KI in ihrer Organisation zu fördern und auf die künftige Einhaltung des KI-Gesetzes hinzuarbeiten,

---

13 Vgl. ErwG 148, 151 KI-Verordnung.

14 https://ec.europa.eu/commission/presscorner/detail/de/qanda_21_1683 (letzter Abruf: 17.10.2024).

15 Vgl. ErwG 150 KI-Verordnung.

16 Press Release 29 May 2024 – Commission establishes AI Office to strengthen EU leadership in safe and trustworthy Artificial Intelligence, abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2982 (letzter Abruf: 17.10.2024).

17 Vgl. ErwG 116 KI-Verordnung.

18 https://digital-strategy.ec.europa.eu/de/policies/ai-pact (letzter Abruf: 17.10.2024).

- Identifizierung und Kartierung von KI-Systemen, die nach der KI-Verordnung aller Voraussicht nach als Hochrisiko-KI einzustufen sind, und
- Förderung eines gesunden Bewusstseins für KI, Etablierung von Kompetenzen zu ihrer verantwortungsvollen Verwendung sowie die Gewährleistung einer ethischen und verantwortungsvollen KI-Entwicklung.[19]

Ob der KI-Pakt den Teilnehmenden einen echten Mehrwert bietet, bleibt abzuwarten. Die durch den KI-Pakt eröffneten Möglichkeiten, Lösungen auszutesten, zu teilen und so unter Umständen Compliance mit der KI-Verordnung voranzutreiben, ist dennoch zu begrüßen und hat – jedenfalls auf dem Papier – Potenzial, einen sicheren und verlässlichen Umgang mit KI im Einklang mit der KI-Verordnung zu stärken.

IV. Kompetenzen auf nationaler Ebene

1. Grundkonzept

Die Struktur der Zuständigkeiten auf nationaler Ebene wirkt auf den ersten Blick einfach gestrickt. Zuständige nationale Behörden soll es nach der KI-Verordnung zwei geben: Die notifizierende Behörde und die Marktüberwachungsbehörde. Beide müssen die Mitgliedstaaten nach dem Wortlaut von Art. 70 Abs. 1 Satz 1 KI-Verordnung „einrichten oder benennen", was bedeutet, dass Deutschland hierfür entweder eine eigene neue Behörde zu schaffen oder die Aufgaben bestehenden Behörden zu übertragen hat. Eine Marktüberwachungsbehörde muss daneben für den jeweiligen Mitgliedstaat als sogenannte zentrale Anlaufstelle für Fragen rund um die KI-Verordnung dienen. Geeignete Stellen gibt es hierfür viele.[20]

2. Supranationale Naivität trifft deutschen Föderalismus

Auf EU-Ebene fungiert der Europäische Datenschutzbeauftragte als zuständige Marküberwachungsbehörde. Der Europäische Datenschutzausschuss hat sich dafür ausgesprochen, den Datenschutzbehörden auch auf nationaler Ebene die Aufgaben der Marktaufsichtsbehörden zu übertragen, dies zumindest für bestimmte Hochrisiko-KI-Systeme. Ferner sollen die nationalen Datenschutzbehörden nach den Vorstellungen des Europäischen Datenschutzausschusses die Funktion der zentralen Anlaufstelle für KI wahrnehmen.[21]

Wie eine sinnvolle Aufteilung zwischen den 17 Landesdatenschutzbehörden und dem Bundesbeauftragten für Datenschutz aussähe, oder ob Letzterer die Aufgaben der Marktüberwachungsbehörde zentralisiert wahrnehmen soll, bleibt bislang offen; unterschiedliche Stellen befürworten hier unterschiedliche Ansätze.[22] Allerdings könnten auch innerhalb der Bundesnetzagentur, des Bundesamtes für Sicherheit in der Informationstechnik („BSI") und/oder dem Bundeskartellamt entsprechende Kompetenzen geschaffen werden. Schenkt man dem neuesten „Leak" eines Thesenpapiers[23] aus der Politik Glauben, würde die Bundesnetzagentur die Funktion der Marktüberwachungsbehörde, der notifizierenden Behörde und zentralen Anlaufstelle übernehmen – mit Bereichsausnahmen für KI, die in bereits regulierten Produkten zum Einsatz kommt, sowie Mitwirkungsmöglichkeiten der genannten anderen Behörden in ihren jeweiligen fachlichen Kompetenzbereichen.[24]

Was auf den ersten Blick durchschaubar scheint, entpuppt sich bei näherem Hinsehen, insbesondere aus der Sicht von Akteuren, die europaweit tätig sind, eher als Behördendschungel. So steht es den Mitgliedstaaten gemäß Art. 70 Abs. 1 Satz 4 KI-Verordnung etwa frei, Aufgaben „gemäß den organisatorischen Erfordernissen" auf mehrere Behörden zu verteilen. Daneben gibt es eine Reihe spezieller Fälle und Ausnahmen, in denen die KI-Verordnung bereits vorschreibt, wer als Marktüberwachungsbehörde zu fungieren hat (hierzu näher unter IV.4.). Soweit bestehende Harmonisierungsvorschriften der Union Anwendung finden, gilt die dort für die Marktüberwachung benannte Behörde auch als Marktüberwachungsbehörde für die Zwecke der KI-Verordnung (Art. 74 Abs. 3 KI-Verordnung). Dies wären im Anwendungsbereich der Maschinen-Richtlinie 95/16/EG in Deutschland gemäß § 25 Abs. 1 Satz 1 ProdSG die nach Landesrecht zuständigen Behörden, in Nordrhein-Westfalen damit die Bezirksregierungen (§ 1 Abs. 1 S. 1 ZustVO ArbtG i. V. m. Nr. 3 Anlage 1 ZustVO ArbtG). Doch auch hiervon können die Mitgliedstaaten nach Art. 74 Abs. 3 Satz 2 KI-Verordnung „unter geeigneten Umständen" Rückausnahmen vorsehen. Steht Inverkehrbringen, Inbetriebnahme oder Verwendung eines Hochrisiko-KI-Systems in direktem Zusammenhang mit Finanzdienstleistungen, gilt für diese Finanzdienstleistungen die hierfür zuständige nationale Behörde – in Deutschland demnach die Bundesanstalt für Finanzdienstleistungsaufsicht („BaFin") – als Marktüberwachungsbehörde für die Zwecke der KI-Verordnung (Art. 74 Abs. 6 KI-Verordnung). Aber auch hier können die Mitgliedstaaten wiederum Ausnahmen vorsehen (Art. 74 Abs. 7 KI-Verordnung). Darüber hinaus sollen für Hochrisiko-KI-Systeme im Zusammenhang mit „Biometrie", „Strafverfolgung", „Migration, Asyl und Grenzkontrolle" sowie „Rechtspflege und demokratische Prozesse" die Datenschutzaufsichtsbehörden als Marktüberwachungsbehörden zuständig sein (Art. 74 Abs. 8 KI-Verordnung). Zu alledem tritt dann auch noch das AI Office auf den Plan, sofern es um die Überwachung und Beaufsichtigung der Konformität eines KI-Systems geht, das auf einem KI-Modell mit allgemeinem Verwendungszweck beruht und Modell und System vom selben Anbieter entwickelt worden sind (Art. 75 Abs. 1 KI-Verordnung).

Einige wenige europäische Länder sind beim Thema KI-Governance bereits etwas weiter: Spanien etwa hat schon im letzten Jahr eine eigene Behörde für die Überwachung von KI geschaffen.[25] In den Niederlanden will die Datenschutzaufsichtsbehörde eine wichtige Rolle im Rahmen der Marktüberwachung einnehmen, empfahl jedoch

19 Der Text der unterzeichnenden Beitrittserklärungen ist unter https://ec.europa.eu/newsroom/dae/redirection/document/107430 abrufbar (letzter Abruf: 17.10.2024).

20 Vgl. z.B. https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/nationale-ki-aufsicht (letzter Abruf: 17.10.2024).

21 https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_de (letzter Abruf: 17.10.2024).

22 Vgl. etwa https://www.tagesschau.de/wirtschaft/digitales/ai-act-kuenstliche-intelligenz-regulierung-100.html (letzter Abruf: 17.10.2024).

23 https://www.businessinsider.de/politik/bi-papers/bundesregierung/thesenpapier-zur-ki-governance-struktur-diese-deutsche-behoerde-soll-den-markt-fuer-kuenstliche-intelligenz-beaufsichtigen/?purchase=true (Abruf kostenpflichtig).

24 Siehe dazu auch https://www.heise.de/news/KI-Verordnung-Bundesregierung-verraet-Aufsichtsregime-Plan-9954083.html (letzter Abruf: 17.10.2024); nach jüngsten Berichten wird die BNetzA tatsächlich die Rolle der Marktüberwachungsbehörde übernehmen, siehe https://www.haufe.de/recht/weitere-rechtsgebiete/wirtschaftsrecht/nationale-marktueberwachungsbehoerde-bei-der-ki-aufsicht_210_635468.html (letzter Abruf: 6.11.2024).

25 https://www.trendingtopics.eu/spanien-will-sich-mit-eigener-ki-behoerde-als-fuehrende-ai-nation-positionieren/#:~:text=Durch%20die%20Einf%C3%BChrung%20der%20AESIA,Digitalisierung%20und%20K%C3%BCnstliche%20Intelligenz%20geleitet (letzter Abruf: 17.10.2024).

vor kurzem, sektorspezifische Überwachung so weit wie möglich in bestehende Überwachungsstrukturen einzugliedern, z.B. dort, wo bereits CE-Kennzeichnungen vorgeschrieben sind.[26] Auch Österreich hat eine „KI-Servicestelle" eingerichtet, bezeichnet diese jedoch lediglich als „eine wichtige Wissens- und Erfahrungsquelle" für die notifizierenden und Marktüberwachungsbehörden.[27]

3. Notifizierende Behörde

Die notifizierende Behörde ist gemäß Art. 28 Abs. 1 Satz 1 KI-Verordnung zuständig für die Bewertung, Benennung, Notifizierung und Überwachung von Konformitätsbewertungsstellen. Konformitätsbewertungsstellen, bzw. sobald notifiziert, notifizierte Stellen, überprüfen gemäß Art. 34 Abs. 1 KI-Verordnung die Konformität, das heißt die Übereinstimmung von Hochrisiko-KI-Systemen mit den Anforderungen der Art. 8–15 KI-Verordnung, anhand der in Art. 43 KI-Verordnung festgelegten Konformitätsbewertungsverfahren. Gemäß Art. 16 lit. f) KI-Verordnung muss jeder Anbieter eines Hochrisiko-KI-Systems sicherstellen, dass dieses vor seinem Inverkehrbringen oder seiner Inbetriebnahme ein solches Konformitätsbewertungsverfahren durchlaufen hat. Die Bewertung und Überwachung von Konformitätsbewertungsstellen kann gemäß Art. 28 Abs. 2 KI-Verordnung alternativ von Akkreditierungsstellen durchgeführt werden. In Deutschland wäre dies die Deutsche Akkreditierungsstelle GmbH („DAkkS"). Die Entscheidung hierüber obliegt dem jeweiligen Mitgliedsstaat in eigener Verantwortung.

a) Organisation

Die zu etablierende Organisation der notifizierenden Behörde ist in Art. 28 KI-Verordnung grob umrissen: Sie muss demnach mit in den Bereichen IT, KI und Recht ausreichend kompetenten Mitarbeitern ausgestattet sein. Interessenkonflikte mit Konformitätsbewertungsstellen sind bereits qua Organisation zu vermeiden, um die Objektivität und Unparteilichkeit ihrer Tätigkeit zu gewährleisten. Es ist sicherzustellen, dass Konformitätsbewertungsverfahren, die ein wesentliches Quality Gate auf dem Weg eines Hochrisiko-KI-Systems in den Markt hinein darstellen, objektiv und kompetent ablaufen. Hier darf gar nicht erst der Eindruck entstehen, dass eine notifizierende Behörde genehme oder verbundene Konformitätsbewertungsstellen notifizieren könnte, zum Leidwesen der Qualität durchzuführender Konformitätsbewertungsverfahren. Dies erfordert unter anderem eine klare organisatorische Trennung von der Bewertung einer Konformitätsbewertungsstelle und der Entscheidung über ihre Notifizierung. Daneben ist es der notifizierenden Behörde gemäß Art. 28 Abs. 5 KI-Verordnung untersagt, gleiche oder ähnliche Leistungen wie die Konformitätsbewertungsstellen zu erbringen.

b) Notifizierung

Die Notifizierung, das heißt ihre Benennung als sogenannte notifizierte Stelle (Art. 3 Nr. 22 KI-Verordnung), erfolgt auf Antrag der Konformitätsbewertungsstelle gemäß Art. 29 KI-Verordnung bei der notifizierenden Behörde, und zwar dann, wenn die Konformitätsbewertungsstelle die Anforderungen von Art. 31 KI-Verordnung erfüllt (Art. 30 Abs. 1 KI-Verordnung). Zu den vorgenannten Voraussetzungen zählen eine eigene Rechtspersönlichkeit, angemessene Ressourcenausstattung und Cybersicherheit ebenso wie die Voraussetzung der Unabhängigkeit, insbesondere von Anbietern von Hochrisiko-KI-Systemen, aber auch hinreichende (Fach)Kompetenz. Wie die Anforderungen an Ressourcenausstattung oder Cybersicherheit letztlich genau aussehen sollen, ergibt sich aus der KI-Verordnung selbst nicht. Allerdings liegt es nahe, dass die Anforderungen von Art. 31 KI-Verordnung erfüllt sein dürften, soweit eine Konformitätsbewertungsstelle nachweist, dass sie die Kriterien einschlägiger harmonisierter Normen erfüllt (Art. 32 KI-Verordnung).[28]

c) Aufgaben

Die notifizierende Behörde hat die Kommission und die übrigen Mitgliedstaaten über alle notifizierten Stellen, über alle Änderungen von Notifizierungen sowie alle Einschränkungen, Aussetzungen oder Widerrufe von Benennungen zu unterrichten. Die Letztentscheidung über die Notifizierung obliegt der notifizierenden Behörde gleichwohl nicht. Hat sie eine Konformitätsbewertungsstelle notifiziert, können die Kommission, aber auch andere Mitgliedstaaten, innerhalb von zwei Wochen bzw. zwei Monaten, je nachdem, welche Unterlagen im Verfahren vorgelegt wurden, Einwände erheben (Art. 30 Abs. 4 KI-Verordnung). Unterbleiben solche Einwände, darf die Konformitätsbewertungsstelle die Tätigkeiten einer notifizierten Stelle wahrnehmen. Im Falle von Einwänden entscheidet die Kommission nach Konsultation der betreffenden Mitgliedstaaten und der Konformitätsbewertungsstelle. Auch ist es die Kommission, die Identifizierungsnummern an notifizierte Stellen vergibt und ein entsprechendes Verzeichnis verwaltet (Art. 35 KI-Verordnung).

4. Marktüberwachungsbehörde

Die Aufgaben der Marktüberwachungsbehörden sind komplexer und umfangreicher. Sie sind beispielsweise zuständig für

- die Entgegennahme von Mitteilungen und Informationen unter der KI-Verordnung, insbesondere im Zusammenhang mit Hochrisiko-KI-Systemen;[29]
- die ausnahmsweise Genehmigung des Inverkehrbringens oder der Inbetriebnahme bestimmter Hochrisiko-KI-Systeme ohne das vorherige Durchlaufen eines Konformitätsbewertungsverfahrens aus „außergewöhnlichen Gründen der öffentlichen Sicherheit, des Schutzes des Lebens und der Gesundheit von Personen, des Umweltschutzes oder des Schutzes wichtiger Industrie- und Infrastrukturanlagen" (Art. 46 Abs. 1 KI-Verordnung);
- die Genehmigung von Tests von Hochrisiko-KI-Systemen außerhalb von KI-Reallaboren (Art. 60 Abs. 4 KI-Verordnung) sowie die Überprüfung der Einhaltung insoweit einschlägiger Anforderungen;
- die Entgegennahme von Meldungen schwerwiegender Vorfälle, das heißt Vorfällen oder Fehlfunktionen eines KI-Systems, die zum Tod oder einer schweren Gesundheitsschädigung einer Person, einer schweren und unumkehrbaren Störung der Verwaltung oder des Betriebs kritischer Infrastrukturen, der Verletzung von unionsrechtlichen Pflichten zum Schutz der Grundrechte oder schweren Sach- oder Umweltschäden führen können (Art. 73 KI-Verordnung), sowie
- die Durchführung technischer Tests an Hochrisiko-KI-Systemen auf Antrag einer zum Schutz der Unionsgrundrechte berufenen Behörde oder öffentlichen Stelle zum Zwecke der Feststellung, ob in Bezug auf ein in Anhang III der KI-Verordnung genanntes Hochrisiko-KI-System ein Verstoß gegen Unionsgrundrechte vorliegt (Art. 77 KI-Verordnung).

---

26 https://www.autoriteitpersoonsgegevens.nl/en/current/ap-and-rdi-supervision-of-ai-systems-requires-cooperation-and-must-be-arranged-quickly (letzter Abruf: 17.10.2024).

27 https://www.digitalaustria.gv.at/Themen/KI.html (letzter Abruf: 17.10.2024).

28 D.h. zum Beispiel DIN- oder ISO-Normen.

29 Siehe z.B. Art. 20 Abs. 2 KI-Verordnung.

Für Konformitätsbewertungsverfahren für Hochrisiko-KI-Systeme gemäß Anhang VII der KI-Verordnung (das heißt Konformitätsbewertungsverfahren auf der Grundlage einer Bewertung des Qualitätsmanagementsystems und einer Bewertung der technischen Dokumentation) die von Strafverfolgungs-, Einwanderungs- oder Asylbehörden oder von Organen, Einrichtungen oder sonstigen Stellen der Union in Betrieb genommen werden, übernimmt die Marktüberwachungsbehörde zugleich die Funktion der notifizierten Stelle (Art. 43 Abs. 1 Unterabs. 2 KI-Verordnung). Im Zusammenhang mit Tests von Hochrisiko-KI-Systemen unter Realbedingungen gemäß Art. 60 KI-Verordnung haben die Marktüberwachungsbehörden unter anderem die Aufgabe, solche Tests auf Antrag der (zukünftigen) Anbieter zu genehmigen, deren ordnungsgemäße Durchführung sowie das damit zusammenhängende Hochrisiko-KI-System zu überprüfen und Meldungen über schwerwiegende Vorfälle im Verlauf eines solchen Tests entgegenzunehmen.

a) Marktüberwachung als Kern der Tätigkeit

Den Kern der Tätigkeiten der Marktüberwachungsbehörden stellt, wie in ihrer Bezeichnung angelegt, jedoch die Überwachung der Akteure der KI-Verordnung dar. Insoweit finden die Regelungen der Verordnung (EU) 2019/1020 („Marktüberwachungsverordnung") in leicht modifizierter Form Anwendung (Art. 74 Abs. 1 KI-Verordnung).[30] Vergleichbar mit den Aufsichts- und Durchsetzungskompetenzen des AI Office bei GPAI-Modellen sind auch die Kompetenzen der Marktüberwachungsbehörde auf nationaler Ebene gelagert: Hat die Marktüberwachungsbehörde „hinreichend Grund zu der Annahme", dass KI-Systeme ein Risiko bergen, prüft sie, beispielsweise auf der Basis hierzu angeforderter Informationen und Dokumente nach Art. 21 Abs. 1 KI-Verordnung, ob die Anforderungen und Pflichten der KI-Verordnung erfüllt sind, und fordert, falls dies nicht der Fall ist, den jeweiligen Akteur auf, Korrekturmaßnahmen zu ergreifen, das KI-System vom Markt zu nehmen oder es zurückzurufen (Art. 79 Abs. 2 Unterabs. 1 KI-Verordnung). Daneben sind „geeignete einschränkende Maßnahmen" in Bezug auf das Produkt oder KI-System zu treffen, wie etwa die Aufforderung, das betreffende Produkt oder KI-System unverzüglich vom Markt zu nehmen (Art. 79 Abs. 9 KI-Verordnung).

b) Weitere Befugnisse

Art. 14 der Marktüberwachungsverordnung sieht daneben eine Vielzahl weiterer Befugnisse vor, die die Mitgliedstaaten den Marktüberwachungsbehörden ebenfalls übertragen können. Danach kann die Marktüberwachungsbehörde z. B. auf eigene Initiative Ermittlungen einleiten, Dokumente, Daten und Informationen anfordern, Räumlichkeiten oder Grundstücke betreten oder Fern- oder Vor-Ort-Inspektionen durchführen.

c) Zentrale Anlaufstelle

Der Marktüberwachungsbehörde kommt, wie erwähnt, auch die Aufgabe der sogenannten zentralen Anlaufstelle für Themen rund um die KI-Verordnung zu. Ob und inwieweit mit dieser Rolle weitere Besonderheiten, Verpflichtungen oder Zuständigkeiten einhergehen, bleibt offen. Nach Erwägungsgrund 153 zur KI-Verordnung verspricht sich der Gesetzgeber aus der Aufgabe als zentrale Anlaufstelle offenbar mehr Effizienz aufseiten der Mitgliedstaaten und etabliert ein Sprachrohr für die Öffentlichkeit. Da auf ihrer Seite Informationen gebündelt zusammentreffen, liegt eine weitere Zusammenarbeit mit den Europäischen Gremien, z. B. bei der Erarbeitung von Praxisleitfäden (die gemäß Art. 56 KI-Verordnung zunächst nicht verbindlich sind, jedoch deren ordnungsgemäße Anwendung sicherstellen sollen, aber gemäß Art. 56 Abs. 6 KI-Verordnung auch von der Kommission im Wege eines Durchführungsakts genehmigt werden können, um ihnen allgemeine Gültigkeit zu verleihen), nicht außerhalb der Wahrscheinlichkeit (Art. 56 Abs. 3 KI-Verordnung).

V. Praktische Erwägungen und Ausblick

Es darf mit Spannung erwartet werden, wie der deutsche Gesetzgeber die einzelnen Kompetenzen im nationalen Behördendschungel verteilen wird. Das von der KI-Verordnung propagierte KI-Governance-Modell ist für sich bereits ausreichend kompliziert und verlangt in seiner nationalen Spezifizierung eher nach Pragmatismus als nach weiterer Verkomplizierung. Die aus dem eingangs erwähnten Thesenpapier hervorgehenden Ansätze erscheinen logisch und sinnvoll. Insbesondere ist der gesetzgeberische Ansatz, der Bundesnetzagentur – nicht den nationalen Datenschutzbehörden – im Grundsatz die Funktion der Marktüberwachungsbehörde, der notifizierenden Behörde und der zentralen Anlaufstelle zu übertragen, zu begrüßen. Zur Umsetzung der gesetzgeberischen Intention, nicht nur das Vertrauen in sichere KI, sondern auch ihre Innovation zu fördern, scheint die Bundesnetzagentur aufgrund ihrer technischen Affinität und Marktnähe eher geeignet als die erfahrungsgemäß eher von überwiegend protektivem Mindset geprägten Datenschutzbehörden – abgesehen davon, dass es in Deutschland von Letzteren 18 verschiedene gibt. Dennoch wären die angedachten Mitwirkungsmöglichkeiten von BfDI, BSI, BKartA und BaFin klar und unmissverständlich gesetzgeberisch auszugestalten, um ein zwischenbehördliches Kompetenz-Wirrwarr zu vermeiden.

Die Planung eines Gesetzesentwurfs noch im Herbst 2024, wie aus dem Thesenpapier ersichtlich, erscheint angesichts der noch klärungsbedürftigen Punkte äußert ambitioniert. So sind ausweislich des Thesenpapiers zunächst noch Gesetzgebungskompetenzen zu klären, bevor man den Diskurs in Richtung einer konkreten Ausgestaltung von Organisations- und Zuständigkeitsstrukturen sowie der Zusammenarbeit der einzelnen Behörden führen kann, von Stakeholder-Beteiligungen ganz zu schweigen. Bleibt zu hoffen, dass der Gesetzgeber die Durchführungsfristen nicht bereits in diesem frühen Stadium verpasst, was unter anderem auch für das zum 2.8.2025 in Kraft tretende Bußgeldregime nicht ohne Konsequenzen bliebe.

Schließlich bleibt abzuwarten, wieweit das AI Office auf europäischer Ebene der Vielzahl seiner Durchsetzungs- sowie Forschungs-, Entwicklungs- und gesellschaftspolitischen Kompetenzen bei der Entwicklung und Anwendung von KI-Systemen in der Union nachkommen wird. Die Idee des Europäischen Gesetzgebers, mit dem AI Office eine zentrale Institution zu schaffen, die – mittels beratender Gremien – Experten aus Wissenschaft, Industrie, Thinktanks und der Zivilgesellschaft bei Fragen und Entscheidungen im Zusammenhang mit Künstlicher Intelligenz einbezieht, ist grundsätzlich positiv zu bewerten. Der Ansatz verspricht das Potenzial, Wissen aus verschiedensten Bereichen bündeln und im Rahmen der Entscheidungsprozesse berücksichtigen zu können. Gleichzeitig birgt der Ansatz die Gefahr komplexer und langwieriger Entscheidungsprozesse.

Wie die Europäische Kommission mit diesen Herausforderungen umgehen und ob es gelingen wird, eine angemessene Balance

30 Abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R1020 (letzter Abruf: 17.10.2024).

zwischen Innovation und Regulierung zu finden, bleibt ebenso spannend wie zu hoffen, dass auch unser nationaler Gesetzgeber Behördenkontakte im Zusammenhang mit KI praktikabler ausgestalten wird als die Prozesse um Passierschein A38. Will heißen: Unsere gewählten Volksvertreter haben es noch in der Hand. Hoffen wir, dass sie vorher *Asterix* gelesen haben.

AUTOREN

Dr. Thorsten Ammann *ist Rechtsanwalt und Partner bei DLA Piper UK LLP in Köln und Frankfurt. Schwerpunkte seiner Tätigkeit sind digitale Transformationsprojekte und die Implementierung disruptiver Technologien, insbesondere Künstlicher Intelligenz.*

Florian Achnitz, *LL.M., ist Rechtsanwalt und Associate bei DLA Piper UK LLP in Köln und berät national und international operierende Unternehmen zu Rechtsfragen in den Bereichen Informationstechnologie, IT-Sicherheit, Telekommunikation und Künstliche Intelligenz.*

Ludwig Lauer *ist Rechtsreferendar am OLG Köln und absolviert zur Zeit seine Anwaltsstation bei DLA Piper UK LLP in Köln.*

CB-NEWS

Bundesregierung: Entwurf zur NIS-2-Umsetzung vorgelegt

Die Bundesregierung hat einen Gesetzentwurf zur Umsetzung der sogenannten NIS-2-Richtlinie der EU vorgelegt, der zugleich der „Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ (Drucksache 20/13184) dienen soll.

Die unionsrechtlichen Vorgaben der NIS-2-Richtlinie sollen im Rahmen einer Novellierung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) sowie einzelner Fachgesetze umgesetzt werden. Zusätzlich werden entsprechende Vorgaben für die Bundesverwaltung eingeführt.

Schwerpunktmäßig sieht der Entwurf folgende Änderungen vor:

- Einführung der durch die NIS-2-Richtlinie vorgegebenen Einrichtungskategorien, die mit einer signifikanten Ausweitung des bisher auf Betreiber Kritischer Infrastrukturen, Anbieter digitaler Dienste und Unternehmen im besonderen öffentlichen Interesse beschränkten Anwendungsbereichs einhergeht.
- Der Katalog der Mindestsicherheitsanforderungen des Artikels 21 Absatz 2 NIS-2-Richtlinie wird in das BSI-Gesetz übernommen, wobei in der Intensität der jeweiligen Maßnahme aus Gründen der Verhältnismäßigkeit zwischen den Kategorien ausdifferenziert wird.
- Die bislang einstufige Meldepflicht bei Vorfällen wird durch das dreistufige Melderegime der NIS-2-Richtlinie ersetzt. Dabei soll der bürokratische Aufwand für die Einrichtungen im Rahmen des bestehenden mitgliedstaatlichen Umsetzungsspielraums minimiert werden.
- Ausweitung des Instrumentariums des Bundesamts für Sicherheit in der Informationstechnik (BSI) im Hinblick auf von der NIS-2-Richtlinie vorgegebene Aufsichtsmaßnahmen.
- Gesetzliche Verankerung wesentlicher nationaler Anforderungen an das Informationssicherheitsmanagement des Bundes und Abbildung der zugehörigen Rollen und Verantwortlichkeiten.
- Harmonisierung der Anforderungen an Einrichtungen der Bundesverwaltung aus nationalen und unionsrechtlichen Vorgaben, um ein insgesamt kohärentes und handhabbares Regelungsregime zu gewährleisten.
- Etablierung eines CISO Bund als zentralem Koordinator für Maßnahmen zur Informationssicherheit in Einrichtungen der Bundesverwaltung und zur Unterstützung der Ressorts bei der Umsetzung der Vorgaben für das Informationssicherheitsmanagement.

Ziel der NIS-2-Richtlinie ist die Einführung verbindlicher Maßnahmen für Verwaltung und Wirtschaft, mit denen in der gesamten Europäischen Union ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden soll. Wichtige und besonders wichtige Einrichtungen sollen vor Schäden durch Cyberangriffe geschützt und das Funktionieren des europäischen Binnenmarktes verbessert werden.

(Aus dem Gesetzentwurf der Bundesregierung, Drucksache 20/13184, vom 2.10.2024)

BAFA: Berichtspflicht erneut verschoben

Vor dem Hintergrund der Entwicklungen zur Umsetzung der unionsrechtlichen Vorgaben hinsichtlich der Nachhaltigkeitsberichterstattung von Unternehmen (Richtlinie (EU) 2022/2464) wird das BAFA erstmalig zum Stichtag 1.1.2026 das Vorliegen der Berichte nach dem LkSG sowie deren Veröffentlichung prüfen. Auch wenn die Übermittlung eines Berichts an das BAFA und dessen Veröffentlichung nach dem LkSG bereits vor diesem Zeitpunkt fällig war, wird das BAFA die Überschreitung der Frist nicht sanktionieren, sofern der Bericht spätestens zum 31. Dezember 2025 beim BAFA vorliegt.

Die Erfüllung der übrigen Sorgfaltspflichten gemäß der §§ 4 bis 10 Absatz 1 LkSG sowie deren Kontrolle und Sanktionierung durch das BAFA, für welche auch Angaben aus einem Bericht Anlass geben können, werden von dieser Stichtagsregelung nicht berührt.

(Meldung BAFA vom 25.10.2024)

Compliance-Berater Zitierweise CB: / ISSN 2195-6685

CHEFREDAKTION:
Dr. Malte Passarge
HUTH DIETRICH HAHN Rechtsanwälte
Partnerschaftsgesellschaft mbB
Neuer Jungfernstieg 17
20354 Hamburg
Tel.: +49 40 41 525 0
Passarge@HDH.net

REDAKTION:
Christina Kahlen-Pappas, Tel. 0151-27 24 56 63,
christina.kahlen-pappas@dfv.de

HERAUSGEBER:
Prof. Dr. Frank Beine, WP / StB
Jörg Bielefeld
Hanno Hinzmann
Univ.-Prof. Dr. Annemarie Matusche-Beckmann
Dr. Dirk Christoph Schautes
Prof. Dr. Martin Schulz, LL.M. (Yale)
Eric S. Soong
Prof. Dr. Gregor Thüsing, LL.M. (Harvard), Attorney at law (New York)
Dr. Martin Wienke

BEIRAT:
Dr. Martin Auer
Dr. Martin Bünning, RA / StB
Dr. José Campos Nave, RA / FAHaGesR / FAStR
Dr. Peter Christ, RA / FAArbR
Dr. Katharina Hastenrath
Dr. Susanne Jochheim, RAin
Dr. Ulf Klebeck, RA
Kai Leisering
Tobias Neufeld, LL.M. (London), RA / FAArbR, Solicitor (England & Wales)
Jürgen Pauthner, LL.M. (San Diego), MBA
Mario Prudentino, RA
Dr. Manfred Rack, RA
Dr. Sarah Reinhardt, RAin / FAArbR
Dr. Roman Reiß, RA / FAStR
Gunther A. Weiss, LL.M. (Yale), RA, Attorney at law (New York), Advokát (Praha)
Wolfgang Werths
Tim Wybitul, RA / FAArbR
Prof. Dr. Dr. Jörg Zehetner, RA

dfv Mediengruppe

VERLAG: Deutscher Fachverlag GmbH,
Mainzer Landstr. 251, 60326 Frankfurt am Main,
Tel. 069-7595-2788, Fax 069-7595-2780,
Internet: www.dfv.de

GESCHÄFTSFÜHRUNG: Peter Esser (Sprecher), Thomas Berner, Markus Gotta
AUFSICHTSRAT: Andreas Lorch, Catrin Lorch, Dr. Edith Baumann-Lorch, Peter Ruß
GESAMTVERLAGSLEITUNG FACHMEDIEN RECHT UND WIRTSCHAFT: Torsten Kutschke
Tel. 0 69-75 95-27 01, Torsten.Kutschke@dfv.de

REGISTERGERICHT: AG Frankfurt am Main, HRB 8501

BANKVERBINDUNG: Frankfurter Sparkasse, Frankfurt am Main, Kto.-Nr. 34 926 (BLZ 500 502 01)

In der dfv Mediengruppe, Fachmedien Recht und Wirtschaft, erscheinen außerdem folgende Fachzeitschriften: Betriebs-Berater (BB), Datenschutz-Berater (DSB), Diversity in Recht & Wirtschaft (DivRuW), Europäisches Wirtschafts- und Steuerrecht (EWS), Geldwäsche & Recht (GWuR), Zeitschrift zum Innovations- und Technikrecht (InTeR), Kommunikation & Recht (K&R), Logistik und Recht (LogR), Netzwirtschaften & Recht (N&R), Recht Automobil Wirtschaft (RAW), Recht der Internationalen Wirtschaft (RIW), Recht der Finanzinstrumente (RdF), Recht der Zahlungsdienste (RdZ), Sanierungs-Berater (SanB), Der Steuerberater (StB), Wettbewerb in Recht und Praxis (WRP), Zeitschrift für das gesamte Handels- und Wirtschaftsrecht (ZHR), Zeitschrift für Umweltpolitik & Umweltrecht (ZfU), Zeitschrift für Wett- und Glücksspielrecht (ZfWG), Zeitschrift für das gesamte Lebensmittelrecht (ZLR), Zeitschrift für Neues Energierecht (ZNER) und Zeitschrift für Vergleichende Rechtswissenschaft (ZVglRWiss).

ANZEIGEN:
Matthias Betzler, Tel. +49 69 7595-2785,
E-Mail: matthias.betzler@dfv.de
Es gilt Preisliste Nr. 12.

Leitung Produktion: Hans Dreier, Tel. 069/7595-2463

Leitung Logistik: Ilja Sauer, Tel. 069/7595-2201

VERTRIEB: R&W Kundenservice, kundenservice@ruw.de, Tel. +49 69 7595-2788, Fax. +49 69 7595-2770

ERSCHEINUNGSWEISE: monatlich. Nicht eingegangene Hefte können nur bis zu 10 Tage nach Erscheinen des nächstfolgenden Heftes kostenlos reklamiert werden.
BEZUGSPREISE: Jahresvorzugspreis Deutschland (11 Ausgaben): 619,00 € inkl. Versandkosten und MwSt., alle weiteren Abonnement-Preise unter www.ruw.de/abo. Rechnungslegung erfolgt jährlich. Die Abonnementgebühren sind im Voraus zahlbar. Der Abonnementvertrag ist auf unbestimmte Zeit geschlossen. Eine Kündigung ist jederzeit bis 3 Monate vor Ende des Bezugszeitraumes möglich. Liegt dem Verlag zu diesem Zeitpunkt keine Kündigung vor, verlängert sich das Abonnement automatisch um ein weiteres Jahr zum dann gültigen Jahrespreis, zahlbar im Voraus. Auslandspreise auf Anfrage. Die Zeitschrift und alle in ihr enthaltenen Beiträge und Abbildungen sind urheberrechtlich geschützt.

Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen. Die Verlagsrechte erstrecken sich auch auf die veröffentlichten Gerichtsentscheidungen und deren Leitsätze, die urheberrechtlichen Schutz genießen, soweit sie vom Einsender oder von der Redaktion redigiert bzw. erarbeitet sind.

Keine Haftung für unverlangt eingesandte Manuskripte. Mit der Annahme zur Alleinveröffentlichung erwirbt der Verlag alle Rechte, einschließlich der Befugnis zur Einspeisung in eine Datenbank.

Autorenmerkblatt herunterladbar unter:
www.compliance-berater.de

© 2024 Deutscher Fachverlag GmbH, Frankfurt am Main

SATZ: DFV – inhouse production

DRUCK: medienhaus Plump GmbH, Rolandsecker Weg 33, 53619 Rheinbreitbach

VORSCHAU CB 1-2/2025

Timo Hochmuth
Betrug im Krankenhaussektor

Hartmut T. Renz
Die Aktualisierung der MaComp

Dr. Philipp Irmscher und **Christian Hellwig**
Geopolitik zwischen Strategie- und Recht(-sberatung)

Maximilian Müller
Die Geschäftsführerhaftung im internationalen Kontext

BB 47/2024

WIRTSCHAFTSRECHT

Prof. Dr. Stefan Stolte, RA
Die Verbrauchsstiftung: Praktische Einsatzmöglichkeiten, rechtliche und steuerliche Besonderheiten

Dr. Kristina Schreiber, RAin, und **Pauline Brinke**
Geschäftsführerhaftung im neuen Informationssicherheitsrecht: Kommt der Cyber-Vorstand? Auswirkungen der Umsetzung der NIS2-Richtlinie auf die Pflichten der Leitungsebene

STEUERRECHT

Dr. Axel-Michael Wagner, RA, und **Stefan Groß**, StB, CISA
Zu den neuen Vorgaben des BSI bei der Kassendatenfiskalisierung, oder: Die Grenzen administrativer Rechtssetzung im Rechtsstaat – Teil II

BILANZRECHT UND BETRIEBSWIRTSCHAFT

Ines Klein, StB/WPin, und **Dr. Holger Seidler**, RA/StB/WP
Praxisfragen bei der Änderung eines handelsrechtlichen Jahresabschlusses aufgrund von Fehlern

ARBEITSRECHT

Prof. Dr. Gerrit Horstmeier
Schadensersatz für „ungute Gefühle"? Der Art. 82 DSGVO im Arbeitsrecht

Das Compliance-Berater-Serviceteam beantwortet Ihnen alle Fragen rund um den CB
Tel. +49 69 7595-2788, Fax. +49 69 7595-2770
E-Mail: kundenservice@ruw.de