N&R
Netzwirtschaften & Recht
Energie, Telekommunikation, Verkehr und andere Netzwirtschaften

6/2025 S. 273 – 336 22. Jahrgang

dfv Mediengruppe · Frankfurt am Main

Aufsätze

Prof. Dr. *Alexander Koch*

Cyber und resilient: das IT-Sicherheitsrecht im Überblick

Die Netzwirtschaften – insbesondere Energie, Telekommunikation, Bahn und Logistik – zählen zu den kritischen Infrastrukturen, die in besonderer Weise von Informationstechnologie (IT) abhängen und über Cyberangriffe verwundbar sind. Das IT-Sicherheitsrecht ist inzwischen in einer nur noch schwer überschaubaren Fülle an Rechtsakten auf unionaler und nationaler Ebene geregelt. Der folgende Aufsatz gibt einen Überblick über die wichtigsten dieser Rechtsakte. Dabei richtet er den Blick über die Netzwirtschaften hinaus und bezieht weitere Sektoren mit ein. Insoweit bestehen zunächst Abhängigkeiten, als beispielsweise die Cybersicherheit von Endgeräten Auswirkungen auf die Sicherheit der Netze haben kann. Außerdem zeigen Vergleiche mit weiteren Sektoren, welche zukünftigen rechtlichen Entwicklungen möglicherweise bevorstehen – rein exemplarisch seien etwa die Meldezeiten für Cybervorfälle im Finanzsektor genannt, die deutlich schärfer sind als die derzeitigen Fristen in den Netzwirtschaften.

I. Einführung

Erschwert wird der Zugang zum IT-Sicherheitsrecht dadurch, dass die Begrifflichkeiten über die verschiedenen Rechtsakte hinweg nicht unbedingt intuitiv sind. So ist die Cybersicherheit von (bestimmten) Produkten nicht etwa im Rechtsakt zur Cyber*sicherheit* geregelt, sondern in der Cyber*resilienz*verordnung, während der Rechtsakt zur Cyber*sicherheit* primär auf die Cyber*resilienz* der Union abzielt (ohne den Begriff auch nur zu verwenden).

Zur Systematisierung ist zunächst zwischen Verordnungen der EU, Richtlinien und deren Umsetzungsgesetzen sowie sonstigem nationalen Recht zu differenzieren (hierzu sogleich, unter II.). Jeder weitere Systematisierungsversuch wird dadurch erschwert, dass die relevanten Rechtsakte häufig mehrere Aspekte der IT-Sicherheit adressieren. Sehr grob kann aber differenziert werden zwischen Rechtsakten, die primär auf einen Infrastrukturschutz abzielen (hierzu unten, unter III.), Rechtsakten, die primär Fragen der Produktverantwortlichkeit (aus öffentlich-rechtlicher und zivilrechtlicher Perspektive) regeln (hierzu unten, unter IV.), und sonstigen Vorschriften (hierzu – exemplarisch – unten, unter V.). Die folgenden Ausführungen orientieren sich dabei zunächst am Unionsrecht und stellen die nationalen Gesetze ggf. im Zusammenhang mit den Richtlinien vor, deren Umsetzung sie dienen.

Der Aufsatz gibt einen Überblick zu den wesentlichen Regelungen und verweist zur Vertiefung auf ausgewählte Literatur.[1] Der Schwerpunkt liegt dabei auf Bestimmungen, die sich auf die Privatwirtschaft beziehen.

Nicht betrachtet werden Rechtsakte, die primär auf eine Strafverfolgung oder Sanktionierung von Cyberangriffen abzielen. Hier wären – exemplarisch – zu nennen: die Richtlinie 2013/40/EU über Angriffe auf Informationssysteme, das Übereinkommen über Computerkriminalität des Europarates (also nicht der EU)[2] oder die Verordnung (EU) 2019/796 über restriktive Maßnahmen gegen Cyberangriffe, welche die Union oder ihre Mitgliedstaaten bedrohen[3].

II. Zusammenspiel von unionalem und nationalem Recht

Eine weitere Herausforderung für den Zugang zum IT-Sicherheitsrecht liegt darin, dass es in verschiedenen Arten von Rechtsakten geregelt ist. Hier gilt es zunächst abzuschichten: Verordnungen der EU haben nach Art. 288 UAbs. 2 AEUV allgemeine Geltung. Sie erzeugen unmittelbar Rechte und Pflichten für die jeweiligen Adressaten. Es bedarf dabei keines Umsetzungsakts. Hierdurch unterscheiden sie sich wesentlich von den Richtlinien der EU. Diese richten sich nach Art. 288 UAbs. 3 AEUV zunächst an die Mitgliedstaaten der EU und müssen ggf. von diesen in nationales Recht umgesetzt werden. Die Datenschutz-Grundverordnung 2016/679 (DSGVO) gilt etwa unmittelbar in allen Mitgliedstaaten und erzeugt (unmittelbar) Rechte und Pflichten für Bürger und Unternehmen. Die zweite Netz-und-Informations-Sicherheits-Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie) gilt hingegen nicht unmittelbar – von ihr gehen auch keine (unmittelbaren) Pflichten für Unternehmen aus.[4] Erforderlich ist hierfür eine Umsetzung in nationales Recht – etwa dem BSIG. Weiter verkompliziert wird die Rechtslage schließlich durch sog. Durchführungsrechtsakte bzw. delegierte Rechtsakte, durch die Verordnungen und Richtlinien ergänzt werden.

III. Infrastrukturschutz

Einen Schwerpunkt des Unionsrechts zur IT-Sicherheit – jedenfalls gemessen an der Anzahl der unterschiedlichen Rechtsakte – bildet der Schutz der europäischen IT-Infrastruktur. Eine ganze Reihe von Verordnungen betrifft dabei zunächst institutionelle Aspekte (hierzu sogleich, unter 1.). Hinzu kommen Vorschriften, die unmittelbar auf eine Absicherung der Infrastruktur durch die Betroffenen selbst – insbesondere die jeweiligen Unternehmen – abzielen (hierzu unten, unter 2.).

1. Institutionelle Aspekte

a) Cybersolidaritätsverordnung (EU) 2025/38

Die Cybersolidaritätsverordnung (EU) 2025/38[5] ist am 25. Januar 2025 in Kraft getreten.[6] Sie regelt die Einrichtung eines unionsweiten Netzes von „Cyber-Hubs" bzw. eines „europäischen Warnsystems für Cybersicherheit".[7] Beschließt ein Mitgliedstaat, an diesem System teilzunehmen, richtet er einen

1 Siehe außerdem *Deutsch/Eggendorfer*, K&R 2024, 169; 242.
2 Vertrag Nr. 185 des Europarates.
3 Die Verordnung listet in der Fassung der Durchführungsverordnung (EU) 2025/173 siebzehn natürliche und vier juristische Personen auf, die wegen Cyberangriffen mit Sanktionen belegt sind.
4 Siehe zu den hiermit verbundenen Problemen für Vertrauensdienste *Ritter*, CR 2025, 154.
5 Siehe hierzu *Karniyevich/Emmerich*, K&R 2025, 145.
6 Art. 25 der Cybersolidaritätsverordnung (EU) 2025/38.
7 Art. 1 Abs. 1 lit. a der Cybersolidaritätsverordnung (EU) 2025/38.

„nationalen Cyber-Hub" ein, der seiner Aufsicht untersteht.[8] Mehrere (mindestens drei) Mitgliedstaaten können ein Aufnahmekonsortium bilden und einen grenzübergreifenden Cyber-Hub einrichten.[9] Die Cyber-Hubs sollen alle Informationen über Cyberbedrohungen, Schwachstellen, gegnerische Taktiken usw. untereinander austauschen.[10]

Außerdem wird ein „Cybernotfallmechanismus" geschaffen, um die Resilienz der Union gegenüber Cyberbedrohungen zu verbessern und um auf Cybersicherheitsvorfälle im „Geiste der Solidarität" reagieren zu können.[11] Hierzu zählen (u. a.) – freiwillige – koordinierte Tests der Abwehrbereitschaft.[12] Zentraler Baustein des Systems ist die Einrichtung einer EU-Cybersicherheitsreserve.[13] Diese besteht aus zuvor ausgewählten „vertrauenswürdigen Anbietern verwalteter Sicherheitsdienste".[14] (Private) IT-Sicherheitsdienstleister können sich hierfür bewerben. Kommt es zu (schwerwiegenden) Cybersicherheitsvorfällen, können die zuständigen Behörden[15] – etwa nationale Computernotfallteams („Computer Emergency Response Teams", CERTs) – kurzfristig (innerhalb von 48 Stunden[16]) auf die entsprechenden Ressourcen zugreifen.[17] Sie erhalten dann Unterstützung bei der Reaktion auf einen solchen Cybersicherheitsvorfall und einer evtl. notwendigen anschließenden Wiederherstellung.

Unmittelbare Auswirkungen hat die Cybersolidaritätsverordnung (EU) 2025/38 zunächst für den IT-Sicherheitssektor, der von öffentlichen Aufträgen im Rahmen der Cybersicherheitsreserve profitieren kann. Die sonstigen Auswirkungen auf die nationale Wirtschaft sind indirekter Natur, da durch die Verordnung die Cybersicherheit insgesamt verbessert werden soll und im Falle von Cybersicherheitsvorfällen solidarische Hilfe über die EU erreicht werden kann.

b) Rechtsakt (EU) 2019/881 zur Cybersicherheit („Cybersecurity Act")

Der Rechtsakt (EU) 2019/881 zur Cybersicherheit[18] ist eine Verordnung der EU, welche die Ziele, Aufgaben und Organisation der Agentur der Europäischen Union für Cybersicherheit (European Union Agency for Cybersecurity) regelt, die in Anknüpfung an ihre vorherige englischsprachige Bezeichnung als European Network and Information Security Agency (Europäische Agentur für Netz- und Informationssicherheit) nach wie vor ENISA abgekürzt wird; außerdem gestaltet die Verordnung den Rahmen für die Festlegung europäischer Schemata für die Cybersicherheitszertifizierung aus.[19] Die Verordnung begründet *keine* unmittelbaren Rechte oder Pflichten für Unionsbürger oder Unternehmen. Sie ist gleichwohl ein wichtiger Baustein im unionalen IT-Sicherheitsrecht, weil sie die Arbeit der ENISA verstetigt,[20] ihre Position stärkt und hierdurch insgesamt die IT-Sicherheit in der Union erhöht.

Die ENISA ist das Kompetenzzentrum der EU für Cybersicherheit.[21] Sie unterstützt die EU sowie die Mitgliedstaaten in Fragen der Cybersicherheit.[22] Sie erstellt hierzu u. a. unabhängige Stellungnahmen und Analysen, begleitet die Unionspolitik auf dem Gebiet der Cybersicherheit[23] und unterstützt die operative Zusammenarbeit innerhalb der Union[24]. Sie ist hierzu in die Entwicklung von Cybersicherheitszertifikaten für Produkte, Dienste und Prozesse der Informations- und Kommunikationstechnologie (IKT) sowie die Normung eingebunden.[25] Als Kompetenzzentrum forscht die ENISA zu Cyberbedrohungen und Sicherheitsvorfällen[26] und leistet Öffentlichkeitsarbeit[27].

Die ENISA wird von einer ENISA-Beratungsgruppe und einer Gruppe der Interessenträger für Cybersicherheitszertifizierung unterstützt. In beiden Gruppen sind Vertreter der „einschlägigen Interessenträger" – also insbesondere der Industrie – vertreten.[28]

c) ECCC-Verordnung (EU) 2021/887 und Verordnung (EU, EURATOM) 2023/2841 für ein hohes Cybersicherheitsniveau

Auf institutioneller Ebene ist außerdem die ECCC-Verordnung (EU) 2021/887 in den Blick zu nehmen. Durch sie wird (u. a.) ein europäisches Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (European Cybersecurity Competence Centre, ECCC) sowie ein Netzwerk nationaler Koordinierungszentren eingerichtet.[29] Das Kompetenzzentrum soll eine zentrale Rolle bei der Umsetzung der Cybersicherheitskomponenten des Programms „Digitales Europa"[30] spielen.[31] Aufgabe des Zentrums ist (u. a.) die Forschungsförderung in diesem Bereich, insbesondere mit Blick auf (u. a.) die Cybersicherheit der Wirtschaft einschließlich kleiner und mittlerer Unternehmen (KMU).[32]

Zu erwähnen ist schließlich die Verordnung (EU, EURATOM) 2023/2841 für ein hohes Cybersicherheitsniveau in der Union.[33] Die Verordnung verpflichtet alle Einrichtungen der Union, eine Cybersicherheitsüberprüfung durchzuführen,[34] regelmäßig ihren Cybersicherheitsreifegrad zu bewerten[35] und Maßnahmen zum Management von Cybersicherheitsrisiken zu ergreifen (etwa ein Backup-Management oder die Verwendung von Multifaktorauthentifizierung)[36]. Außerdem wird durch die Verordnung ein Interinstitutioneller Cybersicherheitsbeirat (Interinstitutional Cybersecurity Board, IICB) eingerichtet, der u. a. die Durchführung der Verordnung überwacht.[37]

8 Art. 4 Abs. 1 und 2 der Cybersolidaritätsverordnung (EU) 2025/38.
9 Art. 5 Abs. 1 und 2 der Cybersolidaritätsverordnung (EU) 2025/38.
10 Art. 6 Abs. 1 der Cybersolidaritätsverordnung (EU) 2025/38; siehe auch Erwägungsgrund 15 der Verordnung.
11 Art. 10 der Cybersolidaritätsverordnung (EU) 2025/38.
12 Art. 12 der Cybersolidaritätsverordnung (EU) 2025/38.
13 Art. 14 der Cybersolidaritätsverordnung (EU) 2025/38. Die Kommission hat hierfür 36 Mio. Euro aus dem Programm „Digitales Europa" zur Verfügung gestellt, vgl. die DIGIBYTE-Seite „ENISA betreibt die EU-Cybersicherheitsreserve" der Kommission v. 26.8.2025, abrufbar unter https://digital-strategy.ec.europa.eu/de/news/enisa-operate-eu-cybersecurity-reserve (zuletzt abgerufen am 30.10.2025).
14 Art. 17 der Cybersolidaritätsverordnung (EU) 2025/38.
15 Art. 14 Abs. 3 lit. c der Cybersolidaritätsverordnung (EU) 2025/38.
16 Art. 16 Abs. 1 der Cybersolidaritätsverordnung (EU) 2025/38.
17 Art. 15 der Cybersolidaritätsverordnung (EU) 2025/38.
18 Siehe hierzu *Gitter*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2. A., 2024, § 15 Rn. 9, 30.
19 Art. 1 Abs. 1 des Rechtsakts (EU) 2019/881 zur Cybersicherheit.
20 Die Agentur wurde durch die Verordnung (EG) 460/2004 errichtet.
21 Art. 3 Abs. 1 des Rechtsakts (EU) 2019/881 zur Cybersicherheit.
22 Art. 4, 6 des Rechtsakts (EU) 2019/881 zur Cybersicherheit.
23 Art. 5 Abs. 1 des Rechtsakts (EU) 2019/881 zur Cybersicherheit.
24 Art. 7 des Rechtsakts (EU) 2019/881 zur Cybersicherheit.
25 Art. 8 Abs. 1 des Rechtsakts (EU) 2019/881 zur Cybersicherheit.
26 Art. 9 des Rechtsakts (EU) 2019/881 zur Cybersicherheit.
27 Art. 10 des Rechtsakts (EU) 2019/881 zur Cybersicherheit.
28 Art. 21 und 22 des Rechtsakts (EU) 2019/881 zur Cybersicherheit.
29 Art. 1 Abs. 1 der ECCC-Verordnung (EU) 2021/887.
30 Hierbei handelt es sich um ein (finanzielles) Förderprogramm der Kommission zur Beschleunigung des digitalen Wandels der europäischen Wirtschaft, Industrie und Gesellschaft.
31 Art. 1 Abs. 2 der ECCC-Verordnung (EU) 2021/887.
32 Art. 4 Abs. 1, Abs. 2 lit. a der ECCC-Verordnung (EU) 2021/887. Im Oktober 2025 waren mehr als 170 Partner an den Programmen des Kompetenzzentrums beteiligt, vgl. die Informationsseite zur „EU-Cybersicherheitspolitik" der Kommission, abrufbar unter https://digital-strategy.ec.europa.eu/de/policies/cybersecurity-policies (zuletzt abgerufen am 30.10.2025).
33 Siehe hierzu *Gräfin von Wintzingerode/Müllmann/Spiecker gen. Döhmann*, NVwZ 2021, 690.
34 Art. 6 Abs. 1 der Verordnung (EU, EURATOM) 2023/2841 für ein hohes Cybersicherheitsniveau.
35 Art. 7 Abs. 1 der Verordnung (EU, EURATOM) 2023/2841 für ein hohes Cybersicherheitsniveau.
36 Art. 8 (Abs. 2 lit. o und Abs. 3 lit. c) der Verordnung (EU, EURATOM) 2023/2841 für ein hohes Cybersicherheitsniveau.
37 Art. 10 ff. der Verordnung (EU, EURATOM) 2023/2841 für ein hohes Cybersicherheitsniveau.

2. Absicherung von Infrastruktur

Zentrale Rechtsakte der Union zur Absicherung der europäischen kritischen (digitalen) Infrastrukturen sind die NIS-2-Richtlinie (EU) 2022/2555 (sogleich, unter a)) und die CER-Richtlinie (EU) 2022/2557 (unten, unter b)). Wichtige Regelungen finden sich zudem in der DSGVO hinsichtlich personenbezogener Daten (hierzu unten, unter c)). Hinzu kommen für den Finanzsektor die Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act, DORA) (hierzu unter, unter d)) und für die Digitalwirtschaft die Gesetze über digitale Dienste (Digital Services Act, DSA) und Märkte (Digital Markets Act, DMA) (hierzu unten, unter e)).

a) NIS-2-Richtlinie (EU) 2022/2555

Die NIS-2-Richtlinie (EU) 2022/2555[38] ist *die* zentrale Vorschrift der EU zur Regelung der Cybersicherheit in der Union. Der Anwendungsbereich wurde gegenüber der NIS(-1)-Richtlinie (EU) 2016/1148 deutlich erweitert und erfasst neben den Betreibern kritischer Infrastrukturen zahlreiche mittelständische Unternehmen. Die NIS-2-Richtlinie (EU) 2022/2555 hätte bis zum 17. Oktober 2024 in nationales Recht umgesetzt werden müssen.[39] Der deutsche Gesetzgeber hat dies nicht geschafft. Seit dem 15. August 2025 liegt aber der Entwurf der Bundesregierung für ein „Gesetz[…] zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung" vor.[40] Da die Kernvorschriften die NIS-2-Richtlinie (EU) 2022/2555 umsetzen müssen, ist im weiteren Gesetzgebungsverfahren nicht mit – *hier* relevanten – grundlegenden Änderungen zu rechnen, weshalb sich die folgenden Ausführungen am Gesetzentwurf der Bundesregierung orientieren.

aa) BSIG-RegE

Das deutsche IT-Sicherheitsrecht ist, soweit es die Absicherung der (Unternehmens- oder Behörden-) IT gegen Sicherheitsvorfälle betrifft, im BSIG geregelt. Das hat vor allem historische Gründe. Der Aufgabenbereich des Bundesamts für Sicherheit in der Informationstechnik (BSI) wurde im Verlauf der Jahre immer mehr ausgeweitet und umfasst nun die Aufsicht über die IT-Sicherheit (des Bundes sowie) großer Teile der Wirtschaft.

Der BSIG-RegE erweitert den Adressatenkreis erheblich und ändert die Terminologie. Erfasst werden künftig besonders wichtige Einrichtungen und wichtige Einrichtungen.

Besonders wichtige Einrichtungen sind (u. a.) Betreiber kritischer Anlagen, qualifizierte Vertrauensdiensteanbieter, große Telekommunikationsanbieter und (bestimmte) sehr große Unternehmen.[41] Kritische Infrastrukturen umfassen – weitgehend wie bisher – die Sektoren Energie, Transport und Verkehr, Finanzwesen, Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitssuchende, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Siedlungsabfallentsorgung. Neu hinzugekommen ist der Weltraumsektor. Erfasst werden aber nur Unternehmen, deren Beeinträchtigung zu erheblichen Versorgungsengpässen oder einer Gefährdung der öffentlichen Ordnung führen würde und die bestimmte Schwellenwerte gemäß der BSI-KritisVO erfüllen.[42] Besonders wichtige Einrichtungen sind außerdem (u. a.) Unternehmen, die mindestens 250 Mitarbeiter beschäftigen oder einen Jahresumsatz von 50 Millionen Euro aufweisen und in der Anlage 1 zum BSIG-RegE aufgezählt sind. Das sind z. B. Luftfahrtunternehmen oder Betreiber von Wasserversorgungsanlagen.[43] Wichtige Einrichtungen sind sonstige Vertrauensdiensteanbieter, kleine und mittlere Telekommunikationsunternehmen sowie (u. a.) Unternehmen nach der Anlage 2, die mindestens 50 Mitarbeiter beschäftigen oder einen Jahresumsatz (und eine Jahresbilanzsumme)[44] von über 10 Millionen Euro aufweisen.[45] Die erfassten Unternehmen reichen dabei weit in den Mittelstand hinein, etwa Kurierdienste, Lebensmittelgroßhändler oder Maschinenbauer.[46]

Die betroffenen Unternehmen müssen Risikomanagementmaßnahmen ergreifen, um IT-Störungen zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten.[47] Hierzu zählen beispielsweise ein Backup-Management, Sensibilisierungsmaßnahmen,[48] kryptographische Verfahren und Multifaktorauthentifizierung.[49] Dabei ist eine Risiko-Nutzen-Abwägung vorzunehmen.[50] Bei der Beurteilung kann auf branchenspezifische Sicherheitsstandards (B3S) zurückgegriffen werden.[51]

Besonders wichtige Einrichtungen dürfen bestimmte IKT-Produkte und -Dienstleistungen nur einsetzen, wenn diese über eine Cybersicherheitszertifizierung verfügen.[52]

Betreiber kritischer Anlagen müssen grundsätzlich auch aufwendigere Maßnahmen ergreifen.[53] Ausdrücklich geregelt ist, dass sie etwa ein Angriffserkennungssystem („Intrusion Detection System", IDS) betreiben müssen, das geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfasst und auswertet.[54] Sie müssen zudem den Einsatz kritischer Komponenten dem Bundesinnenministerium anzeigen. Das Ministerium kann dann den Einsatz aus Gründen der öffentlichen Sicherheit und Ordnung untersagen – etwa wenn der Hersteller von einem Drittstaat kontrolliert wird.[55]

Verantwortlich für die Maßnahmen ist die Geschäftsleitung. Diese muss regelmäßig an entsprechenden Schulungen teilnehmen und haftet ggf. persönlich.[56] Die ergriffenen Maßnahmen sind regelmäßig nachzuweisen.[57]

---

38 Siehe hierzu *Grosmann/Gerecke/Aschenbrenner*, CR 2024, 665; *Leßner*, MMR 2024, 226; *Scheibenpflug/Monschke/Hildebrandt*, CR 2024, 712; *Schmidt*, K&R 2023, 705; *Werry/Éles*, MMR 2024, 829.

39 Art. 41 Abs. 1 der NIS-2-Richtlinie (EU) 2022/2555. Vgl. zum „aktuellen Stand der NIS-2-Umsetzung in der EU" *Karniyevich/Emmerich*, K&R 2025, 366; 446.

40 Gesetzentwurf der Bundesregierung, BR-Drs. 369/25; BT-Drs. 21/1501. Der Entwurf entspricht im Wesentlichen dem Entwurf aus der 20. Legislaturperiode (allerdings wurde der Begriff der „Zeitenwende", der im alten Entwurf immerhin acht Mal Erwähnung fand, nun komplett gestrichen): Gesetzentwurf der Bundesregierung, BR-Drs. 380/24; BT-Drs. 20/13184. Siehe hierzu *Kipker/Dittrich*, MMR 2023, 481; *Leßner*, MMR 2024, 226; *Voigt/Schmalenberger*, CR 2023, 717; *Werry/Éles*, MMR 2024, 829. Zum Zeitpunkt des Manuskriptschlusses waren eine erste Beratung im Bundestag (BT-Plenarprotokoll 21/21, 2058 C) sowie ein erster Durchgang im Bundesrat (BR-Plenarprotokoll 1057, TOP 32) erfolgt.

41 § 28 BSIG-RegE.

42 § 1 Nr. 22, 24 i. V. m. § 56 Abs. 4 BSIG-RegE; zur Änderung der BSI-KritisVO: Art. 8 des Gesetzentwurfs der Bundesregierung, BR-Drs. 369/25, 75. Dabei wird ein Gleichklang mit dem KRITIS-Dachgesetz (hierzu unten, unter b)) angestrebt, vgl. die Begründung zum Gesetzentwurf der Bundesregierung, BR-Drs. 369/25, 101, 187.

43 § 28 Abs. 1 i. V. m. Anlage 1 Nr. 2.1.1 und 5.1.1 BSIG-RegE.

44 Siehe auch § 28 Abs. 2 Nr. 2 BSIG-RegE für kleine und mittlere Telekommunikationsunternehmen: „*weniger* als 50 Mitarbeiter … *und* … einen Jahresumsatz *oder* eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder *weniger*" (Hervorhebung nur hier).

45 § 28 Abs. 2 BSIG-RegE.

46 Anlage 2 Nr. 1.1.1, 4.1.1 und 5.4.1 BSIG-RegE.

47 § 30 BSIG-RegE.

48 Der neue Entwurf verzichtet insoweit auf den wenig klaren Begriff „Cyberhygiene". In § 5c Abs. 4 Nr. 7 EnWG-RegE wird der Begriff aber weiterhin verwendet. Kritisch zu solchen Wortneuschöpfungen *Appelt/Enzmann/Selzer*, DuD 2025, 379, 381.

49 § 30 Abs. 2 Nr. 3, 7, 8 und 10 BSIG-RegE.

50 § 30 Abs. 1 BSIG-RegE.

51 § 30 Abs. 8 BSIG-RegE.

52 § 30 Abs. 6 BSIG-RegE.

53 § 31 BSIG-RegE.

54 § 31 Abs. 2 BSIG-RegE.

55 § 41 BSIG-RegE.

56 § 38 BSIG-RegE.

57 § 39 BSIG-RegE.

Kommt es zu erheblichen Sicherheitsvorfällen, sind diese spätestens 24 Stunden nach Bekanntwerden dem BSI zu melden. Innerhalb von 72 Stunden ist eine Erstbewertung vorzulegen und innerhalb eines Monats ein Abschlussbericht.[58]

Verstöße sind bußgeldbewehrt, wobei der Bußgeldrahmen deutlich ausgeweitet wird: Zukünftig sind Bußgelder bis zu zehn Millionen Euro oder 2 % des Jahresumsatzes möglich.[59]

Die Regelungstechnik mit Anhängen und ergänzenden (nationalen) Verordnungen[60] wird zusätzlich durch eine in der NIS-2-Richtlinie (EU) 2022/2555 enthaltene Ermächtigung der Kommission zum Erlass von Durchführungsrechtsakten verkompliziert.[61] Die Durchführungsrechtsakte treten dann neben die nationalen Rechtsvorschriften und genießen diesen gegenüber grundsätzlich Anwendungsvorrang.

bb) NIS-2-Durchführungsverordnung (EU) 2024/2690

Eine erste Durchführungsverordnung ist inzwischen von der Kommission angenommen worden und am 7. November 2024 in Kraft getreten.

Der Rechtsakt betrifft verschiedene Anbieter von Internetdiensten (Domänennamensystem [„Domain Name System", DNS], Namensregister für Domänennamen der obersten Stufe [„Top Level Domains", TLD], Cloud-Computing usw.). Anders als die NIS-2-Richtlinie (EU) 2022/2555 gilt die NIS-2-Durchführungsverordnung (EU) 2024/2690 unmittelbar. Sie bedarf also keines nationalen Umsetzungsrechtsakts. Die Verordnung regelt im Detail, wann meldepflichtige Sicherheitsvorfälle in den betroffenen Branchen vorliegen (z. B. wenn ein Cloud-Computing-Dienst mehr als 30 Minuten nicht verfügbar ist).[62]

Die NIS-2-Durchführungsverordnung (EU) 2024/2690 enthält außerdem einen langen Anhang mit technischen und methodischen Anforderungen, die im Bereich der Cybersicherheit von den entsprechenden Unternehmen umgesetzt werden müssen.

cc) TKG und EnWG

Der BSIG-RegE erfasst zwar zunächst Unternehmen der Telekommunikations-, Energie- und Finanzbranche. Die Unternehmen werden dann aber weitgehend von der Geltung des BSIG-RegE wieder ausgenommen.[63] Grund hierfür ist, dass die entsprechenden Fachgesetze – insbesondere das TKG, das EnWG[64] sowie der DORA[65] – bereits über vergleichbare Regelungen verfügen. Für Außenstehende erschwert dies den Zugang zum IT-Sicherheitsrecht erheblich. Auch ist fraglich, ob es sinnvoll ist, wenn etwa § 28 Abs. 1 BSIG-RegE Energieversorger zunächst *erfasst*, § 28 Abs. 5 BSIG-RegE die Unternehmen dann teilweise aus dem Anwendungsbereich des BSIG-E *ausschließt* und § 5d Abs. 3 EnWG-RegE den BSIG-RegE für teilweise „entsprechend" *anwendbar* erklärt.

Eine Besonderheit im Telekommunikations- und Energierecht sind verbindliche IT-Sicherheitskataloge der Bundesnetzagentur.[66] Diese Kataloge sind im Gegensatz zu den branchenspezifischen Sicherheitsstandards des BSI verbindlich und müssen umgesetzt werden.

b) Richtlinie (EU) 2022/2557 über die Resilienz kritischer Infrastrukturen (CER-Richtlinie) und KRITIS-Dachgesetz-RegE

Die Richtlinie (EU) 2022/2557 über die Resilienz kritischer Infrastrukturen[67] – verbreiteter dürfte die englische Abkürzung CER für „Critical Entities Resilience" sein – zielt wie die NIS-2-Richtlinie (EU) 2022/2555 auf die Resilienz der EU gegenüber Sicherheitsvorfällen. Der Anwendungsbereich ist gegenüber der NIS-2-Richtlinie (EU) 2022/2555 einerseits deutlich enger, da nur kritische Infrastrukturen erfasst werden. Andererseits erfasst die CER-Richtlinie (EU) 2022/2557 nicht nur Cyberrisiken, sondern legt einen Allgefahrenansatz zugrunde.

Die Richtlinie hätte bis zum 17. Oktober 2024 in nationales Recht umgesetzt werden müssen.[68] Das ist nicht erfolgt. Die Bundesregierung hat allerdings am 10. Oktober 2025 den Entwurf für ein Gesetz zur Stärkung der Resilienz kritischer Anlagen vorgelegt.[69] Kern des Entwurfs ist ein KRITIS-Dachgesetz.

Adressaten des Gesetzes sind die Betreiber kritischer Anlagen[70] – die (KRITIS-) Sektoren sind dabei identisch mit dem (§ 2 Nr. 24) BSIG-RegE. Eingegrenzt wird der Anwendungsbereich durch eine noch zu erlassende Verordnung, welche die einzelnen kritischen Dienstleistungen ausdifferenziert, Kategorien von Anlagen benennt und Schwellenwerte festlegt.[71]

Die betroffenen Betreiber müssen ihre kritischen Anlagen beim Bundesamt für Bevölkerungsschutz registrieren – und zwar erstmalig bis zum 17. Juli 2026.[72] Sie müssen mindestens alle vier Jahre eine umfassende Risikoanalyse durchführen. Hiervon umfasst sind u. a. – und rein exemplarisch – Extremereignisse durch Naturgefahren, gesundheitliche Notlagen, (hybride) feindliche Bedrohungen, terroristische Angriffe, Abhängigkeiten von anderen Sektoren oder Drittstaaten.[73] Es sind sodann Resilienzmaßnahmen zur Abschirmung der Risiken zu treffen. Hierzu zählen – erneut rein exemplarisch – bauliche Schutzmaßnahmen, Schulungen der Mitarbeitenden und Übungen.[74] Sicherheitsvorfälle sind innerhalb von 24 Stunden zu melden.[75] Die Geschäftsleitungen sind – persönlich haftend – für die Umsetzung verantwortlich.[76]

Kritische Einrichtungen, die in mindestens sechs Mitgliedstaaten der EU tätig sind, können als „kritische Einrichtung von besonderer Bedeutung für Europa" eingestuft werden. Sie können dann durch eine Beratungsmission der Kommission spezielle Unterstützungsleistungen erhalten.[77]

Auch im Bereich der CER-Richtlinie (EU) 2022/2557 und des KRITIS-DachG sind weitere Ausgestaltungen durch (nationale)

58 § 32 BSIG-RegE.
59 § 65 BSIG-RegE.
60 Verordnungsermächtigungen finden sich in § 30 Abs. 5 sowie § 56 BSIG-RegE.
61 Etwa Art. 23 Abs. 11 der NIS-2-Richtlinie (EU) 2022/2555. Siehe auch § 30 Abs. 3 ff. BSIG-RegE.
62 Art. 2 ff. (Art. 7 lit. a) der NIS-2-Durchführungsverordnung (EU) 2024/2690.
63 § 28 Abs. 5 und 6 BSIG-RegE.
64 Siehe zum EnWG-RegE *Appelt/Enzmann/Selzer*, DuD 2025, 379.
65 Vgl. hierzu unten, unter d).
66 § 167 TKG und § 11 Abs. 1a und 1b EnWG. Der „aktuelle" IT-Sicherheitskatalog für den Betrieb von Energieversorgungsnetzen stammt aus dem Jahr 2015, der für den Betrieb von Energieanlagen immerhin aus 2018. Die Bundesnetzagentur hat am 7.5.2025 Eckpunkte zur Aktualisierung der IT-Sicherheitskataloge für die Betreiber von Strom- und Gasnetzen und von Energieanlagen veröffentlicht, vgl. Bundesnetzagentur, Festlegungsverfahren „Erstellung eines IT-Sicherheitskatalogs nach § 11 Abs. 1a und 1b EnWG" – Az. 4.12.10.01. Am 3.11.2025 hat die Bundesnetzagentur außerdem die Konsultation zur Überarbeitung des Katalogs von Sicherheitsanforderungen nach § 167 TKG begonnen.
67 Siehe hierzu: *Hornung/Muttach/Schaller*, CR 2024, 229; *Scheibenpflug/Monschke/Hildebrandt*, CR 2024, 712.
68 Art. 26 der CER-Richtlinie (EU) 2022/2557.
69 Gesetzentwurf der Bundesregierung, BR-Drs. 558/25. Der Entwurf basiert auf dem Entwurf aus der 20. Legislaturperiode: Gesetzentwurf der Bundesregierung, BR-Drs. 550/24; BT-Drs. 20/13961. Siehe hierzu *Voigt/Schmalenberger*, CR 2023, 717.
70 § 4 Abs. 1 KRITIS-DachG-RegE.
71 § 4 Abs. 3, § 5 KRITIS-DachG-RegE. § 5 Abs. 2 S. 2 KRITIS-DachG-RegE sieht dabei einen Regelwert von grundsätzlich 500 000 von einer Anlage versorgten Einwohnern vor.
72 § 8 KRITIS-DachG-RegE.
73 § 12 KRITIS-DachG-RegE.
74 § 13 KRITIS-DachG-RegE.
75 § 18 Abs. 1 KRITIS-DachG-RegE.
76 § 20 KRITIS-DachG-RegE.
77 § 10 KRITIS-DachG-RegE. Siehe auch die Begründung zum Gesetzentwurf der Bundesregierung, BR-Drs. 558/25, 29, 57.

Verordnungen[78] und Durchführungsrechtsakte[79] der Kommission vorgesehen.

c) Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO)

Die DSGVO[80] regelt den grundrechtlichen Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und den freien Verkehr mit solchen Daten.[81] Der Fokus liegt hierbei auf den betroffenen Personen, um derentwillen die Daten geschützt werden. Die DSGVO enthält aber auch zahlreiche Regelungen zu technischen und organisatorischen Maßnahmen (TOM) beim Umgang mit personenbezogenen Daten, die einen unmittelbaren Bezug zur IT-Sicherheit haben.

Die DSGVO ist insoweit von immenser praktischer Bedeutung, weil sie die Verarbeitung personenbezogener Daten fast ausnahmslos erfasst und somit praktisch allgemeine Geltung hat.[82] Adressaten sind nicht nur europäische Unternehmen, sondern – stark verkürzt – weltweit alle Akteure, die irgendwie (virtuell) auf den europäischen Märkten präsent sind, etwa indem sie Personen in der Union (nicht notwendigerweise Unionsbürger) (virtuelle – auch kostenlose –) Dienstleistungen anbieten.[83]

Die DSGVO regelt verschiedene „Grundsätze für die Verarbeitung personenbezogener Daten".[84] Hierzu zählen u. a. die Grundsätze der „Datenminimierung" und „Speicherbegrenzung". Personenbezogene Daten müssen auf das für die Verarbeitung notwendige Maß beschränkt sein und dürfen nur so lange gespeichert werden, wie sie benötigt werden.[85] Dieser Grundsatz ist auch mit Blick auf die IT-Sicherheit immens relevant – so trivial es ist: Daten, die erst gar nicht erhoben wurden oder nicht mehr vorhanden sind, können auch nicht missbraucht werden.

In Art. 32 enthält die DSGVO eine zentrale Vorschrift für die „Sicherheit der Verarbeitung".[86] Die DSGVO wählt dabei einen risikobasierten Ansatz. Sie schreibt also nicht konkrete Maßnahmen vor, sondern überlässt die Umsetzung den Verantwortlichen. Dabei ist ein Ausgleich zwischen der Eintrittswahrscheinlichkeit und der Schwere von Risiken auf der einen Seite und dem Aufwand – insbesondere den Implementierungskosten – für Schutzmaßnahmen andererseits zu schaffen. Hierbei ist der Stand der Technik zu berücksichtigen. Die DSGVO benennt sodann vier technische und organisatorische Maßnahmen, die dabei zu berücksichtigen sind:

1. die Pseudonymisierung und Verschlüsselung von Daten,
2. Resilienzmaßnahmen, um u. a. die Integrität der Systeme sicherzustellen,
3. ein betriebliches Kontinuitätsmanagement („Business-Continuity-Management") sowie
4. (Pen-) Tests der ergriffenen Maßnahmen.

Die entsprechenden Pflichten haben inzwischen auch eine praktische Bedeutung erlangt: Das OLG Schleswig hat hieraus etwa eine Verpflichtung abgeleitet, Rechnungen per E-Mail nur Ende-zu-Ende-verschlüsselt zu verschicken, und im konkreten Fall einen Schadensersatzanspruch zugebilligt.[87]

Kommt es zu Verletzungen des Schutzes personenbezogener Daten – etwa durch Hackerangriffe –, müssen die zuständigen Aufsichtsbehörden unverzüglich – möglichst binnen 72 Stunden – informiert werden.[88] Ggf. sind außerdem die betroffenen Personen zu informieren.[89]

Verstöße gegen die DSGVO sind bußgeldbewehrt. Der Bußgeldrahmen für Verstöße gegen die Pflichten aus Art. 32 DSGVO reicht bis zu zehn Millionen Euro bzw. 2 % des gesamten weltweit erzielten Jahresumsatzes.[90] Die DSGVO kennt im Übrigen Bußgelder bis zu 20 Millionen Euro bzw. 4 % des gesamten weltweit erzielten Jahresumsatzes.[91]

d) Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act, DORA)

Der DORA[92] vereinheitlicht die Vorschriften über die digitale operationale Resilienz im Finanzsektor. Hierunter versteht der DORA „die Fähigkeit eines Finanzunternehmens, seine operative Integrität und Betriebszuverlässigkeit aufzubauen, zu gewährleisten und zu überprüfen, indem es entweder direkt oder indirekt durch Nutzung der von IKT[93]-Drittdienstleistern bereitgestellten Dienste das gesamte Spektrum an IKT-bezogenen Fähigkeiten sicherstellt, die erforderlich sind, um die Sicherheit der Netzwerk- und Informationssysteme zu gewährleisten, die von einem Finanzunternehmen genutzt werden und die kontinuierliche Erbringung von Finanzdienstleistungen und deren Qualität, einschließlich bei Störungen, unterstützen".[94] Die erfassten Unternehmen sind in Art. 2 der Verordnung aufgezählt und umfassen u. a. Kreditinstitute, Wertpapierfirmen, Zentralverwahrer sowie bestimmte Kryptodienstleister. Der DORA gilt seit dem 17. Januar 2025.

Die Verordnung enthält mitunter sehr detaillierte Regelungen zu allen Aspekten der IT-Sicherheit. Dies beginnt bei Fragen von „Governance und Organisation"[95] und endet mit Vorgaben für „wesentliche Vertragsbedingungen" gegenüber IKT-Dienstleistern.[96] Die entsprechenden Regelungen können hier nur exemplarisch vorgestellt werden. Nach dem DORA sind grundsätzlich die Leitungsorgane umfassend verantwortlich für die IT-Sicherheit. Sie müssen über entsprechende Kenntnisse und Fähigkeiten verfügen und diese durch regelmäßige spezielle Schulungen auf dem neusten Stand halten.[97] Die betroffenen Unternehmen müssen über einen IKT-Risikomanagementrahmen verfügen und diesen regelmäßig – mindestens jährlich – überprüfen.[98] Hierzu zählt etwa die Fähigkeit, „anomale Aktivitäten" zu erkennen,[99] Backups physisch und logisch getrennt zu erstellen[100] und über redundante IKT-Kapazitäten (ggf. sogar an einem sekundären Standort) zu verfügen[101]. Die

78 § 3 Abs. 3, § 4 Abs. 3, § 5 Abs. 1, § 11 Abs. 8, § 12 Abs. 3, § 14 Abs. 1, 3, 4, § 17 Abs. 3 KRITIS-DachG-RegE.
79 Art. 13 Abs. 6, Art. 18 Abs. 6, Art. 19 Abs. 6 der CER-Richtlinie (EU) 2022/2557.
80 Siehe hierzu *Deutsch/Eggendorfer*, K&R 2018, 753; *Grosmann/Michel*, ZD 2025, 250; *Krügel*, MMR 2017, 795; *Sowa*, DuD 2024, 651; *Thode*, CR 2017, 714.
81 Art. 1 DSGVO.
82 Art. 2 DSGVO.
83 Art. 3 DSGVO.
84 Art. 5 DSGVO.
85 Art. 5 Abs. 1 lit. c und e DSGVO.
86 Zum Verhältnis zu Art. 21 der NIS-2-Richtlinie (EU) 2022/2555 *Grosmann/Michel*, ZD 2025, 250, 252.
87 OLG Schleswig, Urt. v. 18.12.2024 – Az. 12 U 9/24. Vgl. zu Verschlüsselungspflichten und -obliegenheiten auch *Koch*, DuD 2014, 691. An den tatsächlichen technischen Möglichkeiten hat sich in der Zwischenzeit nichts grundlegend geändert. Eine flächendeckende Infrastruktur zum Versenden von Ende-zu-Ende-verschlüsselten E-Mails ist nach wie vor nicht vorhanden. Mit S/MIME und GPG stehen zwar zwei etablierte Standards zur Verfügung. Diese werden aber in der Praxis kaum genutzt.
88 Art. 33 Abs. 1 DSGVO.
89 Art. 34 Abs. 2 DSGVO.
90 Art. 83 Abs. 4 lit. a DSGVO.
91 Art. 83 Abs. 5 DSGVO.
92 Siehe hierzu *Bernau/Lutterbach*, BKR 2023, 506; *Dittrich/Heinelt*, RDi 2023, 164; *Voigt/Ritter-Döring*, CR 2023, 82.
93 Die Legaldefinition der Abkürzung findet sich nicht etwa in Art. 3 DORA zu den Begriffsbestimmungen, sondern in Art. 1 Abs. 1 lit. a i) DORA.
94 Art. 3 Nr. 1 DORA.
95 Art. 5 DORA.
96 Art. 30 DORA.
97 Art. 5, insbesondere Abs. 4 DORA.
98 Art. 6, insbesondere Abs. 5 DORA.
99 Art. 10 Abs. 1 DORA.
100 Art. 12 Abs. 3 DORA.
101 Art. 12 Abs. 4 und 5 DORA.

digitale Resilienz muss mindestens einmal im Jahr durch angemessene Tests überprüft werden.[102] Mindestens alle drei Jahre sind bedrohungsorientierte Penetrationstests („Threat-Led Penetration Testing", TLPT) durchzuführen, bei denen reale Angriffe durch sog. Red-Teams simuliert werden.[103] Da IKT-Dienstleistungen häufig ausgelagert werden, müssen die hiermit verbundenen Risiken besonders in den Blick genommen werden.[104] Grundsätzlich bleiben die Unternehmen für die Einhaltung der Verpflichtungen nach der Verordnung verantwortlich.[105] Es können also keine Verantwortungen outgesourct werden. Werden kritische oder wichtige Funktionen an IKT-Dienstleister ausgelagert, müssen die Unternehmen über eine Ausstiegsstrategie verfügen.[106] Die Verträge mit IKT-Dienstleistern müssen so ausgestaltet sein, dass den Unternehmen eine fortlaufende Überwachung – einschließlich eines uneingeschränkten Zugangs – möglich ist.[107]

Schwerwiegende IKT-bezogene Vorfälle müssen der Aufsichtsbehörde – und ggf. den betroffenen Kunden – gemeldet werden.[108] Der DORA regelt hierfür keine Fristen, sondern überlässt diese den europäischen Aufsichtsbehörden.[109] Der finale Entwurf des technischen Standards sieht eine Erstmeldung binnen vier (sic!) Stunden, eine Zwischenmeldung innerhalb von 72 Stunden sowie einen Abschlussbericht nach einem Monat vor.[110]

Die Überwachungsbehörde erhält weitreichende Auskunfts- und Untersuchungsbefugnisse, einschließlich des Rechts, Inspektionen durchzuführen.[111] Die Verordnung legt selbst keinen Bußgeldrahmen fest. Vielmehr überlässt sie es den Mitgliedstaaten, Bußgelder – und Strafvorschriften – vorzusehen.[112] Das KWG sieht in § 56 Abs. 5e i. V. m. Abs. 6a Bußgelder bis zu 10 % des Jahresgesamtumsatzes vor. Eine Besonderheit ist, dass verwaltungsrechtliche Sanktionen unverzüglich auf der amtlichen WWW-Seite der Aufsichtsbehörde veröffentlicht werden müssen.[113]

e) Verordnung (EU) 2022/2065 (Gesetz über digitale Dienste [Digital Services Act, DSA]), Verordnung (EU) 2022/1925 (Gesetz über digitale Märkte [Digital Markets Act, DMA])

Mit den Gesetzen über digitale Dienste[114] und Märkte[115] hat die Union zwei Verordnungen für die Digital- bzw. Internetwirtschaft erlassen. Das Gesetz über digitale Dienste richtet sich an die Anbieter von „Vermittlungsdiensten" – das sind (soweit hier relevant) u. a. Hosting-Dienste.[116] Ein Teil der Vorschriften gilt aber nur für „sehr große Online-Plattformen" und „sehr große Online-Suchmaschinen" mit mindestens 45 Millionen aktiven Nutzern in der Union.[117] Das sind etwa Unternehmen wie Aylo Freesites (Pornhub), Amazon, Booking.com, Google, TikTok, Twitter (X) oder Zalando.[118] Das Gesetz über digitale Märkte erfasst die „Torwächter" auf dem digitalen Sektor.[119] Letzteres sind – sehr stark verkürzt – die sehr großen Digitalunternehmen, die erheblichen Einfluss auf den Binnenmarkt haben,[120] wie etwa Alphabet (Google), Amazon und Meta (Facebook, Instagram und WhatsApp).[121] Beide Verordnungen regeln am Rande auch Fragen der IT-Sicherheit.

Nach dem Gesetz über digitale Dienste müssen sehr große Online-Plattformen und -Suchmaschinen eine Risikobewertung hinsichtlich aller systemischen Risiken vornehmen, etwa im Hinblick auf „gesellschaftliche Debatten und auf Wahlprozesse". Dabei sind auch vorsätzliche Manipulationen in den Blick zu nehmen.[122] Sie müssen sodann Maßnahmen zur Risikominimierung treffen.[123] Im Krisenfall – etwa in Folge einer Pandemie, von Terrorangriffen oder bewaffneter Konflikte[124] – kann die Kommission durch einen (nach Art. 288 UAbs. 3 AEUV verbindlichen) Beschluss die Unternehmen verpflichten, Krisenreaktionsmaßnahmen zu ergreifen.[125] Sie müssen zudem eine Compliance-Abteilung einrichten.[126] Verstöße gegen das Gesetz über digitale Dienste können mit Bußgeldern bis zu 6 % des weltweiten Jahresumsatzes sanktioniert werden.[127]

Torwächter, die „nummernunabhängige interpersonelle Kommunikationsdienste" anbieten (etwa WhatsApp), müssen eine Interoperabilität mit anderen Diensten einschließlich einer Ende-zu-Ende-Verschlüsselung sicherstellen.[128]

IV. Produktrecht

Die IT-Sicherheit von Produkten wird in der EU auf (wenigstens) drei Ebenen geregelt: Die Ebene der Produktsicherheit normiert Sicherheitsanforderungen an Produkte, die ggf. öffentlich-rechtlich durch die Aufsichtsbehörden durchgesetzt werden (hierzu sogleich, unter 1.). Sind Produkte fehlerhaft, stehen dem Käufer regelmäßig (zivilrechtliche) Gewährleistungsansprüche gegenüber dem Verkäufer zu (hierzu unten, unter 2.). Führt ein fehlerhaftes Produkt zu einem Schaden, stellen sich schließlich (ebenfalls zivilrechtliche) Fragen der Produkthaftung (hierzu unten, unter 3.).

1. Produktsicherheit

a) Cyberresilienzverordnung (EU) 2024/2847 (Cyber Resilience Act, CRA)

Die Cyberresilienzverordnung (EU) 2024/2847[129] regelt die Cybersicherheit bei der Bereitstellung von „Produkten mit digitalen Elementen" auf dem Markt. Erfasst werden Kombinationen aus Hard- und Software wie beispielsweise Smartphones, aber auch reine Softwareprodukte wie Betriebssysteme.[130] Solche Produkte müssen „grundlegende

102 Art. 24 Abs. 6 DORA.
103 Art. 26 Abs. 1 i. V. m. Art. 3 Nr. 17 DORA.
104 Art. 28 ff. DORA.
105 Art. 28 Abs. 1 lit. a DORA.
106 Art. 28 Abs. 8 DORA.
107 Art. 30 Abs. 3 lit. e DORA.
108 Art. 19 Abs. 1 und 3 DORA.
109 Art. 20 lit. a DORA.
110 Art. 6 des Joint Technical Standards on major incident reporting, abrufbar unter https://www.eba.europa.eu/sites/default/files/2024-07/6d341d14-0c54-44 ff-a849-21561baee157/JC%202024-33%20-%20Final%20report%20on%20the%20draft%20RTS%20and%20ITS%20on%20incident%20reporting.pdf (zuletzt abgerufen am 30.10.2025).
111 Art. 35 ff. DORA.
112 Art. 50 Abs. 3 und Art. 52 DORA.
113 Art. 54 Abs. 1 DORA.
114 Siehe hierzu *Brorsen/Falk*, MMR 2024, 32; *Dregelies*, MMR 2022, 1033; *Raue/Heesen*, NJW 2022, 3537; *Schmid/Grewe*, MMR 2021, 279; *Spindler*, MMR 2023, 73.
115 Siehe hierzu *Gielen/Uphues*, EuZW 2021, 627; *Herbers*, RDi 2022, 252; *Podszun/Bongartz/Kirk*, NJW 2022, 3249.
116 Art. 2 Abs. 1 i. V. m. Art. 3 lit. g des Gesetzes über digitale Dienste.
117 Art. 33 des Gesetzes über digitale Dienste.
118 Vgl. die Informationsseite „Supervision of the designated very large online platforms and search engines under DAS" der Kommission, abrufbar unter https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (zuletzt abgerufen am 30.10.2025).
119 Art. 1 des Gesetzes über digitale Märkte.
120 Art. 3 des Gesetzes über digitale Märkte.
121 Vgl. Kommission, Pressemitteilung IP/23/4328 v. 6.9.2023.
122 Art. 34 Abs. 1 lit. c und Abs. 2 UAbs. 2 des Gesetzes über digitale Dienste.
123 Art. 35 des Gesetzes über digitale Dienste.
124 Erwägungsgrund 91 des Gesetzes über digitale Dienste.
125 Art. 36 des Gesetzes über digitale Dienste.
126 Art. 41 des Gesetzes über digitale Dienste.
127 Art. 52 Abs. 3 des Gesetzes über digitale Dienste i. V. m. § 33 DDG.
128 Art. 7 Abs. 3 des Gesetzes über digitale Märkte.
129 Siehe hierzu *Biendl/Füllsack*, CR 2024, 376; *Bronner/Heckmann/Ziegler*, DuD 2025, 572; *Do Chi*, K&R 2025, 440; *Murati*, DuD 2025, 89; *Piltz/Weiß/Zwerschke*, CR 2023, 289; *Scheibenpflug/Monschke/Hildebrandt*, CR 2024, 712; *Schöttle*, MMR 2024, 741; 834; *Siglmüller*, ZfPC 2023, 221; *Teichmann*, DuD 2025, 505; K&R 2025, 542; *Voigt/Falk*, MMR 2023, 88; *Wiebe/Daelen/Kerger*, K&R 2025, 79.
130 Vgl. die Legaldefinition in Art. 3 Nr. 1 der Cyberresilienzverordnung (EU) 2024/2847. Siehe außerdem zum Anwendungsbereich *Teichmann*, DuD 2025, 505.

Cybersicherheitsanforderungen" erfüllen.[131] Adressaten sind – soweit hier von Interesse – die „Wirtschaftsakteure". Das sind insbesondere Hersteller, Einführer und Händler.[132]

Die Cyberresilienzverordnung (EU) 2024/2847 orientiert sich am neuen Konzept – „New Approach" – des Produktsicherheitsrechts der EU, wie es sich aus dem „Blue Guide" der Kommission[133] ergibt.[134] Produkte mit digitalen Elementen müssen den grundlegenden Cybersicherheitsanforderungen der Verordnung genügen.[135] Hierzu zählen etwa Kontrollmechanismen zum Schutz vor unbefugtem Zugriff und das aus dem Datenschutzrecht[136] bekannte Gebot der Datenminimierung.[137] Die Produkte müssen sich außerdem automatisch aktualisieren lassen, wobei Sicherheitsaktualisierungen – für mindestens fünf Jahre[138] – kostenlos zur Verfügung gestellt werden müssen.[139] Verantwortlich hierfür sind zunächst die Hersteller.[140] Sie können hierbei – wie im sonstigen EU-Produktsicherheitsrecht – auf harmonisierte Normen zurückgreifen, wodurch vermutet wird, dass das Produkt den grundlegenden Cybersicherheitsanforderungen genügt.[141] Das Konformitätsbewertungsverfahren kann grundsätzlich intern durch den Hersteller durchgeführt werden.[142] Für „wichtige Produkte mit digitalen Elementen" – etwa Passwortmanager oder Betriebssysteme[143] – sowie „kritische Produkte mit digitalen Elementen" – etwa Hardwaregeräte mit Sicherheitsboxen[144] – gelten strengere Voraussetzungen.[145]

Die Hersteller treffen außerdem verschiedene Meldepflichten. Aktiv ausgenutzte Schwachstellen müssen unverzüglich – jedenfalls innerhalb von 24 Stunden[146] – über eine einheitliche Meldeplattform gemeldet werden; ggf. müssen weitere – detailliertere – Meldungen nach spätestens 72 Stunden und nach 14 Tagen erfolgen.[147]

Die sonstigen Wirtschaftsakteure treffen die im EU-Produktsicherheitsrecht etablierten Pflichten – Einführer müssen sicherstellen, dass der Hersteller ein Konformitätsbewertungsverfahren durchgeführt hat[148], und Händler müssen überprüfen, ob das Produkt mit der CE-Kennzeichnung versehen ist[149].[150] Für quelloffene Software sowie kleine und mittlere Unternehmen gibt es Sondervorschriften.[151]

Die Verordnung sieht Bußgelder bis zu 2,5 % des gesamten weltweiten Jahresumsatzes vor. Die Hauptvorschriften der Verordnung gelten ab dem 11. Dezember 2027, die Meldepflichten für Hersteller bereits ab dem 11. Juni 2026.[152]

b) Weitere Produktsicherheitsverordnungen der EU (Produktsicherheitsverordnung [EU] 2023/988, Maschinenverordnung [EU] 2023/1230 und Medizinprodukteverordnung [EU] 2017/745)

Vorschriften zur Cybersicherheit von Produkten finden sich zudem in weiteren Rechtsakten der Union. So müssen etwa Produkte, die von der Produktsicherheitsverordnung (EU) 2023/988[153] (die seit dem 13. Dezember 2024 gilt und das alte auf den Produktsicherheitsrichtlinien 87/357/EWG und 2001/95/EG beruhende ProdSG[154] in weiten Teilen ablöst) erfasst werden, Cybersicherheitsmerkmale aufweisen, „die erforderlich sind, um das Produkt vor äußeren Einflüssen, einschließlich böswilliger Dritter, zu schützen, sofern sich ein solcher Einfluss auf die Sicherheit des Produkts auswirken könnte, einschließlich eines möglichen Ausfalls der Verbindung".[155]

Die Maschinenverordnung (EU) 2023/1230[156] (gilt in allen Teilen ab dem 14. Januar 2027) schreibt vor, dass – wie schon bisher – Maschinen die grundlegenden Sicherheits- und Gesundheitsschutzanforderungen erfüllen müssen.[157] Hierzu zählt zukünftig auch ein Schutz gegen Korrumpierung der Hard- und Software – insbesondere bei Fernzugriffen.[158]

Die Medizinprodukteverordnung (EU) 2017/745[159] erfasst neben Geräten auch Software[160] und regelt in zahlreichen Vorschriften entsprechende Aspekte. So müssen – beispielhaft – Medizinprodukte so hergestellt werden, dass Risiken im Zusammenhang mit möglichen negativen Wechselwirkungen zwischen Software und der IT-Umgebung, in der sie eingesetzt wird, so weit wie möglich reduziert werden.[161]

c) Verordnung über künstliche Intelligenz (KI) (EU) 2024/1689

Die KI-Verordnung (EU) 2024/1689[162] regelt – soweit hier von Interesse – die Sicherheit von KI-Systemen.[163] Sie orientiert sich im Grundansatz ebenfalls am „Blue Guide" für die Produktsicherheit in der Union.[164] (Voll) verantwortlich für die Sicherheit der Systeme sind daher zunächst die Anbieter.[165] Diese entsprechen den „Herstellern" im herkömmlichen Produktsicherheitsrecht[166] und haben – wie dort – eine Konformitätsbewertung durchzuführen[167]. Die Verordnung differenziert zwischen unterschiedlichen Risikoklassen.

131 Art. 1 lit. a und b der Cyberresilienzverordnung (EU) 2024/2847.
132 Art. 3 Nr. 12 ff. der Cyberresilienzverordnung (EU) 2024/2847.
133 Kommission, Bekanntmachung „Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 (‚Blue Guide')", ABl. EU 2022 C 247, 1.
134 *Teichmann*, DuD 2025, 505, 506.
135 Art. 6 lit. a der Cyberresilienzverordnung (EU) 2024/2847.
136 Siehe oben, unter II. 2. c).
137 Anhang I Teil I (2) lit. d und g der Cyberresilienzverordnung (EU) 2024/2847.
138 Art. 13 Abs. 8 UAbs. 3 der Cyberresilienzverordnung (EU) 2024/2847.
139 Anhang I Teil II (7) und (8) der Cyberresilienzverordnung (EU) 2024/2847.
140 Art. 13 der Cyberresilienzverordnung (EU) 2024/2847.
141 Art. 27 Abs. 1 der Cyberresilienzverordnung (EU) 2024/2847.
142 Art. 32 Abs. 1 lit. a der Cyberresilienzverordnung (EU) 2024/2847.
143 Anhang III Klasse I Nr. 3 und 11 der Cyberresilienzverordnung (EU) 2024/2847.
144 Anhang IV Nr. 1 der Cyberresilienzverordnung (EU) 2024/2847. Solche Geräte werden etwa für kryptographische Operationen verwendet.
145 Art. 7 Abs. 1, Art. 32 Abs. 2 und 3 der Cyberresilienzverordnung (EU) 2024/2847. Siehe auch *Hansen*, DuD 2025, 288, 290.
146 Kritisch hierzu *Siglmüller*, ZfPC 2023, 221, 223, der fürchtet, es entstehe hierdurch „eine hochsensible Sammlung an Angriffsmöglichkeiten auf die Europäische Union".
147 Art. 14 Abs. 2 der Cyberresilienzverordnung (EU) 2024/2847.
148 Art. 19 Abs. 2 lit. a der Cyberresilienzverordnung (EU) 2024/2847.
149 Art. 20 Abs. 2 lit. a der Cyberresilienzverordnung (EU) 2024/2847.
150 Siehe den Überblick bei *Do Chi*, K&R 2025, 440.
151 Art. 24 und 33 der Cyberresilienzverordnung (EU) 2024/2847.
152 Art. 71 Abs. 2 der Cyberresilienzverordnung (EU) 2024/2847.
153 Siehe hierzu *Becker/Maier*, K&R 2025, 73; *Mattheis*, CCZ 2024, 325; *Neumann*, BB 2024, 2882.
154 Die Bundesregierung hat unter dem 10.10.2025 den Entwurf für ein „Gesetz zur Änderung des Produktsicherheitsgesetzes und weiterer produktsicherheitsrechtlicher Vorschriften" vorgelegt, siehe den Gesetzentwurf der Bundesregierung, BR-Drs. 548/25. Der Entwurf baut auf dem Gesetzentwurf aus der 20. Legislaturperiode – Gesetzentwurf der Bundesregierung, BR-Drs. 231/24; BT-Drs. 20/12716 – auf.
155 Art. 6 Abs. 1 lit. g der Produktsicherheitsverordnung (EU) 2023/988.
156 Siehe hierzu *Deusch/Eggendorfer*, K&R 2024, 169, 172.
157 Art. 8 UAbs. 1 der Maschinenverordnung (EU) 2023/1230.
158 Ziffer 1.1.9 Anhang III Maschinenverordnung (EU) 2023/1230.
159 Siehe hierzu *Hessel/Kiefer/Dillschneider*, DuD 2025, 181.
160 Art. 2 Nr. 1 der Medizinproduktverordnung (EU) 2017/745.
161 Ziffer 14.2 Anhang I der Medizinproduktverordnung (EU) 2017/745.
162 Siehe hierzu *Binder/Egli*, MMR 2024, 626; *Borges*, CR 2024, 565; *Chibanguza/Steege*, NJW 2024, 1769; *Denga*, ZfPC 2023, 154; *Kilian/Denga*, NJW 2024, 2945; *Kohpeiß/Schaller*, CR 2024, 22; *Teichmann*, ZD 2025, 495. Siehe außerdem zu „IT-Sicherheit und Künstliche Intelligenz" *Pohlmann*, DuD 2025, 5, sowie *Halvani/Müller*, DuD 2025, 302.
163 Art. 1 Abs. 1 der KI-Verordnung (EU) 2024/1689.
164 Siehe hierzu bereits oben, unter a).
165 Art. 16 i. V. m. Art. 3 Nr. 3 der KI-Verordnung (EU) 2024/1689.
166 Vgl. die Legaldefinitionen von „Anbieter" a. a. O. und „Hersteller" etwa in Art. 3 Nr. 13 der Cyberresilienzverordnung (EU) 2024/2847, hierbei handelt es sich jeweils um eine Person, die Produkte/KI-Systeme herstellt/entwickelt oder herstellen/entwickeln lässt und sie unter ihrem Namen oder ihrer Marke vermarktet.
167 Etwa Art. 43 der KI-Verordnung (EU) 2024/1689.

Die strengsten Vorschriften gelten für Hochrisiko-KI-Systeme[168] – hierunter fallen etwa „biometrische Fernidentifizierungssysteme" oder KI-Systeme zur Unterstützung von Justizbehörden. Für solche Systeme muss ein Risikomanagementsystem eingerichtet werden.[169] Sie müssen außerdem widerstandsfähig gegen Angriffe Dritter sein. Die Verordnung nennt ausdrücklich die Manipulation von Trainingsdatensätzen oder vortrainierter Komponenten, die beim Training verwendet werden, sowie von Eingabedaten. Angriffe müssen erkannt und verhütet werden.[170] Schwerwiegende Vorfälle sind den Marktüberwachungsbehörden zu melden.[171]

Bei KI-Modellen mit allgemeinem Verwendungszweck[172] – etwa großen Sprachmodellen wie ChatGPT oder Mistral – differenziert die Verordnung danach, ob diese ein „systemisches Risiko" aufweisen. Für die Einordnung ist u. a. die Menge der für die Berechnung verwendeten Gleitkommaoperationen entscheidend[173] – also die „Größe" des Modells. KI-Modelle mit einem systemischen Risiko müssen u. a. ein angemessenes Maß an Cybersicherheit für die Modelle und ihre physische Infrastruktur gewährleisten.[174]

d) BSI-ITSiKV

Anders als die zuvor erläuterten Verordnungen betrifft die Verordnung zum IT-Sicherheitskennzeichen des BSI (BSI-ITSiKV)[175] freiwillige Maßnahmen von Herstellern. Diese können beim BSI die Freigabe eines IT-Sicherheitskennzeichens für ein Produkt beantragen. Solche Kennzeichen sollen einen schnellen und einfachen Überblick zu Aspekten der IT-Sicherheit bei der Produktauswahl für Verbraucher ermöglichen.[176] Zur Erlangung eines IT-Sicherheitskennzeichens müssen die Hersteller gegenüber dem BSI versichern, dass ihr Produkt den einschlägigen IT-Sicherheitsanforderungen genügt.[177] Das BSI führt dann (lediglich) eine Plausibilitätskontrolle durch.[178] Bemerkenswert ist dabei, dass auch bei bekannten Sicherheitslücken die Ablehnung eines Antrags in das Ermessen des BSI gestellt ist („kann … ablehnen") und nicht etwa das Kennzeichen verweigert werden muss.[179]

2. Gewährleistungsrecht: Digitale-Inhalte-Richtlinie (EU) 2019/770, Warenkaufrichtlinie (EU) 2019/771 und BGB

Im Bereich des Gewährleistungsrechts haben die Digitale-Inhalte-Richtlinie (EU) 2019/770 und die Warenkaufrichtlinie (EU) 2019/771 eine unionsweite Vereinheitlichung (u. a.) sicherheitsrelevanter Aspekte des Gewährleistungsrechts bewirkt.[180]

Nach § 327f Abs. 1 BGB sind Unternehmer bei Verbraucherverträgen über digitale Produkte – etwa Apps oder Cloud-Dienste – verpflichtet, während des maßgeblichen Zeitraums Sicherheitsaktualisierungen bereitzustellen. Werden für ein digitales Produkt keine (Sicherheits-) Aktualisierungen bereitgestellt, entspricht das Produkt nicht den objektiven Anforderungen und ist mangelhaft. Dem Verbraucher stehen dann Gewährleistungsansprüche – etwa Nacherfüllung, eine Vertragsbeendigung oder Preisminderung – zu.[181]

Eine entsprechende Verpflichtung zur Bereitstellung von Sicherheitsaktualisierungen besteht auch bei Verbrauchsgüterkaufverträgen über Waren mit digitalen Elementen – etwa einem Smartphone, aber auch modernen Fahrzeugen.[182]

3. Produkthaftung: Produkthaftungsrichtlinie (EU) 2024/2853 und ProdHaftG

Während die Digitale-Inhalte-Richtlinie (EU) 2019/770 und die Warenkaufrichtlinie (EU) 2019/771 (u. a.) die gesetzlichen Gewährleistungsrechte adressieren, nimmt die Produkthaftungsrichtlinie (EU) 2024/2853[183] die Haftung für Schäden durch fehlerhafte Produkte in den Fokus.[184] Die Richtlinie muss bis zum 9. Dezember 2026 in nationales Recht umgesetzt werden. Es ist zu erwarten, dass dies in Deutschland wie bisher im ProdHaftG erfolgen wird. Bislang liegt hierfür aber noch kein Gesetzentwurf vor. Die folgenden Ausführungen müssen sich deshalb am Richtlinientext orientieren.

Die Richtlinie regelt (insbesondere) die Haftung von Herstellern (und gleichgestellten Wirtschaftsakteuren – hierzu zählen auch Auftragsabwicklungs- bzw. „Fulfillment"-Dienstleister wie Amazon) gegenüber Verbrauchern für schadhafte Produkte.[185] Vom Produktbegriff ist zukünftig ausdrücklich auch Software erfasst.[186] Ein Schaden kann in der „Vernichtung oder Beschädigung von Daten, die nicht für berufliche Zwecke verwendet werden", vorliegen.[187] Bei der Frage, ob ein Produkt fehlerhaft ist, müssen zukünftig auch die „einschlägigen Anforderungen an die Produktsicherheit, einschließlich sicherheitsrelevanter Cybersicherheitsanforderungen", berücksichtigt werden.[188] Kann ein Produkt über Softwareupdates aktualisiert werden, so gilt es nach der Richtlinie als unter „Kontrolle des Herstellers".[189] Er haftet dann auch für Schäden, die durch fehlerhafte oder unterlassene Updates entstehen.[190]

V. Sonstige gesetzliche Regelungen

Regelungen zur IT-Sicherheit finden sich zudem in einer Vielzahl weiterer nationaler Gesetze. Diese sollen hier nur rein exemplarisch angerissen werden.

1. Öffentlich-rechtliche Verpflichtungen

Ausdrückliche Regelungen finden sich etwa im TDDDG. Dieses erfasst – sehr stark vereinfacht – die Internetbranche (oberhalb der Übertragungsebene).[191] Digitale Dienste müssen hiernach etwa Vorkehrungen gegen unerlaubte Zugriffe sowie

168 Art. 6 Abs. 1 und 2 i. V. m. Anhang III der KI-Verordnung (EU) 2024/1689.
169 Art. 9 der KI-Verordnung (EU) 2024/1689.
170 Art. 15 (insbesondere Abs. 5) der KI-Verordnung (EU) 2024/1689.
171 Art. 73 der KI-Verordnung (EU) 2024/1689.
172 Art. 3 Nr. 63, Art. 53 ff. der KI-Verordnung (EU) 2024/1689.
173 Art. 51 Abs. 2 der KI-Verordnung (EU) 2024/1689.
174 Art. 55 Abs. 1 lit. d der KI-Verordnung (EU) 2024/1689.
175 Die Verordnungsermächtigung ist in § 10 Abs. 3 BSIG (§ 56 Abs. 2 BSIG-RegE) enthalten. Die gesetzlichen Regelungen finden sich in § 9c BSIG (§ 55 BSIG-RegE).
176 Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 19/26106, 30, 38.
177 § 7 Abs. 1 BSI-ITSiKV.
178 § 5 Abs. 1 BSI-ITSiKV.
179 § 5 Abs. 5 BSI-ITSiKV.
180 Siehe hierzu *Buchmann*, K&R 2022, 73; *Buchmann/Panfili*, K&R 2022, 159; 232; *Braun*, CR 2022, 727; *Kirchhefer-Lauber*, JuS 2021, 918; 1125; *Mayer/Möllnitz*, RDi 2021, 333; *Spindler*, MMR 2021, 451; *Thöne*, MMR 2025, 408.
181 § 327e Abs. 3 Nr. 5 i. V. m. § 327i BGB.
182 § 475b Abs. 2 Nr. 2 BGB.
183 *Brenner*, RDi 2024, 345; *Philipp*, EuZW 2024, 492; *Piovano/Hess*, ZfPC 2024, 90; 161; *Suilmann*, EuZW 2024, 961.
184 Art. 1 der Produkthaftungsrichtlinie (EU) 2024/2853.
185 Art. 1 der Produkthaftungsrichtlinie (EU) 2024/2853.
186 Art. 4 Nr. 1 der Produkthaftungsrichtlinie (EU) 2024/2853.
187 Art. 6 der Produkthaftungsrichtlinie (EU) 2024/2853; *Thöne*, MMR 2025, 408, 412.
188 Art. 7 Abs. 2 lit. f der Produkthaftungsrichtlinie (EU) 2024/2853.
189 Art. 4 Nr. 5 lit. a i) und lit. b der Produkthaftungsrichtlinie (EU) 2024/2853.
190 Erwägungsgründe 50, 51 der Produkthaftungsrichtlinie (EU) 2024/2853.
191 § 2 Abs. 1 TDDDG verweist für die Legaldefinition von „digitaler Dienst" auf die Begriffsbestimmung des DDG. Das DDG verweist sodann seinerseits auf die Informationsgesellschaftsdiensterichtlinie (EU) 2015/1535. Diese Regelungstechnik ist geradezu anwendungsfeindlich.

Störungen durch äußere Angriffe ergreifen.[192] Das Gesetz erwähnt hierfür ausdrücklich anerkannte Verschlüsselungsverfahren.

Ein weiteres Beispiel findet sich in § 391 SGB V. Hiernach sind Krankenhäuser verpflichtet, angemessene Vorkehrungen zur Absicherung ihrer informationstechnischen Systeme zu treffen. Dabei kann auf branchenspezifische Sicherheitsstandards zurückgegriffen werden.

2. Zivilrechtliche Regelungen

Verpflichtungen zur Absicherung der Unternehmens-IT können sich zudem aus zivilrechtlichen Generalklauseln ergeben. So umfassen die Sorgfaltspflichten nach § 93 AktG oder § 43 GmbHG selbstverständlich auch eine allgemeine Verpflichtung der Unternehmensleitung, unternehmenskritische IT-Systeme abzusichern.[193]

Mittelbar wirkt sich auch das GeschGehG auf die IT-Sicherheit aus. Hiernach setzt der Begriff des Geschäftsgeheimnisses nämlich voraus, dass angemessene Geheimhaltungsmaßnahmen ergriffen werden.[194]

VI. Fazit

Das IT-Sicherheitsrecht ist in einer Vielzahl von Gesetzen auf nationaler und unionaler Ebene geregelt. Diese Vielfalt ist vor allem dem Umstand geschuldet, dass das IT-Sicherheitsrecht sehr unterschiedliche Bereiche – etwa öffentliches Recht/Zivilrecht oder grundsätzliche institutionelle Aspekte/Detailfragen der Produktsicherheit – betrifft. Während dieser Gesichtspunkt systemimmanent ist, wird das IT-Sicherheitsrecht in der Praxis durch eine bislang nicht erfolgte Umsetzung insbesondere der NIS-2-Richtlinie (EU) 2022/2555 und der CER-Richtlinie (EU) 2022/2557 unnötig erschwert. Hier ist zu hoffen, dass der Gesetzgeber nun für schnelle Abhilfe sorgt.

192 § 19 TDDDG.
193 Vgl. nur *Spindler*, in: Münchener Kommentar zum AktG, 6. A., 2023, § 93 Rn. 88.
194 § 2 Nr. 1 lit. b GeschGehG.

Christopher Meissner

Die Novelle des Kohlendioxid-Speicherung-und-Transport-Gesetzes

Systemwechsel im Kohlendioxidinfrastrukturrecht

Der Entwurf des Kohlenstoffdioxid-Speicherung-und-Transport-Gesetzes (KSpTG-RegE) markiert den Beginn eines neuen Infrastruktursegments der Netzwirtschaften. Erstmals wird der Aufbau einer eigenständigen Transport- und Speicherinfrastruktur für Kohlendioxid rechtlich ermöglicht und mit Elementen des energiewirtschaftlichen Planungs- und Genehmigungsrechts verknüpft. Für die Netzwirtschaften eröffnet der Gesetzentwurf weitreichende Perspektiven: Erstmals wird eine eigenständige Kohlenstoffdioxidtransportinfrastruktur mit EnWG-naher Systematik geschaffen, die langfristig neben Gas-, Wasserstoff- und Elektrizitätsnetzen als vierte Säule der Energieinfrastruktur fungieren kann.

I. Einordnung und Regelungsziel

Die Bundesregierung legt mit dem Entwurf zur Änderung des Kohlendioxid-Speicherungsgesetzes (KSpG[1]) vom 6. August 2025[2] einen grundlegenden Ausbau des Rechtsrahmens für Abscheidung, Transport und dauerhafte Speicherung von Kohlendioxid (CO_2) vor. Ausgangspunkt ist die Treibhausgasneutralität bis 2045 nach § 3 Abs. 2 KSG sowie die im Evaluierungsbericht zum KSpG aus dem Jahr 2022[3] bestätigte Notwendigkeit der Kohlendioxidabscheidung und -speicherung („Carbon Capture and Storage", CCS) und der Kohlenstoffabscheidung und -nutzung („Carbon Capture and Utilization", CCU) zur Zielerreichung. Der Entwurf beseitigt rechtliche Unsicherheiten für Kohlendioxidleitungen, eröffnet den kommerziellen Speicherbetrieb und führt ein einheitliches Zulassungsregime ein. Zugleich werden die im Evaluierungsbericht empfohlenen Anpassungen umgesetzt, einschließlich eines Rechtsrahmens für den Aufbau einer Transportinfrastruktur.

Der Entwurf aktualisiert darüber hinaus Verweisungen in das EnWG, harmonisiert Verfahrensregeln und beziffert den zusätzlichen einmaligen Erfüllungsaufwand der Wirtschaft mit rund 5,89 Millionen Euro sowie den jährlichen mit rund 7,82 Millionen Euro. Für die Verwaltung werden einmalig Kosten von rund 10,39 Millionen Euro und jährlich von rund 2,57 Millionen Euro veranschlagt.

Die „Carbon Management Strategie" (CMS) der Bundesregierung zeigt, dass CCS und CCU nicht beliebig, sondern nur für schwer vermeidbare Restemissionen vorgesehen sind. Dazu nennt sie beispielsweise die Kalk- und Zementproduktion und die thermische Abfallbehandlung, bei der Emissionen anfallen, die nicht vermeidbar sind. Als weiteres Anwendungsfeld stellt sie Industrieprozesse heraus, solange die Umstellung auf Elektrifizierung oder Wasserstoff absehbar noch nicht kosteneffizient möglich ist.[4] Die Funktion von CCS und CCU liegt daher in der Ergänzung, nicht im Ersatz von Emissionsminderungen.[5] Diese teleologische Vorgabe prägt das gesamte Gesetz. Der Ausschluss von Kohlendioxid, das durch die Verbrennung von Kohle entsteht (§ 33 Abs. 5 KSpTG-RegE), ist deshalb nicht nur ordnungspolitisch sinnvoll, sondern unmittelbarer Ausdruck der „Carbon Management Strategie" und als

1 Gesetz zur Demonstration der dauerhaften Speicherung von Kohlendioxid (Kohlendioxid-Speicherungsgesetz – KSpG) v. 17.8.2012, BGBl. 2012 I, 1726; zuletzt geändert durch Gesetz v. 27.2.2025, BGBl. 2025 I Nr. 70.
2 Gesetzentwurf der Bundesregierung, BT-Drs. 21/1494.
3 Bundesregierung, Evaluierungsbericht zum Kohlendioxid-Speicherungsgesetz, BT-Drs. 20/5145.
4 Bundesregierung, Eckpunkte für eine Carbon Management-Strategie v. 26.2.2024, S. 3 f.
5 *Westmark*, KlimR 2025, 8, 9 f.