Kommunikation & Recht

K&R
5 | Mai 2026
29. Jahrgang
Seiten 293 - 364

dfv Mediengruppe
Frankfurt am Main

Wer halluziniert? Und wenn ja: Wie viele?
Prof. Dr. Simon J. Heetkamp

293 Nach der Umsetzung der NIS-2-Richtlinie ist vor der Reform der NIS-2-Richtlinie
Prof. Dr. Alexander Koch

297 Update IT-Sicherheitsrecht 2026
Dr. Florian Deusch und Prof. Dr. Tobias Eggendorfer

303 Entwicklungen im zivilrechtlichen Telekommunikationsrecht im Jahr 2025
Dr. Thomas Sassenberg, Dr. Reto Mantz und Dr. Gerd Kirparski

311 Die geplanten Neuerungen des Digital Networks Act
Dr. Michael Biendl

317 Update: Besteuerung der digitalen Wirtschaft 2025/2026 – Teil 2
Prof. Dr. Jens M. Schmittmann

323 Länderreport Schweiz
Nicole Beranek Zanon

326 **EuGH:** Rechtsmissbräuchlicher Auskunftsanspruch zu personenbezogenen Daten
mit Kommentar von **Franziska Ladiges und Dr. Stefan Peintinger**

333 **EuGH:** Urheberrechtsschutz für kritische Ausgabe eines gemeinfreien Werks

339 **BGH:** Grenzen der Quellen-TKÜ bei heimlicher Aufschaltung auf Messenger-Accounts
mit Kommentar von **Claus Erhard**

343 **BGH:** Berechtigtes Interesse an Herausgabe von E-Mail-Adressen
mit Kommentar von **Conrad S. Conrad und Elena Folkerts**

347 **BGH:** Reichweite der Störerhaftung bei rechtswidriger Erstberichterstattung

352 **BGH:** Auftraggeber haftet für Google-Ads-Anzeigen

355 **OLG Schleswig-Holstein:** Irreführende Hinweise bei Online-Kündigung von Mobilfunkverträgen

362 **LG Köln:** Unzureichende Parodie-Kennzeichnung eines Social-Media-Accounts

und im Übrigen nur alle drei Monate in anonymisierter und aggregierter Form informieren.[51]

IX. Fazit

Die vorgesehenen Änderungen betreffen zunächst sinnvolle Anpassungen des Anwendungsbereichs der NIS-2-RL. Unausgereift scheinen bislang aber die Vorschriften zu Informationspflichten über Lösegeldzahlungen. Hier wird es rechtsgebietsübergreifender Regelungen im nationalen wie unionalen Recht bedürfen, um Strafverfolgungsrisiken für die handelnden natürlichen Personen und ordnungs- und verwaltungsrechtliche Sanktionen für die betroffenen Unternehmen auszuschließen.

Grundsätzlich zu begrüßen ist der Ansatz in der Digital-Omnibus-Verordnung, die betroffenen Einrichtungen bei der Meldung von Sicherheitsvorfällen zu entlasten. Allerdings sollte erneut erwogen werden, ob eine zentrale Meldestelle bei der ENISA der richtige Weg ist. Hierüber wird ein einzelner Angriffspunkt („Single-Point-of-Failure") geschaffen, über den ein Angreifer sämtliche Meldungen in der EU verhindern kann. Das ist ein Risiko, welches es überaus sorgfältig gegenüber dem Nutzen für die betroffenen Einrichtungen abzuwägen gilt. Dabei ist zu bedenken, dass der bisherige Vorschlag ohnehin nur die Erstmeldung adressiert. Die Einrichtungen sind weiterhin mit einer Vielzahl von Rechtsvorschriften und Aufsichtsbehörden konfrontiert. Zu erwägen wäre deshalb, zentrale Anlaufstellen auf nationaler Ebene vorzuschreiben und vorzusehen, dass Einrichtungen nur noch in einem Mitgliedstaat eine Meldung abzugeben haben.

Es ist zu hoffen, dass der Gesetzgebungsprozess auf Unionsebene zügig abgeschlossen wird und die nationalen Gesetzgeber dann für eine schnelle Umsetzung sorgen. Die unionsweiten Verzögerungen bei der Umsetzung der NIS-2-RL dürfen sich angesichts der Bedeutung der Cybersicherheit unter einer massiv veränderten Weltsicherheitslage nicht wiederholen.

Der deutsche Gesetzgeber sollte nicht auf die Kommission warten, bis er erste Korrekturen der NIS-2-Umsetzung angeht. Die Umsetzung weist einige handwerkliche Fehler auf, die schnellstmöglich korrigiert werden sollten. Das beginnt bei kleineren Fehlern, wie Verweise auf nicht mehr existierende Paragraphen – die Verweise auf § 3 EnWG in Ziffer 1 der Anlage beziehen sich auf den EnWG-Gesetzesstand bis Dezember 2025. Hier dürften sich die Gesetzgebungsvorhaben schlicht überschnitten haben. Schwerer wiegen – vermutlich unbeabsichtigte – Systembrüche bei den Bußgeldern: Während das BSIG – wie von Art. 34 der NIS-2-RL vorgesehen – Bußgelder für unterlassene Meldungen bis 10 Millionen Euro oder 2 % des Gesamtumsatzes vorsieht, ist der Bußgeldrahmen für entsprechende Verstöße nach dem TKG nicht angepasst worden und liegt weiterhin bei lediglich 10 000 Euro.[52] Das sollte Anlass zu einer grundsätzlichen Überprüfung der deutschen Regelungstechnik geben. Historisch ist es nachvollziehbar, weshalb die Verpflichtungen für TK- und Energieunternehmen im TKG bzw. dem EnWG geregelt wurden. Das führt nun aber dazu, dass Änderungen am Cybersicherheitsrecht in jeweils drei Gesetzen – dem TKG, dem EnWG und BSIG – umgesetzt werden müssen. Das ist nicht nur fehleranfällig, sondern auch unnötig. Es sollte deshalb erwogen werden, das Cybersicherheitsrecht für alle Unternehmen in einem einheitlichen Gesetz zu regeln und die Sonderregelungen aus dem TKG und EnWG herauszulösen.

Schließlich ist es wenig hilfreich, wenn die Terminologie des deutschen Rechts von der Terminologie des Unionsrechts abweicht. So ist unverständlich, warum das deutsche Recht zwischen besonders wichtigen und wichtigen Einrichtungen unterscheidet, während das Unionsrecht auf wesentliche und wichtige Einrichtungen abstellt. Hier wäre eine Anpassung der Terminologie sinnvoll.

Prof. Dr. Alexander Koch
Rechtsanwalt und Partner in der Kanzlei Koch & Neumann, einer der Geschäftsführer des Instituts für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie (IRNIK) und Honorarprofessor an der Philipps-Universität Marburg, wo er (IT-) Strafrecht lehrt, und Dozent an der Westfälischen Hochschule Gelsenkirchen für IT-Recht, Datenschutz und Ethik.

51 Art. 23 Abs. 6 und 9 NIS-2-RL.
52 Siehe hierzu schon *Koch*, N&R 2026, 13, 22, Fn. 96.

RA Dr. Florian Deusch und Prof. Dr. Tobias Eggendorfer*

Update IT-Sicherheitsrecht 2026

Kurz und Knapp

Die Autoren stellen anschließend an ihr Update aus den Vorjahren in K&R 2024, 169 ff. und 242 ff. die Entwicklung des IT-Sicherheitsrechts im Zeitraum 2024 - 2026 anhand ausgewählter Akte der Gesetzgebung und der Rechtsprechung dar. Aufgrund der Betriebsamkeit der legislativen Ebenen liegt der Schwerpunkt auf der Gesetzgebung.

I. Einführung und Gefährdungslage

Die Gefährdungslage aus dem Cyberraum für gewerbliche und private IT-Nutzer ist im Berichtszeitraum ungebrochen angespannt geblieben. An der Tagesordnung stehen für viele Unternehmen nach wie vor arbeitsteilig orchestrierte Ransomware-Attacken (80 % der Opfer in Deutschland waren kleine und mittlere Unternehmen). Die Täter nutzen zahlreiche Sicherheitslücken in gängiger Software für ihre Zwecke aus, z. B. indem sie die Opfer durch teilweise mit KI erzeugten Phishingmails überzeugen, ihre Schadsoftware zu installieren,[1] was sichere Betriebssysteme selbständig verhindern sollten.

* Mehr über die Autoren erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 25. 3. 2026.
1 ENISA Threat Landscape 2025, https://ruw.link/2026/79 (enisa.europa.eu); BSI-Lagebericht zur IT-Sicherheit 2025 (https://medien.bsi.bund.de/lagebericht/de/index.html).

Der vorliegende Beitrag setzt sich damit auseinander, wie Gesetzgebung und Rechtsprechung mit den hieraus folgenden Rechtsfragen umgehen. Er stellt grundlegende verfassungsrechtliche Aspekte voran und beleuchtet im Anschluss die Spezialregelungen des IT-Sicherheitsrechts.

II. Verfassungsrechtliche Aspekte

Nutzer erwarten, dass IT-Systeme Daten sicher vor fremdem Zugriff (Vertraulichkeit), unverändert (Integrität) und mit nachweisbarer Urheberschaft (Authentizität) halten und ihre Datenverarbeitung nachvollziehbar ist. Aus Sicht des Verfassungsrechts verlangen Rechtsstaatlichkeit, Demokratieprinzip und Grundrechte vom Staat, dass er die Kontrollierbarkeit und Nachvollziehbarkeit gewährleistet, wenn er selbst IT einsetzt.[2] Vor diesem Hintergrund haben die folgende Gerichtsentscheidung und Gesetzgebungsvorhaben Relevanz für die IT-Sicherheit.

1. BVerfG: Strategische Fernmeldeaufklärung und Funktionsfähigkeit der IT

Das BVerfG hatte über die Befugnis des BND zur strategischen Fernmeldeaufklärung gemäß § 5 Abs. 1 Nr. 8 G-10-Gesetz zu entscheiden. Hiernach darf der BND die grenzüberschreitende elektronische Kommunikation jeglicher Nutzer vom Inland ins Ausland und vice versa überwachen, z. B. Telefonate, E-Mails oder Messenger-Nachrichten. Das BVerfG stellte einerseits fest, dass ein überragendes öffentliches Interesse besteht, die Funktionsfähigkeit der informationstechnischen Systeme (mithin die IT-Sicherheit) insbesondere von kritischen Infrastrukturen i. S. d. Art. 2 Nr. 1, 4 und 5 RL (EU) 2022/2557 (CER-RL) sowie von Verfassungsorganen und Gerichten gegen IT-Angriffe zu schützen. Allerdings muss der Gesetzgeber transparent regeln, wie er diesen Schutz ausgestaltet. Hierzu gehört es für das BVerfG auch, „Daten aus der reinen Inlandskommunikation mit allen zur Verfügung stehenden Mitteln technisch herauszufiltern und spurenlos zu löschen."[3] Offen bleibt allerdings in praxi, anhand welcher Parameter ein abgegriffenes Kommunikationsdatum in einem automatisierten Verfahren als Inlands- oder Auslands-Kommunikation identifiziert werden kann. Zwar würden die IP-Adressen einen Anhalt geben, weil sie landesweise vergeben werden, doch könnten zwei Inländer auch über einen ausländischen Server Daten austauschen – das ist z. B. bei Cloud-Lösungen wie MS Office 365 typisch. Fraglich ist daher, ob eine Kommunikation von Inländern über ausländische Infrastruktur in gleicher Weise schützenswert ist, wie eine „reine Inlandskommunikation" i. S. d. BVerfG, bzw. als solche gelten kann. Es wäre auch zu hinterfragen, inwieweit das Risiko, Teil der Überwachung als Auslandsnutzer zu werden, für normale Nutzer ersichtlich ist.

Technisch fraglich ist weiterhin, ob nach der Vorstellung des BVerfG ausländische Straftäter, die sich über geeignete Tunnel,[4] z. B. VPNs, auf deutsche Server verbinden, von der Überwachung ausgenommen sein sollen. Damit stellt sich die Frage, ob hier das BVerfG nicht technisch Unmögliches verlangt.

2. KI-gestützte Polizeiarbeit

Kritisch zu beobachten bleibt zudem der Einsatz KI-gestützter Analysesoftware durch die Polizeibehörden. Umstritten ist sie nicht nur wegen der Datenhaltung in der Cloud, der Nutzung von Daten als Lernmaterial für die KI und weiteren Fragen, die auch weitere Anbieter betreffen, sondern vor allem auch wegen der politisch-ideologischen Verflechtungen des Herstellers Palantir, dessen Produkte in verschiedenen Bundesländern Einsatz finden. Die Rechtsgrundlagen sind in den Polizei- und Ordnungsgesetzen von Bayern, Baden-Württemberg, Hessen und Nordrhein-Westfalen verabschiedet. Obwohl diese Länder die Palantir-Software auf den Servern ihrer LKAs („On-Premises") betreiben, bleiben wesentliche IT-Sicherheitsfragen offen, z. B. weil der Softwareanbieter den Quellcode nur in Teilen zur Prüfung bereitgestellt hat. Weiter ist die Software ohne Internetanbindung dem Vernehmen nach nicht funktionsfähig, womit unklar ist, ob nicht doch ein Datenabfluss stattfinden könnte. Unklar ist zudem, wie dauerhaft sichergestellt bleibt, dass der Programmcode den Sicherheits- und Datenschutzanforderungen über einen Prüfungszeitpunkt hinaus genügt, obwohl die Beschäftigten des US-Anbieters im Rahmen der beauftragten Pflege jederzeit die Gelegenheit haben,[5] ihn zu ändern (insbesondere bei Updates und Änderungen an der Konfiguration).[6]

3. Sachstand Chatkontrolle

Noch immer ungeklärt ist die Umsetzung der sogenannten „Chatkontrolle". Problematisch hieran ist, dass der Staat eine Sicherheitslücke in der elektronischen Kommunikation schafft, in dem er Ende-zu-Ende-Verschlüsselungen durch staatlichen Zwang durchbricht. Unklar ist dabei, ob diese Sicherheitslücke ausschließlich zum vorgesehenen Zweck verwendet wird (Minderjährigenschutz vor sexuellem Missbrauch) oder ob sie nicht weitere staatliche Begehrlichkeiten weckt bzw. sogar durch Kriminelle ausgenutzt werden wird. Bislang waren die Chatkontrollen zulässig aufgrund befristeter Einschränkung der E-Privacy-RL durch VO (EU) 2021/1232, zuletzt verlängert bis 26. 4. 2026 durch VO (EU) 2024/1307. Eine Neuregelung der Chatkontrolle ist aber laut Berichten der Tagespresse ebenso wie eine weitere Verlängerung der derzeitigen Regelung über den 26. 4. 2026 hinaus gescheitert. Unklar bleibt, wie die aktuell vorgeschlagene freiwillige Kontrolle der Anbieter der Messengerdienste technisch funktionieren soll. Denn bei einer Ende-zu-Ende-Verschlüsselung haben auch diese keinen Zugriff. Möglicherweise bietet die eIDAS 2.0 Verordnung eine Hintertür für Behörden.[7]

III. Cybersecurity Act

1. Cybersecurity Act 2

Im Januar 2026 hat die EU-Kommission ein Cybersicherheitspaket vorgeschlagen, bestehend aus einer Neufassung des bisherigen Cybersecurity Act (VO (EU) 2019/887, dazu so-

2 Kuppe, VVdStRL, Band 78, 2018, 312 ff., 331 (Leitsatz 27), *Hornung*, in: Schoch/Schneider, Verwaltungsrecht, VwVfG, 7. Ergänzung, Mai 2025, § 3a VwVfG Rn. 17; *Deusch/Eggendorfer*, in: Taeger/Pohle (Hrsg.), Computerrechts-Handbuch, 40. Aufl. 2025, Kap. 50.1 Rn. 388 sowie Rn. 16 ff. zu den Zielen der IT-Sicherheit.

3 BVerfG, 8. 10. 2024 – 1 BvR 1743/16 u. a., NVwZ 2025, 563 (m. Anm. *Huber*); *Schubert*, jurisPR-ITR 24/2024 Anm. 3.

4 *Eggendorfer*, Netzwerktunnel. Hintergründe, Funktionsweise und Gegenmaßnahmen, 2026.

5 Nach US-Recht sind die Anbieter womöglich verpflichtet Änderungen vorzunehmen, die ein Belauschen bzw. einen Regierungszugriff auf Informationen ermöglichen (siehe das Gutachten der Universität zu Köln vom 21. 3. 2025 unter https://ruw.link/2026/80 (fragdenstaat.de)).

6 Rechtsgrundlagen sind z. B. Art. 61a bayer. Polizeiaufgabengesetz, §§ 47a, 57a PolG BW, § 25a HSOG; siehe zum Ganzen *Bäuerle/Denker/Geminn/Schöndorf-Haubold*, in: Schöndorf-Haubold (Hrsg.), Big Data und KI bei der Polizei, 2025; *Deusch/Eggendorfer*, KI-Kompetenz von Sicherheitsbehörden nach dem AI Act; *Pfeffer* (Hrsg.), AI and Policing in the Security Union, Chancen, Risiken und rechtliche Herausforderungen nach dem AI-Act, 8. Hamburger Sicherheitsrechtstag, 2026; zu den IT-Sicherheitsrisiken infolge der unzureichenden Prüfung des Quellcodes und der Softwarepflege siehe die Stellungnahme von *Manuel Atug* beim Petitionsausschusses des baden-württembergischen Landtags zur Petition 17/4192, Landtags-Drucksache 17/9765 (https://ruw.link/2026/81 (landtag-bw.de)).; dort ab Minute 52).

7 Zur bisherigen Chatkontrolle bereits *Deusch/Eggendorfer*, K&R 2024, 169, 173; zur gescheiterten Neuregelung *Heckmann*, jurisPR24/2025, Anm. 1 (Editorial) sowie https://ruw.link/2026/82 (tagesschau.de); zur Ende-zu-Ende-Verschlüsselung *Deusch/Eggendorfer*, K&R 2022, 577 ff.; zur eIDAS 2.0 Verordnung *Eggendorfer/Schmidt-Wudy*, K&R 2024,13 ff.

gleich) sowie einer Anpassung der NIS-2-RL [RL (EU) 2022/2555, dazu siehe unten IV. 2. b)].

Der Vorschlag COM(2026)11 final der EU-Kommission (nachfolgend: E-CSA 2) sieht vor, den bisherigen Cybersecurity Act (VO (EU) 2019/887 als „Cybersecurity Act 2" vollständig neu zu fassen, und zwar mit folgenden Inhalten:[8]

- Das Mandat der ENISA soll neu definiert werden (Titel II, Art. 3 ff. E-CSA 2). Mit zusätzlichen 118 Vollzeitstellen und einer Steigerung des Budgets aus 2025 um 81,5 %[9] soll die ENISA ertüchtigt werden, um zahlreiche Aufgaben aus weiteren EU-Verordnungen und Richtlinien zur Cybersicherheit zu übernehmen, z. B. die Reporting-Plattform für Schwachstellenmeldungen gemäß Art. 16 VO (EU) 2024/2847 (Cyber Resilience Act) und Art. 12 RL (EU) 2022/2555 (NIS-2-RL).[10] Bereits dies sorgt für eine komplexe Verzahnung des geplanten E-CSA 2 mit weiteren EU-Cybersecurity-Rechtsakten.
- Die Art. 71 ff. in Titel III E-CSA 2 regeln die Rahmenbedingungen für Zertifizierungen im Bereich der Cybersecurity neu. Während die Art. 48 ff. des bisherigen CSA (VO (EU) 2019/887) lediglich einen Rahmen zur Entwicklung von Zertifizierungsstandards geschaffen haben,[11] wird der E-CSA 2 weitreichender und verbindlicher: Neu ist insbesondere die Schaffung von Standards zur „Cyber Posture" (Art. 71 Nr. 2 lit. c E-CSA 2); sie sollen Maßstäbe für die Sicherheitslage in einer Einheit schaffen. Die geplante Novellierung der NIS-2-RL (siehe unten Abschnitt IV Ziff. 2) sieht vor, dass die EU-Mitgliedstaaten von NIS-2-regulierten Unternehmen eine „Cyber Posture"-Zertifizierung verlangen können. Neben der Cyber Posture sieht Art. 71 E-CSA 2 Standards zur Zertifizierung von IT-Produkten, Diensten, Prozessen und Managed Security Services vor.
- Schließlich legt Titel IV (Art. 98 ff. E-CSA 2) ein Regelwerk fest, um Sicherheitsanforderungen an die Lieferkette für ICT-Komponenten[12] zu definieren, die NIS-2-regulierte Einheiten einsetzen. Hier geht es zuvorderst um nicht-technische Risiken, die sich aus den Herkunftsländern dieser Komponenten ergeben sollen, z. B. Russland. Die EU-Kommission soll ermächtigt werden, die Nutzung derartiger ICT-Schlüsselkomponenten in NIS-2-Sektoren zu untersagen.[13] Die Art. 110 ff. E-CSA 2 zielen dabei insbesondere auf Komponenten für die Telekommunikation ab (Festnetze und Mobilfunk, Satelliten und gemäß ErwGr (156) E-CSA 2 5-G-Technologie).

2. EUCC-Scheme

Per Durchführungsverordnung (EU) 2024/482 vom 31. 1. 2024 hat die EU-Kommission auf der Grundlage des bestehenden CSA (VO (EU) 2019/887) das europäische System für die Cybersicherheitszertifizierung (EUCC) festgelegt.[14] Hersteller von Produkten der Informations- und Kommunikationstechnologie (IKT-Produkte gemäß Art. 2 Nr. 12 CSA) können auf dieser Grundlage Zertifizierungen erhalten und die Konformität ihres Produkts oder des Herstellungsprozesses nachweisen (Art. 1 Abs. 2 der Durchführungsverordnung). Die Eignung und Zukunftssicherheit sowie Flexibilität bei neuen technischen Entwicklungen der EUCC zu bewerten und einzuordnen bleibt einem eigenen Beitrag vorbehalten.

IV. NIS-2 und BSIG

1. Umsetzung NIS-2-RL durch Neufassung BSIG

Der deutsche Gesetzgeber hat die Vorgaben der NIS-2-RL (RL (EU) 2022/2555) durch eine Neufassung des BSIG mit Wirkung zum 6. 12. 2025 umgesetzt.[15]

Das BSIG gilt für

- „besonders wichtige Einrichtungen" (§ 28 Abs. 1 BSIG, entspricht den „wesentlichen Einrichtungen" i. S. d. Art. 3 Abs. 1 NIS-2-RL[16]) mit der Unterkategorie der „Betreiber kritischer Anlagen" gemäß § 28 Abs. 1 Nr. 1 BSIG[17] und
- „wichtige Einrichtungen" (§ 28 Abs. 2 BSIG, entspricht den „wichtigen Einrichtungen" i. S. d. Art. 3 Abs. 2 NIS-2-RL).
- Einrichtungen der Bundesverwaltung sind in § 29 BSIG gesondert geregelt; Landes- und Kommunalverwaltungen sind vom BSIG nicht erfasst; einige Bundesländer haben entsprechende Regelungen erlassen, z. B. Baden-Württemberg durch die Cybersicherheitsverordnung vom 16. 4. 2025. Sie erfasst auf der Grundlage von § 2 Abs. 1, 3 Cybersicherheitsgesetz BW alle Stellen, die der Aufsicht des Landes unterliegen, nicht aber die Landratsämter als untere Verwaltungsbehörden.[18]

Die „wichtigen" und „besonders wichtigen" Einrichtungen sind in den Anlagen 1 und 2 zum BSIG definiert. Sie betreffen die Sektoren der bisherigen „KRITIS-Unternehmen" i. S. d. § 2 BSIG a. F. und darüber hinaus weitere Unternehmen, insbesondere aus der verarbeitenden Industrie.[19]

Relevant für den Geltungsbereich des BSIG ist die Abgrenzung, ob die Tatbestandsmerkmale der Anlagen 1 und 2 erfüllt sind; hierfür ist bisweilen eine detaillierte Auseinandersetzung mit dem NACE-Code Rev 2 erforderlich, den NIS-2-RL und BSIG heranziehen.[20] Auch für weitere Sektoren ergeben sich Abgrenzungsfragen. So ist z. B. keineswegs geklärt, welche Leistungsangebote zur Kategorie „Cloud-Computing" zählen.[21]

Zudem ist entscheidend, ob das betreffende Unternehmen die KMU-Schwellenwerte überschreitet (§ 28 Abs. 1, 2, 4 BSIG i. V. m. der Empfehlung der Kommission (2003/361/EG)). In Konzernen sind die Daten von Partner- und verbundenen Unternehmen nach der vorgenannten Kommissionsempfehlung grundsätzlich zusammenzurechnen. Dies gilt allerdings nicht, wenn das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informations-

8 https://ruw.link/2026/83 (digital-strategy.ec). Dazu auch *Schmidt*, K&R 2026, 226 - 230.
9 COM(2026)11, S. 14.
10 Art. 15, 16 CRA 2 COM(2026)11.
11 *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 2) Rn. 345.
12 ICT = Information and communication technology (siehe ErwGr 128 E-CSA 2).
13 Siehe die Art. 98, 100 E-CSA 2 zu den nicht-technischen Risiken, S. 11 COM(2026)11 zur Bezugnahme auf Russland und Art. 103 zur Untersagungsbefugnis.
14 https://ruw.link/2026/46 (certification.enisa.europa.eu).
15 BGBl. 2025 I Nr. 301 v. 5. 12. 2025, S. 1 - 68 (mit Änderung weiterer Gesetze und der BSI-KRITIS-VO), zwischenzeitlich bereits wieder geändert durch die Einführung des KRITIS-DachG vom 11. 3. 2026 (BGBl. 2026 I Nr. 66 vom 16. 3. 2026, dazu unter Abschnitt V). Hilfreich mag bisweilen auch ein Blick in die legislativen Entwürfe und deren Begründungen sein: BT-Drs. 21/1501 (Regierungsentwurf), 21/2072 (Bundesrat), 21/2782 (Innenaussch.), abrufbar unter https://ruw.link/2026/84 (bundestag.de).
16 Englischer Wortlaut von Art. 3 Abs. 1 NIS-2-RL „essential entities".
17 § 28 Abs. 8 BSIG i. d. F. v. 5. 12. 2025 (BGBl. 2025 I Nr. 301) enthielt noch eine Definition des „Betreibers kritischer Anlagen"; diese hat der Gesetzgeber des KRITIS-DachG (BGBl. 2026 I Nr. 66 vom 16. 3. 2026) gestrichen (siehe unter Abschnitt V). Sie ergibt sich für das BSIG nunmehr mittelbar, indem § 33 Abs. 2 BSIG zur Registrierung von Betreibern kritischer Anlagen auf § 8 KRITIS-DachG verweist und damit mittelbar auf die Definition in § 2 Nr. 1 KRITIS-DachG.
18 Cybersicherheitsverordnung BW (GBl. BW 2025, Nr. 32), beruhend auf dem Cybersicherheitsgesetz BW (GBl. 2021, 182).
19 Bereits eingearbeitet in: *Voigt*, IT-Sicherheitsrecht, 3. Aufl., 2026, Teil F Rn. 272.
20 Dazu bereits *Deusch/Eggendorfer*, K&R 2024, 169, 170.
21 *Weiss*, PinG 2026, 48; aufschlussreich hierzu auch die Ausführungen in ErwGr 33 NIS-2-RL.

technischen Systeme, Komponenten und Prozesse unabhängig von seinen Partner- oder verbundenen Unternehmen ist (§ 28 Abs. 4 S. 2 BSIG). Laut der Gesetzesbegründung zum BSIG[22] besteht eine solche Unabhängigkeit, wenn die IT-Systeme des betreffenden Unternehmens nicht durch den Konzern, sondern durch einen Dienstleister betrieben werden, „da hier durch vertragliche Regelungen bestimmender Einfluss auf die vorgenannten Eigenschaften ausgeübt werden kann." Hierdurch werde sichergestellt, dass Partnerunternehmen oder Tochterunternehmen für sich alleine zu sehen sind und die vorgesehenen Schwellen nicht überschreiten. Konzernunternehmen haben somit die Möglichkeit, durch Outsourcing der IT-Anlagen kleinerer Tochterunternehmen der Geltung des BSIG zu entgehen.

Zudem eröffnet der Wortlaut des § 28 Abs. 3 BSIG einen Ausweg aus der NIS-2-Regulierung, wenn die betreffende Tätigkeit des betroffenen Unternehmens im Vergleich zu anderen Tätigkeiten vernachlässigbar ist. Dies wird z. T. angenommen, wenn die NIS-2-betreffende Tätigkeit z. B. nicht mehr als 5 - 10 % des Gesamtumsatzes ausmacht. Mehrere Autoren halten die Regelung für unionsrechtswidrig, weil die NIS-2-RL eine solche Ausnahme nicht ermögliche.[23] Für die EU-rechtskonforme Auslegung des § 28 Abs. 3 BSIG könnte allerdings streiten, dass die Systematik des NACE-Codes, auf den die NIS-2-RL verweist, sehr wohl zwischen Haupt-, Neben- und Hilfstätigkeiten unterscheidet und die Kategorisierung nach der Haupttätigkeit vornimmt.[24]

Für die NIS-2-regulierten Unternehmen ordnen die §§ 30 - 35, 38 BSIG Pflichten zum Risikomanagement, zur Meldung von erheblichen Sicherheitsvorfällen nebst Unterrichtung über deren Behandlung und zur Umsetzung, Überwachung und Schulung der Geschäftsführung an. Zum Risikomanagement der Anbieter von Cloudcomputing- und Rechenzentrumsdiensten, Anbieter verwalteter (Sicherheits-)Dienste, Online-Marktplätze, Online-Suchmaschinen, Plattformen für Dienste sozialer Netzwerke sowie Vertrauensdiensteanbieter hat die EU-Kommission bereits die Durchführungsverordnung (EU) 2024/2690 erlassen; die ENISA hat eine „Implementation Guidance" dazu veröffentlicht.[25]

2. Geplante NIS-2-Änderungen

Die EU-Kommission plant bereits Änderungen an der NIS-2-RL.

a) Entwurf der „Digital-Omnibus-Verordnung"

Mit dem „Digital Omnibus" (COM(2025) 837 final) plant die EU-Kommission, die Meldung für sogenannte „Data Breaches" gemäß Art. 33 DSGVO in ihrer Frist von derzeit 72 auf künftig 96 Stunden zu verlängern. Zudem plant sie, die Data-Breach-Anzeigen mit der Meldung von Sicherheitsvorfällen nach Art. 23 RL (EU) 2022/2555 (NIS-2-RL) zu vereinheitlichen, indem die Meldung an eine „zentrale Anlaufstelle" erfolgt. Der Kommissionsvorschlag lässt allerdings die 24-stündige Frist zur Meldung von Sicherheitsvorfällen gemäß Art. 23 Abs. 4 NIS-2-RL unberührt, so dass der Rechtsanwender die beiden Fälle zu unterscheiden hat.[26]

Auch Finanzunternehmen sollen dann die schwerwiegenden IKT-bezogenen Vorfällen gemäß Art. 19 DORA an die gemeinsame Anlaufstelle melden.[27]

b) Entwurf zur Vereinfachung der NIS-2-RL und zur Anpassung an Änderungen des CSA

Mit dem Richtlinien-Entwurf COM(2026) 13 final vom 20. 1. 2026[28] plant die EU-Kommission insbesondere folgende Änderungen an der NIS-2-RL:

- Domänennamensystem-Diensteanbieter sind derzeit gemäß Art. 2 lit. a (iii) NIS-2-RL unabhängig von ihrer Größe der NIS-2-RL unterworfen. Dies soll künftig nur noch für „Top-Level-Domain-Registries" i. S. d. Art. 6 Nr. 21 der aktuellen NIS-2-RL gelten (z. B. die DENIC eG für Domains mit der Endung „.de").[29]
- Anbieter von EU Digital Identity Wallets (Digitale Brieftasche zum elektronischen Identitätsausweis gemäß Art. 5a VO (EU) 510/2014 = eIDAS-VO) und Anbieter von Dual Use Gütern (Güter, die zivil und militärisch genutzt werden können, wie sie im „military mobility" Vorschlag der EU-Kommission COM(2025) 847 final – definiert sind) sollen unabhängig von ihrer Größe der NIS-2-RL unterfallen.[30]
- Für wesentliche Einrichtungen gemäß Art. 3 Abs. 1 NIS-2-RL (besonders wichtige Einrichtungen gemäß § 28 Abs. 1 BSIG) wird eine Differenzierung eingeführt: Bislang waren alle Einrichtungen aus dem Anhang I NIS-2-RL wesentliche Einrichtungen, die die Schwellenwerte für mittlere Unternehmen überschreiten (250 Mitarbeiter, Jahresumsatz € 50 Mio. oder Bilanzsumme € 43 Mio. gemäß Art. 2 des Anhangs zur Empfehlung 2003/361/EG). Dem Entwurf zufolge sollen kleine Midcap-Unternehmen nur noch „wichtige" Einrichtungen i. S. d. Art. 3 Abs. 2 NIS-2-RL sein, auch dann wenn sie Einrichtungen unterhalten, die dem Anhang I NIS-2-RL unterfallen. Kleine Midcap-Unternehmen sind dabei solche mit weniger als 750 Mitarbeitern und einem Jahresumsatz von weniger als € 150 Mio. und einer Bilanzsumme von weniger als € 129 Mio. Diese sollen künftig nur noch die erleichterten NIS-2-Anforderungen für wichtige Einrichtungen erfüllen müssen.[31]
- Weitere Klarstellungen zum Anwendungsbereich enthalten die Änderungsvorschläge zum Anhang der NIS-2-RL. Stromerzeuger sollen z. B. erst ab einer Gesamterzeugungsleistung von mehr als 1 MW der NIS-2-RL unterfallen.[32] Dies dürfte künftig Fragen entschärfen, die sich z. B. für Betriebe ergeben, die (etwa auf ihren Dächern) Solaranlagen betreiben und Mitarbeitern Ladestationen für ihr E-Auto bereitstellen, aber überhaupt nicht zur Energiebranche gehören.
- Erleichterungen will die EU-Kommission durch eine Ergänzung des Art. 21 Abs. 5 NIS-2-RL erzeugen: Wenn die EU-Kommission Anforderungen an das IT-Risikomanagement

22 BT-Drs. 21/1501, S. 145, dazu auch *Pohle/Wascher/Winter*, CB 2026, 1 ff., 2.

23 Einerseits *Voigt/Schmalenberger*, CR 2026, 17, 20; zur Unionsrechtswidrigkeit *Hessel*, MMR 2026, 258 sowie *Pohle/Wascher/Winter* CB 2026, 1 ff., 3.

24 NACE Rev. 2, Seite 22, Ziff. 2.2 (https://ruw.link/2026/85 (bundesbank.de)).

25 Näher: *Karniyevich*, K&R 2026, 82 - 88 mit Hinweis auf die Durchführungsverordnung auf S. 85; *Schreiber*, BB 2026, 323 ff.; *Voigt*, IT-Sicherheitsrecht (Fn. 19), Rn. 312; Zur persönlichen Verantwortung der Geschäftsführung *Schreiber/Brinke*, BB 2024, 2696 ff.

26 Siehe Art. 3 Nr. 8 und Art. 6 Nr. 1 und 2 des Kommissionsvorschlags COM (2025) 837 final vom 19. 11. 2025 („Digital-Omnibus-Verordnung").

27 Art. 8 des Kommissionsvorschlags COM(2025) 837 final vom 19. 11. 2025 („Digital-Omnibus-Verordnung").

28 https://ruw.link/2026/64 (eur-lex.europa.eu). Siehe dazu den Hinweis der Redaktion auf *Koch*, K&R 2026, 293 ff. (in diesem Heft).

29 Art. 1 (1) (a) (i) COM (2026) final 13.

30 Art. 1 (1) (a) (ii) und (b) sowie Art. 1 (2) (a) (i) und (ii) COM (2026) final 13; technisch kann „Dual Use" indes schwer zu fassen sein. Denn den Anbietern von Standardsoftware, insbesondere bei der Veröffentlichung von Open Source Software, ist selten bekannt, für welche Zwecke ihre Entwicklungen genutzt werden.

31 Art. 1 (2) (a) (i) COM (2026) final 13; die Schwellenwerte der „kleinen Midcap Unternehmen" ergeben sich aus der Empfehlung (EU) 2025/1099 der Kommission vom 21. 5. 2025 zur Definition kleiner Midcap-Unternehmen C/2025/3500, ABl. (EU) L Nr. 251099 vom 28. 5. 2025 (dort Nr. 2 des Anhangs).

32 Nr. 1 und Nr. 2 des Annex COM (2026) final 13.

in Form von Durchführungsrechtsakten stellt, soll es den Mitgliedstaaten verwehrt sein, zusätzliche Maßnahmen zu verlangen. Zudem soll Art. 24 NIS-2-RL dahingehend ergänzt werden, dass die Mitgliedstaaten von den betroffenen Einrichtungen Zertifizierungen nach dem dann novellierten Cyber Security Act 2 (bislang: VO (EU) 2019/881) verlangen können (siehe oben Abschnitt III Ziff. 1).[33]

3. Warnungen des BSI

Zur Befugnis des BSI, Warnungen vor IT-Produkten zu veröffentlichen (§ 7 BSIG a. F. bzw. § 13 BSIG) entschied das VG Köln, dass es sich nicht um eine Warnung handle, wenn die Behörde ein Produkt untersucht hat und es in ihrem Abschlussbericht öffentlich als „auffällig" bezeichnet. Das VG versagte vorläufigen Rechtsschutz.[34]

V. CER-RL und KRITIS-DachG

Zur Umsetzung der RL (EU) 2022/2557 (CER-RL) hat der deutsche Gesetzgeber das KRITIS-DachG erlassen, das seit dem 17. 3. 2026 gilt.[35]

Das KRITIS-DachG richtet sich an Betreiber kritischer Anlagen in den definierten Sektoren Energie, Transport und Verkehr, Finanzwesen, Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitsuchende, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum sowie Siedlungsabfallentsorgung (§§ 2, 4 KRITIS-DachG). In der Sache zielt es auf die physische Sicherheit der regulierten Anlagen ab, während die NIS-RL und das BSIG die IT-Sicherheit dieser Anlagen sichern sollen. Die KRITIS-Betreiber sind zur Registrierung, Analyse, zum Risikomanagement und Aufstellung eines Resilienzplans, zum Nachweis des Risikomanagements, zur Meldung solcher Vorfälle, die nicht bereits durch das BSIG erfasst sind, verpflichtet; die Geschäftsleitungen treffen Umsetzungs- und Überwachungspflichten (§§ 8, 12 - 20 KRITIS-DachG).[36]

VI. TK-Kodex, DNG-E und TKG

An 21. 1. 2026 hat die EU-Kommission vorgeschlagen, den bisherigen TK-Kodex (RL (EU) 2018/1972 – EKEK bzw. EEEC) durch einen „Digital Networks Act" (Gesetz über digitale Netze – DNG) zu ersetzen (COM(2026) 16 final).

Da es sich um eine Verordnung handelt, die gemäß Art. 288 AEUV unmittelbar und zwingend gilt, wird zu prüfen sein, inwieweit noch Raum ist für die IT-Sicherheitsregeln im bisherigen TKG. Vorbehaltlich einer detaillierten Analyse schreibt der Entwurf des DNG die IT-Sicherheit den TK- und Internet-Access-Providern ins Stammbuch (z. B. Art. 9 Nr. 4b, 93 Nr. 3b und 105 DNG-E), wobei die Ausführungen auf Seite 4 des Kommissionsvorschlags Verzahnungen mit dem CSA (siehe oben Abschnitt III) aufzeigen.

VII. IT-Sicherheit im Finanzsektor unter dem DORA-Regime

Seit dem 17. 1. 2025 gelten die Anforderungen für Finanzunternehmen an das Risikomanagement im Bereich der Informations- und Kommunikationstechnologie (IKT) gemäß DORA (VO (EU) 2022/2554) und – soweit eine Umsetzung in nationales Recht notwendig war, das Finanzmarktdigitalisierungsgesetz – FinmadiG.[37] DORA definiert die Sicherheitsauflagen auf der ersten Ebene („Level 1"), während die zugehörigen Durchführungsrechtsakte der EU-Kommission und die Leitlinien der EU-Finanzaufsichtsbehörden[38] Konkretisierungen auf den Leveln 2 und 3 enthalten. Im Anwendungsbereich des IKT-Risikos haben diese Bestimmungen die bisherigen nationalen Regelungen abgelöst: Die §§ 25b KWG, 26 ZAG, 36 KAGB, 80 WpHG und deren Konkretisierungen durch die BaFin (MaRisk, KAMaRisk, BAIT, VAIT und ZAIT) werden von dem DORA-Regime verdrängt, soweit dieses Anwendung findet. Im Einzelfall wird zu prüfen sein, ob die bisherigen Regelungen aufgrund von Übergangsvorschriften bzw. Sonderkonstellationen noch gelten.[39]

VIII. IT-Sicherheit und Corporate Governance

Systematische IT-Sicherheit gehört zur ordnungsgemäßen Organisation und Führung jedes Unternehmens und jeder Behörde.[40]

Haftungsfragen entstehen, wenn vermeidbare Sicherheitslücken ausgenutzt werden und das Unternehmen geschädigt wird. Die Versicherungswirtschaft hat hierfür Angebote von „Cyberversicherungen" entwickelt.[41] Gerichte hatten in diesem Kontext zu entscheiden, dass

- elektronische Daten oder IT-Systeme des Versicherungsnehmers i. S. d. AVB Cyber nicht beeinträchtigt sind, wenn der Versicherungsnehmer eine gefälschte Rechnung per E-Mail erhält und den Betrag an den Täter und nicht den echten Rechnungsaussteller zahlt,[42]
- der Versicherungsnehmer alle ihm bekannten Gefahrumstände anzeigen muss, nach denen der Versicherer in Textform gefragt hat (wahrheitswidrige Mitteilung zu Antivirensoftware und Datensicherung „ins Blaue hinein" macht Versicherungsvertrag im Schadensfall anfechtbar).[43]

IX. IT-Sicherheit und Datenschutz; fehlerhafte Banküberweisungen

1. Reformvorhaben

Abgesehen von der Änderung des Meldeverfahrens bei „Data Breaches" (siehe oben Ziffer II) plant die EU-Kommission mit der „Digital-Omnibus-Verordnung", die Cookie-Regelungen der E-Privacy-RL 2002/58/EG in die DSGVO zu überführen.[44]

---

33 Art. 3 (7) und (9) COM (2026) final 13.

34 VG Köln, 2. 12. 2025 – 1 L 3105/25, ECLI:DE:VGK:2025:1202.1L3105.25.00 = K&R 2026, 282 f.; dazu *Ferner*, K&R 2026, 283 - 285, der die Entscheidung mit dem Beschluss des OVG Münster v. 28. 4. 2022 (4 B 473/22) zur Warnung vor Produkten des Malware-Scanner-Herstellers Kaspersky vergleicht und auf eine „technische Lesart" von § 7 BSIG a. F. (BSI-Befugnis zu Warnungen) abstellt, dazu allerdings die differenzierte Meinung der Verfasser in K&R 2022, 794, 800.

35 BGBl. 2026 I Nr. 66 vom 16. 3. 2026; zu den Gesetzgebungsmaterialien: https://ruw.link/2026/86 (bundestag.de).

36 *Voigt*, IT-Sicherheitsrecht (Fn. 19), Rn. 416 ff.; zum Gesetzesentwurf siehe *Deusch/Eggendorfer*, K&R 2024, 169, 175.

37 BGBl. 2024 I Nr. 438 vom 27. 12. 2024.

38 EU-Wertpapieraufsichtsbehörde (European Securities and Markets Authority – ESMA), die EU-Bankenaufsichtsbehörde (European Banking Authority – EBA) und die EU-Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (European Insurance and Occupational Pensions Authority – EIOPA).

39 Zum DORA-Rechtsrahmen mit Durchführungsverordnungen und Leitlinien siehe die BaFin-Webseite (https://ruw.link/2026/87 (bafin.de)), dort auch die Rubrik „Für wen gelten die BAIT seit 17. 1. 2025 noch?"; zum Verhältnis DORA und nationales Recht *Merwald*, RDi 2024, 590, 501 und *Ilg*, WPg 2025, 1076 ff.

40 *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 2), Rn. 395 ff.

41 Zu den „AVB Cyber" (Stand Februar 2024): https://ruw.link/2026/88 (gdv.de).

42 LG Hagen, 15. 10. 2024 – 9 O 258/23, K&R 2025, 276 ff.

43 OLG Schleswig-Holstein, 14. 10. 2024 – 16 U 63/24, K&R 2025, 195 ff. = ITRB 2025, 93 f.

44 Art. 3 Nr. 15 des Kommissionsvorschlags COM(2025) 837 final vom 19. 11. 2025 („Digital-Omnibus-Verordnung").

2. Gerichtsentscheidungen

Streit um die Versendung von Rechnungen per E-Mail entbrannte anhand von Fällen, in denen Empfänger Rechnungen mit gefälschten Bankdaten erhalten haben. Das OLG Schleswig-Holstein und die Verfasser sind der Auffassung, dass der Rechnungsabsender gemäß Art. 32 DSGVO verpflichtet ist, die Rechnung per Ende-zu-Ende-Verschlüsselung zu versenden bzw. dies dem Empfänger zumindest anzubieten. Allerdings kritisieren die Verfasser in technischer Hinsicht, dass das OLG Schleswig-Holstein die Sicherheitsziele Integrität und Authentizität auf der einen Seite und Vertraulichkeit auf der anderen sowie die jeweiligen Maßnahmen nicht technisch korrekt getrennt hat.[45]

Die Fallkonstellation des OLG Schleswig-Holstein (Überweisung des Opfers infolge einer Fälschung der Rechnung) ist zu trennen von Überweisungen, die nicht das Opfer, sondern ein Täter vorgenommen hat, nachdem er sich z. B. infolge von „Phishing-Kampagnen" die Zugangsdaten (PIN/TAN) verschafft hat. In den letztgenannten Fällen der „nicht autorisierten" Zahlungen lehnten die Banken eine Erstattung ab, da sie gegen das Opfer aufgrund grob fahrlässiger Preisgabe der Zugangsdaten Schadensersatz in entsprechender Höhe für sich reklamierten. Die Schlussanträge des Generalanwalts Athanasios Rantos vom 5. 3. 2026 in der Rechtssache C-70/25 jedoch wenden sich gegen diese Aufrechnung des Erstattungsanspruchs gemäß den Art. 73, 74 RL (EU) 2015/2366 mit einem Schadensersatzanspruch. Dies hat zur Folge, dass die Bank die Erstattung zunächst zu leisten und sodann den Schadensersatzanspruch gesondert geltend machen und auch nachweisen muss.[46]

X. IT-Sicherheit in der KI-VO

Am 19. 11. 2025 hat die EU-Kommission neben der „Digital-Omnibus-Verordnung" eine „Digital-Omnibus-Verordnung zur KI" vorgeschlagen. Unter anderem soll die Pflicht der Anbieter und Betreiber zur KI-Kompetenz gemäß Art. 4 KI-VO durch die Pflicht der Mitgliedstaaten ersetzt werden, die betreffenden Stellen zur Bildung von KI-Kompetenz „zu ermutigen". Außerdem sind Erleichterungen für kleine und mittelständische Unternehmen geplant – auch in dem für die IT-Sicherheit relevanten Hochrisiko-Bereich. Überdies sollen die Pflichten für Hochrisiko-KI-Systeme, die keiner zusätzlichen Produktregulierung nach Maßgabe des Anhang I unterliegen, erst dann Anwendung finden, wenn – von der Kommission gebilligte – angemessene Maßnahmen verfügbar sind, um die Unternehmen bei der Einhaltung dieser Pflichten zu unterstützen.[47]

Mit dem Regierungsentwurf zum „Gesetz zur Durchführung der Verordnung über künstliche Intelligenz" vom 10. 2. 2026[48] ist geplant, die Bundesnetzagentur zur KI-Marktüberwachungsbehörde zu machen. Laut § 10 des Entwurfs soll das BSI die Aufgaben der Marktüberwachungsbehörde nach dem Cyber Resilience Act (CRA – VO (EU) 2024/2847, siehe unten Abschnitt XI) übernehmen und an der Entwicklung von Leitlinien, europäisch harmonisierten Normen und Spezifikationen zur Cybersicherheit mitarbeiten.

XI. Cyber Resilience Act

Der Cyber Resilience Act[49] schreibt für Hersteller, Händler und Einführer ab dem 11. 12. 2027 (Art. 71 CRA) grundlegende Cybersicherheitsanforderungen an alle Produkte mit digitalen Elementen vor (Art. 6 CRA). Die EU-Kommission ist befugt, höhere Anforderungen an wichtige Produkte mit digitalen Elementen (Art. 7 i. V. m. Anlage III CRA) und spezielle Anforderungen an wichtige und kritische Produkte mit digitalen Elementen per Durchführungsverordnung vorzugeben (Art. 7, 8 i. V. m. Anhängen III und IV CRA). Der Entwurf für den Vorschlag einer solchen Durchführungsverordnung ist bereits veröffentlicht.[50]

Außerhalb von EU-Durchführungsrechtsakten können technische Normen und Standards, soweit geeignet, zur Konkretisierung der Sicherheitsvorgaben herangezogen werden. Dazu hat die ENISA in dem „Cyber Resilience Act Requirements Standards Mapping" die derzeit einschlägigen Standards zusammengetragen.[51]

Zudem hat die EU-Kommission mit ihrem Durchführungsbeschluss vom 3. 2. 2025 (C(2025) 618 final) das Europäische Komitee für Normung (CEN), das Europäische Komitee für elektrotechnische Normung (CENELEC) und das Europäische Institut für Telekommunikationsnormen (ETSI) damit beauftragt, neue europäische Normen auszuarbeiten, die für die IT-Sicherheitsanforderungen an Produkte mit digitalen Elementen gemäß dem Cyber Resilience Act gelten sollen. Mit Spannung darf z. B. erwartet werden, welche Anforderungen die beauftragten Stellen gemäß Anhang I des Durchführungsbeschlusses an die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen mit einem „angemessenen Maß an Cybersicherheit" stellen werden (bis 30. 8. 2026) und welche Maßstäbe dafür gelten sollen, dass ein Produkt „ohne bekannte ausnutzbare Schwachstellen" ist (bis 30. 10. 2027).

XII. Maschinenverordnung

Erinnert sei an die Ablösung der bisherigen Maschinenrichtlinie (2006/42/EG) durch die Maschinenverordnung (VO (EU) 2023/1230) mit den spezifischeren IT-Sicherheitsvorgaben zum 14. 1. 2027.[52]

XIII. Produkthaftungsgesetz und EU-Vorgaben; Produktsicherheitsverordnung

Die Produkthaftungsrichtlinie (PHRL – RL (EU) 2024/2853) gilt für alle Produkte, die nach dem 9. 12. 2026 in Betrieb genommen werden (Art. 2 Abs. 1 PHRL). Art. 4 Nr. 1 bezieht Software (Ausnahme: „nicht kommerzielle Open Source Software") ausdrücklich mit ein und beseitigt diesen Streitpunkt aus der Vorgängerregelung. Die PHRL sieht anders als die bisherige Regelung keine Haftungsgrenzen vor; die adressierten Wirtschaftsakteure sind daher gut beraten, ihre derzeitigen Versicherungspolicen zu prüfen.[53] Aus Sicht der IT-Sicherheit

45 Für eine Ende-zu-Ende-Verschlüsselung: OLG Schleswig-Holstein, 18. 12. 2024 – 12 U 9/24, K&R 2025, 272 ff.; *Deusch/Eggendorfer*, K&R 2025, 221 - 226; *dies.*, MMR 2025, 858 ff., LG Koblenz, 28. 4. 2022 – 6 U 39/21, K&R 2022, 628 ff.; dagegen OLG Karlsruhe, 27. 7. 2023 – 19 U 83/22, K&R 2023, 607 ff. (allerdings außerhalb der DSGVO), OVG NRW, 20. 2. 2025 – 16 B 288/23, K&R 2025, 358 ff.

46 https://ruw.link/2026/89 (infocuria.curia.europa.eu).

47 COM(2025) 836 final, dazu bereits die Stellungnahme des Europäischen Datenschutz-Ausschusses: https://www.edpb.europa.eu/system/files/2026-01/edpb_edps_jointopinion_202601_proposal_ai-omnibus_en.pdf sowie *Kaufmann*, K&R 2026, 78 - 82 und zur Änderung des Art. 4 KI-VO *Deusch/Eggendorfer*, KI-Kompetenz von Sicherheitsbehörden nach dem AI-Act (FN 6).

48 https://ruw.link/2026/90 (bmds.bund.de).

49 Dazu generell *Wiebe/Daelen/Kerger*, K&R 2025, 79 - 86 sowie *Heckmann/Ziegler*, ITRB 2024, 159 - 161 zu den Auswirkungen auf Open Source Software, KI-VO und BGB.

50 Ref. Ares(2025)2037850 – 13/03/2025 (https://ruw.link/2026/91 (ec.europa.eu)).

51 https://ruw.link/2026/92 (enisa.europa.eu).

52 Dazu bereits *Deusch/Eggendorfer*, K&R 2024, 169, 172.

53 *Borges*, CR 2025, 1 - 15.

besonders relevant kann Art. 7 Abs. 1 lit. f PHRL werden, der die Fehlerfreiheit ausdrücklich zum Bestandteil der Cybersicherheit macht. Es bleibt abzuwarten, ob damit Programmierungsfehler und sonstige Sicherheitslücken in Softwareprodukten tatsächlich reduziert werden. Die Bundesregierung hat den Gesetzesentwurf zur Umsetzung der EU-Richtlinie am 17. 12. 2025 beschlossen und dem Bundestag am 21. 2. 2026 überwiesen.[54]

Mit Blick auf die Marktüberwachung definiert die Produktsicherheitsverordnung (VO (EU) 2023/988) Sicherheitsanforderungen an alle Verbraucherprodukte, die in der EU auf dem Markt bereitgestellt werden, einschließlich Software.[55]

XIV. IT-Sicherheit, Aktualisierung, Recht auf Reparatur und Sachmangel

Spannende Rechtsfragen wirft die Fallkonstellation auf, in der der Hersteller eines Batteriespeichers einer Photovoltaikanlage durch ein „Sicherheitsupdate" die Speicherkapazität um 30 % reduziert hat. Der Hersteller will damit seine Pflicht zur Aktualisierung gemäß den §§ 327f, 475b BGB erfüllt haben. Das LG Rostock bescheinigte ihm dagegen einen Sachmangel, weil der Speicher nunmehr die vereinbarte Kapazität nicht mehr leiste. Andere Gerichte lehnen einen Sachmangel ab, weil keine bestimmte Kapazität geschuldet sei, sondern lediglich, keine „nennenswerte Kapazitätsverluste".[56]

Die Frage, ob Funktionsbeeinträchtigungen infolge von Sicherheitsupdates hinzunehmen sind, könnte sich auch in anderen Konstellationen für Softwareanwendungen stellen und ebenso, wenn der Verkäufer einer Sache das von der EU beschlossene Recht des Verbrauchers auf Reparatur zu erfüllen hat.[57]

XV. Zusammenfassung

Im Berichtszeitraum erweist sich das IT-Sicherheitsrecht erneut als hoch volatil. Wer „up to date" bleiben will, kommt nicht umhin, die weitere Entwicklung insbesondere zur EU-Rechtssetzung zu verfolgen.

Dr. Florian Deusch
ist Rechtsanwalt und Fachanwalt für Informationstechnologierecht in der Anwaltskanzlei Dr. Gretter in Ravensburg. Er ist zudem als Datenschutzbeauftragter tätig.

Prof. Dr. Tobias Eggendorfer
ist Professor für Sicherheit in verteilten Anwendungen an der TH Ingolstadt, davor war er als Abteilungsleiter „Sichere Systeme" an der Agentur für Innovation in der Cybersicherheit für die Weiterentwicklung der Forschung im Bereich der IT-Sicherheit zuständig. Er ist zudem als IT-Berater und Datenschutzbeauftragter tätig.

54 BT-Drs. 21/4297; zum Referentenentwurf und den Stellungnahmen dazu siehe die Webseite des BMJ https://ruw.link/2026/93 (bmjv.de); zum Referentenentwurf *Müller/Röper*, GmbHR 2025, 380 - 383.

55 *Voigt*, IT-Sicherheitsrecht (Fn. 19), Kap. H Rn. 656; zum bisherigen Streitstand der Produkthaftung für Software *Taeger*, in: Ehring/Taeger, Produkthaftungs- und Produktsicherheitsrecht, 2022, § 2 ProdHG Rn. 18 - 38.

56 *Ferner*, jurisPR-ITR 2/2026 Anm. 6 zu LG Rostock, 18. 12. 2024 – 2 O 316/24 und OLG München, 2. 7. 2025 – 28 U 1077/25 Bau e, und OLG Stuttgart, 28. 10. 2025 – 6 U 33/25.

57 Zum Referentenentwurf des Bundesjustizministeriums: https://ruw.link/2026/94 (bmjv.de), dort relevant insbesondere die §§ 434 Abs. 3 und 479 ff. BGB.

Hinweis der Redaktion:
Vgl. auch der Beitrag von *Koch*, Nach der Umsetzung der NIS-2-Richtlinie ist vor der Reform der NIS-2-Richtlinie, K&R 2026, 293 ff. (in diesem Heft).

RA Dr. Thomas Sassenberg, LL.M., VRiLG Dr. iur. Dipl.-Inf. Reto Mantz und RA Dr. Gerd Kirparski, MBA*

Entwicklungen im zivilrechtlichen Telekommunikationsrecht im Jahr 2025

Vertragslaufzeit stand im Fokus

Kurz und Knapp

Das 13. Update zum zivilrechtlichen Telekommunikationsrecht umfasst den Veröffentlichungszeitraum April 2025 bis einschließlich März 2026 und schließt an den Überblick über das zivilrechtliche Telekommunikationsrecht aus dem letzten Jahr (K&R 2025, 384 ff.) an. Neben der Rechtsprechung der Bewerbung von TK-Diensten war weiter die maximale Vertragsdauer bei Verträgen von zentraler Bedeutung. Gesetzgeberisch sind das TKG-Änderungsgesetz und der Digital Networks Act hervorzuheben.

I. TK-Anbieter und Endkunde

1. Bewerbung von TK-Produkten

a) Werbeaussagen

Das LG Koblenz[1] hatte über einen Sachverhalt zu entscheiden, bei dem das beklagte TK-Unternehmen Verträge für Glasfaser-

* Mehr über die Autoren erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 2. 4. 2026.

1 LG Koblenz, 16. 9. 2025 – 3 HK O 69/24, GRUR-RS 2025, 27588.