Das neue Digitalrecht der Europäischen Union

Übersicht zu den neuen EU-Vorgaben im Digitalbereich mit Fokus auf die praktische Umsetzung im Unternehmen

Dr. Hans Markus Wulf
Rechtsanwalt & Partner bei HEUKING
Fachanwalt für IT-Recht
ISO/IEC 27001 Auditor (TÜV)
CIPP/E | Datenschutzauditor (TÜV)
m.wulf@heuking.de

Stand: Juni 2024

In den letzten Jahren hat die Europäische Union eine Reihe legislativer Initiativen ergriffen, um den Herausforderungen der Digitalisierung zu begegnen, insbesondere in den Bereichen Cybersicherheit und Produktsicherheit sowie im Hinblick auf neue datengestützte Geschäftsmodelle. Viele Unternehmen sehen sich infolgedessen erstmals seit der Datenschutz-Grundverordnung mit vielfältigen und unerwarteten Anforderungen konfrontiert. Dieser Beitrag zielt darauf ab, Unternehmen für die neuen Pflichten zu sensibilisieren und einen Überblick über die notwendigen Umsetzungsmaßnahmen zu geben, die nahezu jedes Unternehmen betreffen werden.

Künstliche Intelligenz

1. AI Act

Nach dem erfolgreichen Abschluss der Trilog-Verhandlungen zum Artificial Intelligence Act (AI Act) erfolgte dessen förmliche Annahme im Mai 2024. Er tritt 20 Tage nach Veröffentlichung im Amtsblatt in Kraft. Parallel dazu hat der Europarat im selben Monat einen internationalen KI-Vertrag zur Festlegung globaler KI-Mindeststandards verabschiedet.

Der AI Act definiert KI sinngemäß als ein maschinengestütztes, autonomes und anpassungsfähiges System, das aus den erhaltenen Eingaben ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können. Der AI-Act verbietet aufgrund des hohen Risikos bestimmte KI-Systeme vollständig (Art. 5 AI Act), etwa solche zur unterschwelligen Verhaltensmanipulation oder zum ungezielten Auslesen von Gesichtsbildern aus dem Internet. Hochrisiko-KI-Systeme nach Art. 6 AI Act sind dagegen zwar zulässig, unterliegen allerdings hohen, regulativen Anforderungen. Hochrisiko-KI ist etwa eine solche zur biometrischen Fernidentifikation, zur Strafverfolgung oder zur Steuerung von Migration.

Besonders praxisrelevant für Unternehmen dürften allerdings die Bereiche **Bildung** und **Beschäftigung** sein, denn diese werden ebenfalls als Hochrisiko-Sektoren eingestuft, so dass bereits der Einsatz von KI im Rahmen von HR-Bewerbungsverfahren einen hohen Umsetzungsaufwand auslöst.

Anbieter, die Hochrisiko-KI im eigenen Namen in Verkehr bringen, müssen umfassende Dokumentationspflichten erfüllen, einschließlich der Einführung von Risikomanagementsystemen und Qualitätsmanagementprozessen. Weitere Pflichten umfassen die Bereitstellung von Gebrauchsanweisungen, transparente Nutzerinformationen, KI-Konformitätsbewertungsverfahren und CE-Kennzeichnung. Darüber hinaus müssen Anbieter, Nutzer und Händler Meldeprozesse installieren.

Importeure und Händler von Hochrisiko-KI müssen insbesondere die CE-Kennzeichnung, die EU-Konformitätserklärung und das Vorhandensein der Gebrauchsanweisung überprüfen. Importeure müssen zusätzlich ihre eigenen Kontaktdaten angeben.

Nutzer von Hochrisiko-KI müssen nach Art. 26 AI Act neben angemessenen technischen sowie organisatorischen Maßnahmen interne Prozesse für die **menschliche Überwachung** und die Nutzung gemäß der Zweckbestimmung des Herstellers sowie der Gebrauchsanweisung etablieren und dokumentieren, ihre Mitarbeiter über die Hochrisiko-KI informieren und eine **Datenschutz-Folgenabschätzung** durchführen. Für allgemeine KI müssen Nutzer lediglich Transparenzpflichten bei biometrischer Kategorisierung, Emotionserkennung oder Deepfakes beachten, während Hersteller stets Transparenz- und Informationspflichten unterliegen.

Anbieter von General Purpose AI (GPAI) müssen zusätzliche Informationspflichten bezüglich der verwendeten Trainingsdaten sowie für GPAI-Nutzer umsetzen, technische Dokumentationen bereithalten und das EU-Urheberrecht beachten. KI-Modelle mit „systemischem“ Risiko – insbesondere solche, die mit sehr hoher Rechenleistung trainiert wurden (wie ChatGPT) – unterliegen zudem Melde- und weiteren Risikominderungspflichten.

2. KI-Haftungsrichtlinie

Die Europäische Union hat ferner den Entwurf einer KI-Haftungsrichtlinie vorgelegt, welche die nationalen Haftungsvorschriften für künstliche Intelligenz harmonisieren soll. Diese könnte neben das bestehende Deliktsrecht und die in Kürze erwartete neue Produkthaftungsrichtlinie treten.

Sollte die Union am aktuellen Entwurf festhalten, könnten Anbieter und Nutzer von KI künftig gerichtlich zur Offenlegung von Beweismitteln verpflichtet werden, sofern ein Anspruchsteller (natürliche oder juristische Personen) einen außervertraglichen, verschuldensabhängigen Schadensersatzanspruch plausibel darlegt. Gemäß Art. 3 Abs. 5 des Entwurfs droht bei Nichtbefolgung die Vermutung eines Sorgfaltspflichtverstoßes. Führt ein Geschädigter den Nachweis, dass ein von der KI erzeugtes Ergebnis den Schaden verursacht hat, wird eine Kausalität der Sorgfaltspflichtverletzung vermutet. Der Beklagte könnte diese Vermutung entkräften, indem er nachweist, dass der Kläger Zugang zu

anderen Beweismitteln und Fachkenntnissen hat. Für die rein private Nutzung von KI sollen Ausnahmen gelten.

Auch wenn eine endgültige Entscheidung der Union zur KI-Haftung noch aussteht, ist zur Vermeidung von Regressansprüchen jedenfalls eine gründliche Dokumentation des KI-Einsatzes sowie der im AI Act vorgesehenen Sorgfaltspflichten unerlässlich.

Online-Dienste

Eine Vielzahl der neuen Verordnungen richtet sich an die Anbieter von Online-Diensten, also etwa solche, die ihren Nutzern Zugang zu einer Webplattform gewähren (z.B. Händlerportal). Obwohl der Anwendungsbereich häufig ähnliche Formulierungen aufweist – insbesondere bei Vermittlungs- und Online-Diensten – bestehen teils erhebliche Unterschiede, die eine klare Abgrenzung erschweren können.

3. Digital Services Act

Der Digital Services Act (DSA) wird durch die 2019 in Kraft tretende P2B-Verordnung und das im Mai 2024 verabschiedete deutsche Umsetzungsgesetz, das „Digitale Dienste Gesetz“ (DDG), ergänzt.

Gemäß Art. 3 lit. g DSA gilt der DSA zunächst für alle **Vermittlungsdienste**, die reine Durchleitungs-, Caching- oder Hosting-Dienste anbieten. Erfasst sind alle Plattformen, auf denen Nutzer selbst Inhalte hochladen oder mit anderen Nutzern interagieren können und Internet Service Provider, z.B. Social Media, Foren, Cloud- und Hosting-Anbieter sowie in der Regel Software-as-a-Service (SaaS). Letztere sind jedoch ausgenommen, wenn die Datenspeicherung nur eine untergeordnete Funktion darstellt.

Zusätzliche Pflichten ergeben sich für **Online-Plattformen** nach Art. 3 lit. i DSA, die „user-generated content“ öffentlich verbreiten, darunter Social Media, Bewertungsportale, App-Stores und Online-Marktplätze. SaaS-Anbieter sind hierbei betroffen, wenn sie nutzergenerierte Inhalte einer unbegrenzten Anzahl von Personen zugänglich machen.

Intermediäre müssen seit Februar 2024 die organisatorischen und rechtlichen Pflichten nach Art. 11-15 DSA sowie alle weiteren Pflichten des DSA erfüllen. Es ist eine Kontaktstelle für Behörden und Nutzer zu benennen, Nutzungsbedingungen sind zu überarbeiten und jährliche Transparenzberichte müssen veröffentlicht werden. Ausgenommen sind Klein- und Kleinstunternehmen.

Hosting-Dienste (insbesondere Cloud-Dienste) und Online-Plattformen müssen zudem ein „Notice and Takedown“-Verfahren für rechtswidrige Inhalte einrichten (vgl. Erwägungsgrund 22 der DSA). Darüber hinaus sind sie verpflichtet, rechtswidrige Inhalte auf behördliche oder gerichtliche Anordnung zu sperren.

Für Online-Plattformen werden zusätzliche Maßnahmen vorgeschrieben, darunter ein Beschwerde- und Abhilfemechanismus zur Anfechtung von Entscheidungen über illegale Inhalte, Transparenzpflichten bei Empfehlungssystemen, Inhaltsmoderation und Online-

Werbung sowie erweiterte Transparenzberichtspflichten. Sie müssen bestimmte Nutzer sperren und Dark Patterns und an Kinder gerichtete Werbung unterbinden. Nutzungsbeschränkungen müssen begründet und die Begründungen in einer Transparenzdatenbank veröffentlicht werden.

B2C-Online-Marktplätze, die keine Kleinst- oder Kleinunternehmen sind, müssen zudem die Identität gewerblicher Nutzer durch die Erhebung von Kontaktdaten überprüfen und Verbraucherinformationen bereitstellen. Für sehr große Online-Plattformen und Suchmaschinen wie Alibaba, Amazon, Google oder Facebook gelten gemäß Art. 33-43 DSA weitergehende Pflichten.

4. DDG

Das DDG ist seit Mai 2024 in Kraft und ersetzt das bisherige NetzDG sowie Teile des Telemediengesetzes. Es soll unter anderem die Zuständigkeit der deutschen Behörden zur Umsetzung des DSA, primär der Bundesnetzagentur, regeln.

Des Weiteren distanziert sich das DDG von den rigiden Fristen des NetzDG für die Löschung illegaler Inhalte. Stattdessen sollen Diensteanbieter „zeitnah, sorgfältig, frei von Willkür und objektiv“ über die Meldung entscheiden. Darüber hinaus sieht das DDG bei Verstößen gegen den DSA Bußgelder von bis zu 6 % des Jahresumsatzes vor.

5. P2B-Verordnung

Die P2B-Verordnung richtet sich an Online-Vermittlungsdienste. Gemäß Art. 2 Nr. 2 P2B sind dies jedoch ausschließlich Dienste der Informationsgesellschaft, die Transaktionen zwischen gewerblichen Nutzern und Verbrauchern in der EU vermitteln (B2C).

Seit dem 12.07.2020 sind etwa Online-Marktplätze, auf denen auch gewerbliche Nutzer aktiv sind, dazu verpflichtet, in ihren B2B-AGB die Informationspflichten neu zu regeln. Die Umsetzung der Artikel 3, 5-10 und 12 der P2B-Verordnung, welche über das strenge deutsche AGB-Recht hinausgehen, beinhaltet beispielsweise die Offenlegung von Ranking-Kriterien. Einige Offenlegungspflichten gelten auch für Suchmaschinen-Anbieter. Zudem müssen Online-Vermittlungsdienste sicherstellen, dass vor einer Beschränkung oder Beendigung ihres Dienstes gegenüber einzelnen gewerblichen Nutzern das Verfahren nach Art. 4 P2B durchlaufen wird. Dieses sieht eine rechtzeitige Begründung und Information des betroffenen Nutzers vor. Des Weiteren ist die Einrichtung eines Beschwerdemanagementsystems für gewerbliche Nutzer gemäß Art. 11 P2B sowie die Benennung von Mediatoren zur außergerichtlichen Streitbeilegung gemäß Art. 12 P2B erforderlich.

6. E-Evidence Verordnung

Die E-Evidence-Verordnung (EEV) zur Europäischen Herausgabeanordnung (EPOC) und zur Europäischen Sicherungsanordnung (EPOC-PR) betrifft alle Diensteanbieter, **die elektronische Kommunikationsdienste**, Internetdomänennamen und IP-Nummern

anbieten. Die Verordnung gilt für Nummerierungsdienste sowie Dienste der Informationsgesellschaft mit Kommunikations- oder (nicht nur untergeordneter) Datenspeicher- oder Datenverarbeitungsfunktion, die in der EU angeboten werden, Art. 2 Abs. 1, 3 Nr. 3 EEV. Dies umfasst Cloud- und SaaS-Anbieter, Foren, Online-Marktplätze mit Kommunikationsfunktion, Messenger- und E-Mail-Dienste, Soziale Medien, Plattformen für Online-Spiele und zahlreiche weitere Akteure.

Grundsätzlich sind diese lediglich verpflichtet zu handeln, wenn sie durch eine Anfrage (EPOC oder EPOC-PR) der Strafverfolgungsbehörde eines anderen EU-Mitgliedstaates zur Herausgabe oder Sicherung elektronischer Beweismittel, also digitaler Daten für die Ermittlung und Verfolgung von Straftaten, verpflichtet werden. Dabei sind jedoch enge Fristen einzuhalten: Die Sicherung muss unverzüglich erfolgen und Herausgabeanordnungen sind in der Regel innerhalb von zehn Tagen, in Notfällen innerhalb von **acht Stunden** zu bearbeiten (Art. 10 EEV).

Die Vielzahl der betroffenen Unternehmen sollte daher bis zum Ende der Umsetzungsfrist am 08.08.2026 in der Lage sein, die Daten in kurzer Zeit zu sichern, die Anfrage auf rechtliche und tatsächliche Unmöglichkeit zu überprüfen, ggf. mit der nationalen Behörde zu kommunizieren und die angeforderten Daten vollständig herauszugeben. Unternehmen sollten bereits jetzt Zuständigkeiten festlegen und Prozesse für die rechtliche Prüfung und Umsetzung von EPOC und EPOC-PR unter Berücksichtigung der Bearbeitungsfristen definieren. Des Weiteren ist es erforderlich, technische Maßnahmen zur kurzzeitigen Datensicherung und -herausgabe sowie zur Wahrung der Vertraulichkeit, Geheimhaltung und Integrität der Anordnungen und Daten gemäß Art. 13 Abs. 4 EEV zu ergreifen.

Parallel dazu führen die EU und die USA Verhandlungen, um den internationalen Zugang zu Beweismitteln zu erleichtern.

7. Warenkaufrichtlinie & Richtlinie über digitale Inhalte und Dienste

Die Schuld- und Kaufrechtsreform, welche Anfang 2022 in Kraft getreten ist, hat zu bedeutenden Änderungen im BGB geführt. Insbesondere die §§ 327 ff. und §§ 475a ff. wurden im Zuge dessen novelliert. Die Änderungen sind auf die Warenkaufrichtlinie (WKRL) und die Richtlinie über Digitale Inhalte und Dienste (DID) zurückzuführen. Die Richtlinien wurden erfahrungsgemäß bislang von vielen Unternehmen entweder nicht oder zumindest ungenügend umgesetzt.

Die Änderungen betreffen Unternehmen, die Verbrauchern digitale Inhalte oder Dienstleistungen wie Software-Downloads, Apps, Videodateien, SaaS oder Social-Media-Dienste anbieten sowie Verkäufer (physischer) Waren mit digitalen Elementen wie vernetzten Haushaltsgeräten oder Smartphones. Die Unternehmen sind verpflichtet, die vertragsgemäße Beschaffenheit und Sicherheit ihrer Produkte während der gesamten Bereitstellungs- oder erwarteten Nutzungsdauer durch Updates sicherzustellen. Dies erfolgt in der Regel mindestens zwei Jahre lang (§§ 327f, 475b BGB). Zudem müssen sie die Sache für diesen Zeitraum mangelfrei halten. Dies erfordert technische Maßnahmen sowie die Festlegung der Beschaffenheit und Updatezeiträume in Verträgen oder AGB. Des

Weiteren ist die Updatepflicht von Lieferanten digitaler Elemente durch entsprechende Vertragsgestaltung zu sichern.

DID-Anbieter sind verpflichtet, ihre Leistungen unverzüglich nach Vertragsschluss in der neuesten Version bereitzustellen und Übereinstimmung mit der Testversion zu garantieren. Leistungsänderungen sind bei dauerhaft bereitgestellten Diensten nur eingeschränkt möglich. Technisch ist insbesondere die Integration eines „Kündigungsbuttons“ bei Dauerschuldverhältnissen erforderlich (§ 312k Abs. 2 BGB)

8. Richtlinie über Finanzdienstleistungen im Fernabsatz

Die Distance Financial Services Directive (DMFSD) zielt darauf ab, den Verbraucherschutz bei Fernabsatzverträgen über Finanzdienstleistungen wie Bankkonten, Versicherungen oder Altersvorsorgeverträge zu stärken, sofern diese beispielsweise über Websites, Apps, Telefon oder Messenger abgeschlossen werden.

Besondere Aufmerksamkeit gilt dem elektronischen Vertragsabschluss via Website oder Applikation, bei dem ein Widerruf über einen entsprechenden Button möglich sein muss (beispielsweise ein zweistufig gestalteter Widerruf-Button). Dark Patterns sind verboten, und bei der Nutzung von Chatbots oder Robo-Advice muss eine Option zur Einschaltung einer natürlichen Person bestehen. Plattformbetreiber, die den Abschluss solcher Verträge ermöglichen, müssen ebenfalls einen Widerruf-Button bereitstellen.

Die Rechtsabteilung muss spätestens nach Inkrafttreten der Umsetzungsgesetze (bis zum 19.12.2025) tätig werden und die neuen vorvertraglichen Informations- und Erläuterungspflichten, die auch bei der telefonischen Kontaktaufnahme gelten, bis zum 19.06.2026 umsetzen.

Datenrecht

Mit dem Data Act und dem Data Governance Act (DGA) hat die EU einen Rechtsrahmen geschaffen, um den Zugang zu Daten zu vereinfachen und datenbezogene Innovationen zu fördern.

9. Data Act

Der Data Act richtet sich primär an Hersteller vernetzter Produkte, Anbieter verbundener Dienste sowie Datenverarbeitungsdienste, wobei Ausnahmen für Kleinst- und kleine Unternehmen gelten. Obwohl er erst ab dem 11.09.2025 gilt, sehen sich viele Unternehmen bereits jetzt mit vielfältigen technischen Anforderungen an die Entwicklung vernetzter Produkte und verbundener Dienste konfrontiert, die einen Handlungsbedarf begründen. Zu den betroffenen Produkten zählen beispielsweise Smart Watches oder vernetzte Fahrzeuge, aber auch industrielle Maschinen sowie Dienste, die mit diesen Produkten verbunden sind, sodass deren Funktionen ohne sie nicht ausgeführt werden können.

Die von diesen Produkten erzeugten Daten müssen den Nutzern – sowohl Verbrauchern als auch Unternehmen – direkt von dem Produkt oder zumindest in Echtzeit, kostenlos und ggf. kontinuierlich zur Verfügung gestellt werden. Des Weiteren sind Texte zu erstellen, welche die vertraglichen und vorvertraglichen **Informationspflichten** (beispielsweise zur Datenportabilität) sowie die Verträge zur eigenen Datennutzung umfassen. Zudem sind rechtskonforme und diskriminierungsfreie **Verträge mit B2B-Datenempfängern** zu verfassen.

Datenverarbeitungsdienste wie Cloud- und SaaS-Anbieter sind dazu verpflichtet, technische Vorgaben, insbesondere zur **Interoperabilität**, einzuhalten und den nahtlosen Wechsel zu anderen Anbietern mit kurzen Kündigungs- und Vorlauffristen zu unterstützen. Dieser Datenzugang eröffnet auch anderen Unternehmen die Möglichkeit, **neue datenbasierte Geschäftsmodelle** zu entwickeln. Allerdings bestehen Datenschutzbedenken, da die Daten oft sensible Bereiche betreffen.

Darüber hinaus sind betroffene Unternehmen in außergewöhnlichen Umständen, wie beispielsweise öffentlichen Notfällen oder Naturkatastrophen, dazu verpflichtet, Daten auf Anforderung unverzüglich an öffentliche Stellen herauszugeben.

10. Data Governance Act

Der DGA ergänzt den Data Act und richtet sich an **Datenvermittlungsdienste**, welche geschäftliche Beziehungen zwischen Dateninhabern und Datennutzern herstellen („Data Broker“, Datenmarktplätze). Zudem sollen die Vorschriften für öffentliche Stellen und die Einführung sogenannter **Datenaltruismus-Dienste** den Zugang zu öffentlichen Daten vereinfachen.

Datenvermittlungsdienste sind dazu verpflichtet, interne Richtlinien und Prozesse zu etablieren, um die eigene Nutzung der vermittelten Daten zu verhindern und ihre Nutzer fair, transparent und nichtdiskriminierend zu behandeln. Dies gilt auch bei der Erstellung von AGB. Zudem müssen sie technische Maßnahmen ergreifen, um Interoperabilität und einen kontinuierlichen Echtzeitzugang zu gewährleisten.

Anbieter von Datenvermittlungsdiensten, welche Daten von allgemeinem Interesse erheben, um Datenanalysen und maschinelles Lernen zu ermöglichen, sind insbesondere dazu verpflichtet, Transparenz- und Aufklärungspflichten zu erfüllen und einen jährlichen Tätigkeitsbericht zu erstellen, sofern sie im entsprechenden nationalen Register eingetragen sind. Der DGA gilt seit dem 24.09.2023. Für Anbieter, die bereits vor dem Inkrafttreten Datenvermittlungsdienste erbracht haben, gilt die Umsetzungspflicht jedoch erst ab dem 24.09.2025.

Informationssicherheit

11. NIS-2-Richtlinie und das deutsche Umsetzungsgesetz, KRITIS-Dachgesetz und CER-Richtlinie

Die NIS-2-Richtlinie sowie das geplante deutsche Umsetzungsgesetz (NIS2UmsuCG-E) zielen darauf ab, die Cybersicherheit in kritischen Sektoren zu stärken. Dies soll insbesondere durch eine Ausweitung des Anwendungsbereichs gegenüber der NIS-Richtlinie auf „wesentliche“ und „**wichtige Einrichtungen**“ erreicht werden (vgl. besonders wichtige und wichtige Einrichtungen gem. § 28 BSIG-E). Dadurch sind zahlreiche Unternehmen erstmals betroffen (in Deutschland ca. 30.000). Verantwortlich für die Umsetzung, Billigung und Überwachung ist nun erstmals auch die **Geschäftsleitung** (§ 38 BSIG-E). In diesem Kontext ist zudem das KRITIS-Dachgesetz zu nennen, welches die Implementierung der CER-Richtlinie zum Ziel hat und somit die physische Sicherheit kritischer Anlagen verbessern soll.

Die Definition der wesentlichen Einrichtungen umfasst Unternehmen in den Bereichen Energie, Bankwesen, Finanzmarktinfrastruktur, Gesundheitswesen, digitale Infrastruktur (inklusive Cloud-Computing) und weitere, sofern es sich nicht um kleine und mittlere Unternehmen (KMU) handelt. Die in Anhang I und II der Richtlinie definierten wichtigen Einrichtungen umfassen zusätzlich Anbieter digitaler Dienste, Post- und Kurierdienste sowie Unternehmen aus der **Chemie- und Lebensmittelbranche** und auch bestimmte **Maschinenbauunternehmen**. Gemäß § 28 Abs. 2 BSIG-E muss es sich jedenfalls um mittlere Unternehmen handeln.

Betroffene Unternehmen sind bei fristgemäßer, nationaler Umsetzung verpflichtet, bis zum 17.10.2024 diverse interne Richtlinien und Prozesse zu entwerfen. Dazu zählen Konzepte zur Risikoanalyse und Sicherheit für Informationssysteme, zur Bewertung des Cybersicherheits-Risikomanagements sowie weitere **Sicherheitskonzepte**. Darüber hinaus können Vertragsanpassungen zur Gewährleistung der Sicherheit der Lieferkette erforderlich sein. Weitere Pflichten umfassen die technische Umsetzung von **Risikomanagementmaßnahmen**, die Übermittlung von Kontaktdaten sowie die Meldung von Sicherheitsvorfällen. Für grenzüberschreitend agierende Unternehmen besteht zudem die Verpflichtung, die unterschiedlichen Anforderungen nationaler Umsetzungsgesetze zu berücksichtigen.

12. Digital Operational Resilience Act

Der Digital Operational Resilience Act (DORA) verpflichtet Finanzunternehmen und ihre IKT-Dienstleister, bis zum 17.01.2025 sektorspezifische Vorgaben zur Cybersicherheit umzusetzen (IKT: Informations- und Kommunikationstechnologie). Verantwortlich zur Umsetzung sind nicht nur die Finanzunternehmen allein, sondern (wie bei der NIS-2) auch die **Geschäftsleitung** als Lenkungsorgan persönlich (Art. 5).

Die Vorgaben des DORA betreffen nahezu alle beaufsichtigten EU-Finanzinstitute und -Unternehmen, darunter Kreditinstitute, Zahlungsinstitute, Kontoinformationsdienstleister,

E-Geld-Institute, Versicherungsunternehmen und -Vermittler oder Einrichtungen der betrieblichen Altersversorgung (Art. 2 Abs. 1 lit. a-t DORA). Ausgenommen sind lediglich kleine und mittlere Unternehmen ohne Verflechtung mit größeren Unternehmen. DORA beinhaltet eine Vielzahl interner Richtlinien zu Governance und IKT-Risikomanagement. Darüber hinaus werden aus dem DORA und den ergänzenden **technischen Regulierungsstandards** (RTS) und Implementierungsstandards (ITS) technische Vorgaben an die digitale Betriebsstabilität abgeleitet, die über die gängigen ISO-Standards hinausgehen. Des Weiteren ist sicherzustellen, dass das Management von Risiken und IKT-Vorfällen durch die Überwachung der IKT-Drittanbieter gewährleistet wird.

Auch für den großen Kreis von Anbietern von **IKT-Dienstleistungen** an Finanzunternehmen ergeben sich neue Pflichten. Betroffen sind etwa Cloud- und Software-Anbieter, Rechenzentren, elektronische Kommunikationsdienste, Anbieter, die Zahlungen abwickeln oder Zahlungsinfrastruktur betreiben, sowie weitere datenbezogene Dienstleister, die ebenfalls interne Richtlinien und Prozesse sowie technische Vorkehrungen zum IKT-Risikomanagement umsetzen müssen. Zusätzlich sind IKT-Drittdienstleister, die von den EU-Aufsichtsbehörden als kritisch eingestuft wurden, direkt von den neuen Vorgaben und der Aufsicht durch die BaFin betroffen.

13. Cybersecurity Act und

14. Cyber Solidarity Act

Der Cybersecurity Act, der die Rahmenbedingungen für eine EU-weite Zertifizierung für IKT-Produkte, -Dienste und -Prozesse schafft, sowie der geplante Cyber Solidarity Act (CSA) richten sich nicht unmittelbar an die Privatwirtschaft.

Unternehmen können jedoch von dem geplanten Zertifizierungssystem für sogenannte verwaltete Sicherheitsdienste profitieren, welche Unternehmen beim Cybersicherheitsrisikomanagement unterstützen, insbesondere bei der Bewältigung von Sicherheitsvorfällen und der anschließenden Wiederherstellung.

Der CSA hingegen zielt darauf ab, den Schutz der EU gegen Cyberbedrohungen zu stärken und somit ein sicheres digitales Umfeld zu schaffen. Dazu sieht er die Einrichtung von Sicherheitseinsatzzentren auf nationaler und internationaler Ebene vor, die sich zu einem „europäischen Cyberschutzschild“ zusammenschließen, sowie weitere Mechanismen für Cybervorfälle. Daneben soll eine „EU-Cybersicherheitsreserve“ aus vertrauenswürdigen privaten Anbietern auf Antrag einer öffentlichen Stelle eingreifen können.

Produktsicherheit

15. Cyber Resilience Act

Der Cyber Resilience Act (CRA) zielt darauf ab, die Cybersicherheit von Produkten mit digitalen Elementen zu stärken. Er dürfte im Juli 2024 verabschiedet werden, sieht jedoch

eine lange, dreijährige Umsetzungsfrist vor. Die Verordnung erfasst Software und Hardware, die über ein Produkt oder Netzwerk zugänglich sind, jedoch nicht rein digitale Dienste wie Cloud-Services oder SaaS. Die Verordnung betrifft etwa smarte Küchengeräte, mobile Endgeräte oder **vernetzte Maschinen** und Betriebssysteme, ausgenommen sind Kraftfahrzeuge, In-Vitro-Diagnostika und Medizinprodukte.

Die Hersteller sind dazu verpflichtet, bereits während der Entwicklung sicherzustellen, dass die unter eigenem Namen vermarkteten Produkte grundlegende **Sicherheitsanforderungen** erfüllen, die Datenvertraulichkeit gewährleisten und Schwachstellen während des gesamten Produktlebenszyklus, üblicherweise fünf Jahre, getestet und durch **automatische kostenlose Updates** behoben werden. Produkte mit bekannten Schwachstellen dürfen nicht vermarktet werden. Zudem sind ausgenutzte Schwachstellen und Sicherheitsvorfälle zu melden. Die Bewertung der Cybersicherheitsrisiken soll Teil der technischen Dokumentation sein. Der CRA fordert darüber hinaus eine **EU-Konformitätserklärung** und CE-Kennzeichnung sowie für besonders kritische Produkte eine Vertrauenswürdigkeitsprüfung oder Prüfung unter Beteiligung einer sachkundigen dritten Partei. Der CRA sieht Ausnahmen für Open-Source-Produkte vor, nicht jedoch für Kleinst- oder kleine Unternehmen.

Importeure und Händler sind primär dafür verantwortlich, die Erfüllung der grundlegenden Sicherheitsanforderungen, das Vorliegen der technischen Dokumentation, der EU-Konformitätserklärung und der CE-Kennzeichnung zu überprüfen. Importeure, die Produkte unter eigenem Namen vermarkten, unterliegen den Herstellerpflichten.

16. Produktsicherheitsverordnung

Die neue Produktsicherheitsverordnung (General Product Safety Regulation, GPSR), deren Umsetzung bis zum 13.12.2024 zu erfolgen hat, definiert neue Sicherheitskriterien für alle Produkte. Im Fokus stehen dabei insbesondere „smarte Produkte“, für die Cybersicherheitsmerkmale sowie lernende und vorausschauende Funktionen als wesentlich erachtet werden. Hersteller, welche die Produkte unter eigenem Namen vermarkten, sind dazu verpflichtet, für alle Produkte eine **Risikoanalyse** durchzuführen, deren Dokumentation und die technischen Unterlagen vorzuhalten sowie zahlreiche **Informationspflichten** zu erfüllen.

Für **Hersteller, Händler und Importeure** gilt außerdem eine Meldepflicht bei Unfällen. Anbieter von Online-Marktplätzen können zudem verpflichtet werden, Inhalte mit Bezug zu gefährlichen Produkten von ihrer Plattform zu löschen.

Produkthaftung

17. Produkthaftungsrichtlinie

Zur Stärkung des Verbraucherschutzes arbeitet die EU an einer umfassenden Neuauflage der Produkthaftungsrichtlinie aus 1985 (vorläufige Einigung war im Dezember 2023).

Nach der Umsetzung in nationales Recht können Hersteller, Importeure, Bevollmächtigte der Hersteller sowie ggf. Online-Plattformen und Einzelhändler auf Schadensersatz in Anspruch genommen werden, wenn ein Produkt, die **integrierte Software** oder eigenständige Software nicht berechtigten Sicherheitserwartungen der Allgemeinheit entspricht oder wenn notwendige Sicherheitsupdates nicht bereitgestellt werden.

Aufgrund der Haftungsrisiken, die sich aus den nachteiligen Beweislastregeln und Offenlegungspflichten ergeben, ist es für Unternehmen ratsam, Produktsicherheitsmaßnahmen sowie Überprüfungen und Sicherheitsupdates zu dokumentieren. Zudem sollten sie bestehende Verträge und Geschäftsbedingungen überarbeiten, falls dies noch nicht geschehen ist.

Marktregulierung

18. Digital Markets Act

Der Digital Markets Act (DMA) sieht seit Mai 2023 umfassende Regeln zur Regulierung großer Digitalunternehmen vor, sogenannte Gatekeeper („Torwächter“). Dies sind ausschließlich Unternehmen, die von der EU-Kommission als Gatekeeper benannt wurden (aktuell Alphabet, Amazon, Apple, Byte-Dance, Meta und Microsoft).

Für die meisten Unternehmen ergeben sich aus der Regulierung keine neuen Pflichten. Sie können jedoch von den Anforderungen an Gatekeeper profitieren, beispielsweise von der Pflicht zur Herstellung von Interoperabilität mit anderen Messenger-Diensten.

Gesundheitsdienste

19. European Health Data Space Act

Der European Health Data Space Act (EHDS) zielt auf die Etablierung eines europäischen Gesundheitsdatenraums ab und umfasst Regelungen sowohl zur primären als auch zur sekundären Nutzung von Gesundheitsdaten im Rahmen von „MyHealth@EU“. Er definiert Anforderungen für Informationssysteme im Gesundheitssektor sowie für Systeme zur elektronischen Patientenakte (EHR-Systeme), deren Bereitstellung in Deutschland künftig im Opt-Out-Modell erfolgen soll. Der EHDS wird wohl noch vor der Sommerpause 2024 verabschiedet und dürfte nach einer Übergangsfrist ab Juni 2026 greifen.

Alle Einrichtungen, die elektronische Gesundheitsdaten von Personen zur **Erbringung von Gesundheitsdiensten** verarbeiten (sog. Primärnutzung), sind verpflichtet, bestimmte Vorgaben einzuhalten. Dies betrifft insbesondere die Rechte der betroffenen Personen zur Kontrolle und Aktualisierung ihrer Daten. Die Verarbeitung umfasst Diagnose und Behandlung, die Abgabe von Arzneimitteln und Medizinprodukten sowie Sozialversicherung, Verwaltung und Kostenerstattung. Auch der **Datenaustausch** zwischen Angehörigen von Gesundheitsberufen, Anbietern, Herstellern und Importeuren von EHR-Systemen sowie Anbietern von Wellness-Anwendungen wie Gesundheits-Apps oder Fitness-

Trackern unterliegen neuen Anforderungen. Insbesondere für Anbieter von EHR-Systemen gelten erweiterte Anforderungen, u.a. zur **Interoperabilität**.

Des Weiteren sind Akteure im Gesundheits- und Pflegesektor verpflichtet, bestimmte Gesundheitsdaten zur **sekundären Nutzung** bereitzustellen, beispielsweise für Forschungs- und Innovationszwecken, die Ausbildung oder die Erprobung von Algorithmen, sofern die Genehmigung einer öffentlichen Stelle vorliegt.

Für die Nutzer der Daten, insbesondere Forschungs- oder Statistikunternehmen sowie Unternehmen, die Gesundheitsprodukte und -Anwendungen entwickeln, gelten weitere strenge Anforderungen.

Mediendienste

20. European Media Freedom Act und

21. Verordnung über Transparenz und Targeting politischer Werbung

Auch das Recht für Mediendienste soll im Digitalzeitalter ankommen. Der European Media Freedom Act (EMFA) soll die Unabhängigkeit von Medienanbietern gewährleisten. Anbieter, die Nachrichten verbreiten und redaktionell kontrollieren, müssen ihre Eigentümerstrukturen offenlegen und Maßnahmen zum Schutz der redaktionellen Unabhängigkeit ergreifen. Die Bestimmungen des EMFA werden insbesondere traditionelle audio-visuelle Mediendienste sowie reichweitenstarke YouTube-Kanäle betreffen. Für sehr große Online-Plattformen im Sinne des DSA sind darüber hinaus weitere Pflichten vorgesehen. Kritiker sehen in den erweiterten behördlichen Befugnissen jedoch eine Bedrohung für die journalistische Freiheit. Der EMFA ist im Mai 2024 in Kraft getreten und greift überwiegend ab August 2025.

Die **Verordnung über die Transparenz und das Targeting politischer Werbung** zielt insbesondere auf Werbedienstleister und Online-Plattformen ab, die für politische Werbung Geld erhalten (Herausgeber politischer Werbung). Diese sind dazu verpflichtet, diese als solche zu kennzeichnen und Informationen zu Targeting und Finanzierung offenzulegen. Dies gilt nicht für reine politische Meinungskundgabe oder nicht-fremdfinanzierte journalistische Inhalte. Die Targeting-Methode politischer Werbung, welche auf persönlichen Daten basiert, ist nur mit Einwilligung des Nutzers zulässig. Zudem ist sie bei sensiblen Daten oder Minderjährigen gänzlich verboten. Die Verordnung wurde im März 2024 vom Europäischen Rat verabschiedet, dürfte noch vor der Sommerpause 2024 in Kraft treten und gilt nach einer Übergangsfrist von 18 Monaten.

Identitätsdienste

22. eIDAS Act

Die Überarbeitung des eIDAS Act sieht die Einführung einer **European Digital Identity Wallet** (EUid-Wallet) für alle EU-Bürgerinnen vor. Diese soll als **digitaler Ausweis**

fungieren und weitere Dokumente wie **Führerschein**, Berufszertifikate oder **Reisetickets** enthalten können. Die Anerkennung der EUid soll hiernach nur öffentlichen Stellen sowie sehr großen Online-Plattformen im Sinne des DSA obliegen. Kleinere Diensteanbieter können die EUid freiwillig akzeptieren und sollten – sofern sie sich dafür entscheiden – die entsprechenden technischen Schnittstellen schaffen, sobald die technischen Spezifikationen für die Wallet vorliegen.

Weitere Vorgaben betreffen **Vertrauensdiensteanbieter**, die etwa qualifizierte elektronische Signaturen, Siegel oder Zeitstempel, elektronische Einschreiben oder Validierungsdienste anbieten. Die Verpflichtung zur Akzeptanz bestimmter EU-Zertifikate durch Webbrowser (Qualified Website Authentication Certificates) wird jedoch von vielen Seiten kritisiert. Diese Zertifikate könnten möglicherweise nicht die gleichen Sicherheitsstandards wie etablierte Zertifikate gewährleisten und Massenüberwachung ermöglichen. Die neue eIDAS-Änderungsverordnung ist im April 2024 in Kraft getreten.

Fazit und Best Practice

Was ist nun aus Unternehmenssicht zu tun? Orientiert man sich an den Umsetzungsfristen, so gilt im Hinblick auf die **Priorität** der neuen Regelungen zum EU-Digitalrecht folgende Reihenfolge:

- Juni 2020 — P2B Act (Online-Dienste)
- September 2023 — Data Governance Act (Datendienste)
- Februar 2024 — **Digital Services Act** (Online-Dienste)
- Mai 2024 — Digitale-Dienste-Gesetz (Online-Dienste)
- **Oktober 2024** — **NIS-2**-Umsetzungsgesetz (wichtige Einrichtungen)
- Dezember 2024 — AI Act (Frist für das Verbot bestimmter KI-Systeme)
- Dezember 2024 — General Product Safety Regulation (Produkthersteller)
- Januar 2025 — **DORA** (Finanzbranche, IT-Dienstleister)
- August 2025 — European Media Freedom Act (Medienunternehmen)
- September 2025 — **Data Act** (Datendienste)
- Mai 2026 — eIDAS Act (Vertrauensdienste)
- Juni 2026 — **AI Act** (Anbieter und Nutzer von KI-Systemen)
- Juni 2026 — European Health Data Space Act (Online-Dienste)
- August 2026 — **E-Evidence** Act (Online-Dienste)
- Januar 2027 — Machinery Regulation (Hersteller von Maschinen)
- Juni 2027 — **Cyber Resilience Act** (vernetzte Produkte)

Unternehmen sollten sich an dieser Reihenfolge orientieren und zunächst per Workshop eine **Betroffenheitsanalyse** durchführen, nach Feststellung der relevanten Verordnungen eine **GAP-Analyse** vornehmen im Hinblick auf die neuen Gesetzesvorgaben sowie anschließend ein internes Projektteam mit der Erstellung einer **Roadmap zur Umsetzung** beauftragen. Erfahrungsgemäß hilft es dem Projektteam, wenn in regelmäßigen Abständen (zumeist einmal pro Woche) ein spezialisierter Berater zur Verfügung steht, der mit wenig Aufwand offene Fragen beantworten und auch aktuelle Dokumente (z.B. KI-Richtlinie, siehe

Art. 4 AI Act) beisteuern kann. Wir bieten mit **HEUKING** neben den obigen Workshops, GAP-Analysen und dem Lieferantenmanagement (Verpflichtung der Dienstleister auf neue Sicherheitsvorgaben) auch **wöchentliche Status-Calls** via Internet an, aktuell insbesondere im Rahmen der Umsetzung von Projekten zur Implementierung von ISMS (Information-Security-Management-System, z.B. ISO/IEC 27001), die im Regelfall notwendig sind zur Erreichung einer NIS-2- oder DORA-Compliance.

Möchten Sie zum Thema EU-Digitalrecht, seine nationale Umsetzung und unsere Best Practices zur Umsetzung auf dem **aktuellen Stand** bleiben? Dann lassen Sie sich von meiner Assistentin Gulchera Zundai (g.zundai@heuking.de) auf Anfrage gern in den Verteiler unseres unverbindlichen Newsletters aufnehmen.

Ihr