PRIVACYXPERTS



Dr. Jens Eckhardt

EU-Cybersecurity – sowie Digital- und Datenregulierungen

NIS-2, DORA, Cyber Resilience Act, Digital Services Act, Data Act, AI Act – was Unternehmen jetzt wissen und umsetzen müssen

www.privacyxperts.de

Dr. Jens Eckhardt

EU-CYBERSECURITY- SOWIE DIGITAL- UND DATEN-REGULIERUNGEN

NIS-2, DORA, Cyber Resilience Act, Digital Services Act, Data Act, AI Act – was Unternehmen jetzt wissen und umsetzen müssen

INHALT

EINFÜHRUNG 8

VORWORT 10

VERLIEREN SIE NICHT DEN ÜBERBLICK 11

I. Überblick über die Rechtsakte 11

II. First Things First – achten Sie auf den Zeitstrahl! 11

III. Generelles Verhältnis der Rechtsakte zum Datenschutzrecht 14

IV. Auslegung: Jeder Rechtsakt für sich und aus sich heraus! 16

A. CYBER SECURITY: NIS-2-UMSETZUNG (SCHWERPUNKT) MIT WEITEREN CYBER-SECURITY-RECHTSAKTEN 17

I. NIS-2-Richtlinie und BSI-Gesetz 17

1. Überblick 17

1.1 NIS-2-Richtlinie und Umsetzung im BSI-Gesetz 18

1.1.1 NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG-RegE) vom 02.10.2024 und Ende des Gesetzgebungsverfahrens 19

1.1.2 Was gilt in der Zwischenzeit? Auswirkungen auf die Praxis? 20

1.2 Worum geht es? 20

1.3 Zeitstrahl 23

1.4 Begrifflichkeiten und Definition 24

2. Verpflichtete 24

2.1 Verpflichtete der §§ 28, 29 BSIG-RegE 24

2.2 Ausnahmen 27

2.3 Mittelbar Verpflichtete (Supply Chain) 28

3. Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen 29

4. Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen und Nachweispflichten für Betreiber kritischer Anlagen 32

5. Meldepflichten sowie Befugnisse der Aufsichtsbehörde und Pflicht zur Unterstützung 32

5.1 Meldepflichten 33

5.2 Pflicht zur Unterrichtung über eine erheblichen Cyberbedrohung 36
5.3 Anordnungen zur Unterrichtung und zur Information der Öffentlichkeit (§§ 35, 36 BSIG-RegE) 37
5.4 Verhältnis zur Melde- und Benachrichtigungspflicht nach Artt. 33, 34 DS-GVO, § 168 TKG 37
6. Registrierungspflicht 38
7. Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen 39
8. Untersagung des Einsatzes kritischer Komponenten 41
9. Aufsicht, Kontrolle und Sanktionen 43
10. Verhältnis zur DS-GVO 44
II. Digital Operational Resilience Act (DORA) 45
1. Überblick 45
1.1 Worum geht es? 46
1.2 Zeitstrahl 49
1.3 Begrifflichkeiten und Definitionen 49
2. Verpflichtete 49
3. Pflichten zum IKT-Risikomanagement 51
3.1 Governance und Organisation (Art. 5 DORA) 51
3.2 IKT-Risikomanagementrahmen (Artt. 6–16 DORA) 52
3.3 Behandlung, Klassifizierung und Berichterstattung von IKT–Vorfällen (Artt. 17–23 DORA) 53
3.4 Test der digitalen operationalen Resilienz (Artt. 24–27 DORA) 54
3.5 Management des IKT–Drittparteienrisikos (Artt. 28–44 DORA) 55
3.6 Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen (Art. 45 DORA) 56
4. Sanktionen 57
5. Verhältnis zur DS-GVO 57
III. Cyber Resilience ACT (CRA) 58
1. Überblick 58
1.1 Worum geht es? 58
1.2 Zeitstrahl 59
1.3 Begrifflichkeiten und Definitionen 59
2. Anwendungsbereich 60

3. Allgemeine Bestimmungen (Artt. 1–12 CRA) ... 61
3.1 Produkte mit digitalen Elementen ... 61
3.2 Hochrisiko-KI-Systeme (Art. 12 CRA) ... 61
4. Pflichten der Wirtschaftsakteure und Bestimmungen in Bezug auf freie und quelloffene Software (Artt. 13–26 CRA) ... 61
5. Sanktionen ... 62
6. Verhältnis zur DS-GVO ... 63

B. DIGITAL SERVICES: DIGITAL SERVICES ACT MIT DIGITAL MARKETS ACT ... 64

I. Digital Services Act ... 64
1. Überblick ... 64
1.1 Worum geht es? ... 65
1.2 Zeitstrahl ... 67
1.3 Begrifflichkeiten und Definition ... 67
2. Verpflichtete und Anwendungsbereich ... 68
3. Haftung der Anbieter von Vermittlungsdiensten (Kapitel II, Artt. 4–10 DSA) ... 71
4. Sorgfaltspflichten für transparentes und sicheres Online-Umfeld (Kapitel III, Artt. 11–48 DSA) ... 74
5. Sanktionen (Art. 52 DSA) ... 76
6. Verhältnis zur DS-GVO ... 77
II. Digital Markets Act (DMA) ... 77
1. Überblick ... 78
1.1 Worum geht es? ... 78
1.2 Zeitstrahl ... 80
1.3 Begrifflichkeiten und Definitionen ... 80
2. Verpflichtete ... 81
3. Benennung als Gatekeeper (Torwächter) ... 82
4. Pflichten des Gatekeepers (Torwächters) ... 82
5. Sanktionen (Art. 30 DMA) ... 84
6. Verhältnis zur DS-GVO ... 85

C. DATA (SHARING): DATA ACT (SCHWERPUNKT) UND HINWEIS AUF DATA GOVERNANCE ACT 86

I. Data Act (DA) bzw. Datenverordnung 86

1. Überblick 87

1.1 Worum geht es? 87

1.2 Zeitstrahl 90

1.3 Begrifflichkeiten und Definitionen 90

2. Verpflichtete 92

3. Kapitel II – Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen 93

4. Kapitel III – Pfilchten der Dateninhaber mit Pflilcht zur Datenbereitstellung gemäß Unionsrecht 94

5. Kapitel IV – Missbräuchliche Vertragsklauseln 94

6. Bereitstellung von Daten für öffentliche Stellen, die Kommission, die Europäische Zentralbank und Einrichtungen der Union wegen außergewöhnlicher Notwendigkeit (Kapitel V) 95

7. Wechsel zwischen Datenverarbeitungsdienst (Cloud Switching) (Kapitel VI) 95

8. Sanktionen 97

9. Verhältnis zur DS-GVO 98

II. Data Governance Act (DGA) 100

1. Überblick 100

1.1 Worum geht es? 100

1.2 Zeitstrahl 101

1.3 Begrifflichkeiten und Definitionen 101

2. Weiterverwendung bestimmter Kategorien geschützter Daten im Besitz öffentlicher Stellen (Kapitel II, Artt. 3–9 DGA) 102

3. Anforderungen an Datenvermittlungsdienste (Kapitel III, Artt. 10–15 DGA) 103

4. Datenaltruismus (Kapitel IV, Artt. 16–25 DGA) 105

5. Verhältnis zur DS-GVO 106

D. KÜNSTLICHE INTELLIGENZ: AI ACT 108

1. Überblick 108
1.1 Worum geht es? 108
1.2 Zeitstrahl 110
1.3 Begrifflichkeiten und Definition 111
2. Was regelt der AI Act? – Was sind KI-Systeme und KI-Modelle mit allgemeinem Verwendungszweck? 112
2.1 KI-System 113
2.2 KI-Modell mit allgemeinem Verwendungszweck 115
2.3 Ausnahmen 116
3. Verpflichtete des AI Act 118
3.1 Verpflichtete des AI Act 118
3.2 Risiko des Rollenwechsels (Art. 25 AI Act) 121
4. Risikobasierter Regelungsansatz – das Risiko bestimmt über die Anwendung der Regelungen! 122
4.1 Risikokategorisierung des AI Act 122
4.2 KI-spezifische Risiken im Überblick 123
4.3 KI-Kompetenz (Art. 4 AI Act) 124
5. Verbotene Praktiken im KI-Bereich (Art. 5 AI Act) 127
6. Hochrisiko KI (Art. 6 AI Act) 130
6.1 Festlegung der Hochrisiko-KI-Systeme (Art. 6 AI Act) 131
6.1.1 Hochrisiko-KI-System nach Art. 6 Abs. 1 AI Act 131
6.1.2 Hochrisiko-KI-System nach Art. 6 Abs. 2 AI Act 131
6.1.3 Leitlinien und Liste praktischer Beispiele für Anwendungsfälle (Art. 6 Abs. 5 AI Act) 132
6.2 Generelle Anforderungen an Hochrisiko-KI-Systeme (Artt. 8–15 AI Act) 132
6.3 Pflichten der Anbieter und Betreiber von Hochrisiko-KI-Systemen und anderer Beteiligter (Artt. 16 ff. AI Act) 136
6.3.1 Pflichten der Anbieter (Artt. 16–22 AI Act) 137
6.3.2 Pflichten der Betreiber (Artt. 26, 27 AI Act) 139
6.3.2.1 Pflichten der Betreiber von Hochrisiko-KI-Systemen (Art. 26 AI Act) 139
6.3.2.2 Grundrechte-Folgenabschätzung für Hochrisiko-KI-Systeme (Art. 27 AI Act) 142
6.3.3 Pflichten der weiteren Akteure in Bezug auf Hochrisiko-KI-Systeme 143

7. Transparenzpflichten für Anbieter und Betreiber bestimmter KI-Systeme (Art. 50 AI Act) 143

8. KI-Modelle mit allgemeinem Verwendungszweck (Artt. 51–56 AI Act) 148

8.1 KI-Modelle mit allgemeinem Verwendungszweck (Artt. 53, 54 AI Act) 149

8.2 KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko (Art. 55 AI Act) 149

9. Sanktionen (Art. 99 AI Act) 150

10. KI-Beauftragter 152

11. Verhältnis zur DS-GVO 153

ABBILDUNGS + ARBEITSHILFENVERZEICHNIS 158

EINFÜHRUNG

Die EU setzt ihre Digitalstrategie durch neue Digitalrechtsakte um. Diese sollen einen regulatorischen Rahmen für die faire Entwicklung von Märkten schaffen und zugleich zu einer einheitlichen Rechtslage in der EU beitragen. Insbesondere handelt es sich um den **Data Act** und **den Data Gorvenance Act** sowie den **Digital Services Act** und den **Digital Markets Act**. Diese Rechtsakte haben eine starke regulatorische Prägung und sollen Wettbewerbsbeschränkungen durch Vormachtstellungen entgegenwirken. Darüber hinaus enthalten sie auch Nachfolgeregelungen zur EU-E-Commerce-Richtlinie. **Vereinfacht lässt sich sagen, dass der Data Act und der Data Gorvenance Act den Zugang zu Daten und das Teilen von Daten regeln, während der Digital Services Act und der Digital Markets Act die Bereitstellung digitaler Dienste regeln.** Diese Rechtsakte beschränken sich jedoch nicht allein hierauf. Der Data Act enthält beispielsweise auch Regelungen zur Erleichterung des Wechsels von Cloud Services („Cloud Switching") und der Digital Services die (abgestufte) Haftung für Inhalte im Internet. Damit zeigt sich auch bereits eine erste Herausforderung: Sie müssen sich einen Überblick verschaffen und behalten, welcher Rechtsakt was regelt.

Daneben reagiert die EU mit einer Reihe von Rechtsakten auf die signifikant gestiegenen Risiken im Bereich der **Cyber-Sicherheit und IT-Sicherheit**. Mit der **NIS-2-Richtlinie** sollen die IT- und Cybersicherheit im Bereich der (besonders) wichtigen Infrastrukturen gesteigert und sichergestellt werden. Unternehmen in bestimmten Branchen und ab einer bestimmten Größe müssen über die allgemeinen Anforderungen der Cyber- und IT-Sicherheit hinaus weitere und strengere Anforderungen erfüllen. Der **Digital Operational Resilience Act (DORA)** ist eine hierüber noch hinausgehende Spezialregelung im Bereich des Finanzwesens. Die in der NIS-2-Richtlinie und der DORA vorgesehenen Anforderungen gelten auch für Unternehmen in der Supply Chain, die Dienstleistungen für verpflichtete Unternehmen erbringen. Dadurch wird der faktische Anwendungsbereich der Regelungen erheblich ausgeweitet. Insbesondere die DORA enthält umfassend Regelungen zum **IKT-Drittparteienrisiko.** Ergänzt werden sie durch den **Cybersecurity Act (CSA)** und die **Resilience of Critical Entities Directive (CER)** sowie jüngst durch den **Cyber Resilience Act (CRA)**, der Sicherheitsanforderungen für die digitalen Produkte vorgibt.

Künstliche Intelligenz wird durch den **AI Act** der EU reguliert. Hierbei handelt es sich nicht um eine Art „Datenschutzrecht 2.0", sondern um eine weitere Regelung des Produktsicherheitsrechts. Durch den AI Act sollen die Risiken, die von

KI-Systemen und KI-Modellen mit allgemeinem Verwendungszweck ausgehen, „beherrschbar“ gemacht werden.

Parallel zu allen vorstehenden neuen Rechtsakten besteht das **Datenschutzrecht**, insbesondere in Gestalt der **DS-GVO** und der im **Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG)** umgesetzten Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG (Stichwort: ePrivacy-Richtlinie).

Das vorliegende Werk gibt einen Überblick über diese Rechtsakte und insbesondere auch über ihr Verhältnis zum Datenschutzrecht.

VORWORT



Die neuen Cybersecurity-Regulierungen sowie die Digital- und Datenregulierungen der EU führen zu einer erheblichen und nachhaltigen Veränderung der Anforderungen in der digitalen Unternehmenswelt. Durch das Inkrafttreten bzw. den Anwendungsbeginn dieser Regelungen innerhalb eines kurzen Zeitfensters müssen Sie sich in einem „gedrängten" Zeitraum mit einer Mehrzahl textlich umfangreicher und nicht stets in leicht eingängiger Sprache verfasster Gesetze auseinandersetzen.

Wegducken hilft nicht! Die Regelungen sind entweder selbst nicht mit scharfen Sanktionen belegt oder können die Grundlage für Schadensersatzansprüche Dritter sein. Eine Befassung mit der gebotenen Sorgfalt ist daher unvermeidbar und unerlässlich.

Das Buch verschafft Ihnen einen strukturierten Überblick über die Anforderungen, damit Sie die Relevanz für sich bewerten können. In der Natur der Sache liegt es, dass eine umfassende und ausdifferenzierte Darstellung nicht erfolgen kann, weil dadurch die Zielsetzung der Überschaubarkeit konterkariert würde. Darüber hinaus gibt Ihnen die gleichförmig strukturierte Darstellung einen Überblick zur Entwicklung einer Herangehensweise zur Umsetzung. Aus diesem Grund werden auch wichtige Aspekte wie First Things First vorweg für alle Themen einheitlich dargestellt.

Ihr Dr. Jens Eckhardt

VERLIEREN SIE NICHT DEN ÜBERBLICK

In der vorstehenden Einleitung sind die aktuell relevantesten und jüngsten Rechtsakte im Kontext der Nutzung von Daten und Digitalen sowie des Schutzes im Kontext der Digitalisierung angesprochen.

Damit sind rund 715 DIN-A4-Seiten Rechtstexte (BSI-RegE, NIS-2-Richtlinie, DORA CRA, DSA, DMA, DA, DGA, AI Act) plus rund 88 DIN-A4-Seiten der DS-GVO angesprochen. Die nachfolgende Übersicht sowie die zeitliche Einordnung der Rechtsakte erleichtern Ihnen den Überblick.

I. Überblick über die Rechtsakte

Die Begriffe DSA, DMA, DA, DGA, AI, NSI-2, DORA, CSA, CER und CRA lassen schnell den Überblick verlieren, was der Regelungsgegenstand dieser Rechtsakte ist. Die Übersicht auf der nächsten Seite erleichtert Ihnen die Zuordnung der Rechtsakte zur Regelungsmaterie und verschafft Ihnen damit eine erste Orientierung, womit Sie sich befassen (müssen).

Die Grafik verdeutlich auch, dass neben allen diesen Spezialgesetzen auch das Datenschutzrecht (Privacy) berücksichtigt werden muss, sofern – was typischerweise der Fall sein wird – bei der Erfüllung der Pflichten nach diesen Gesetzen personenbezogene Daten verarbeitet werden. Das Verhältnis muss in jedem Einzelfall hinterfragt werden.

Die Themenfelder werden im vorliegenden Buch jeweils in eigenen Teilen, die einzelnen Rechtsakte in einzelnen Kapiteln dargestellt. Einleitend wird in jedem Kapitel ein Überblick über die Inhalte der jeweiligen Rechtsakte gegeben, damit Sie sich jeweils schnell orientieren können.

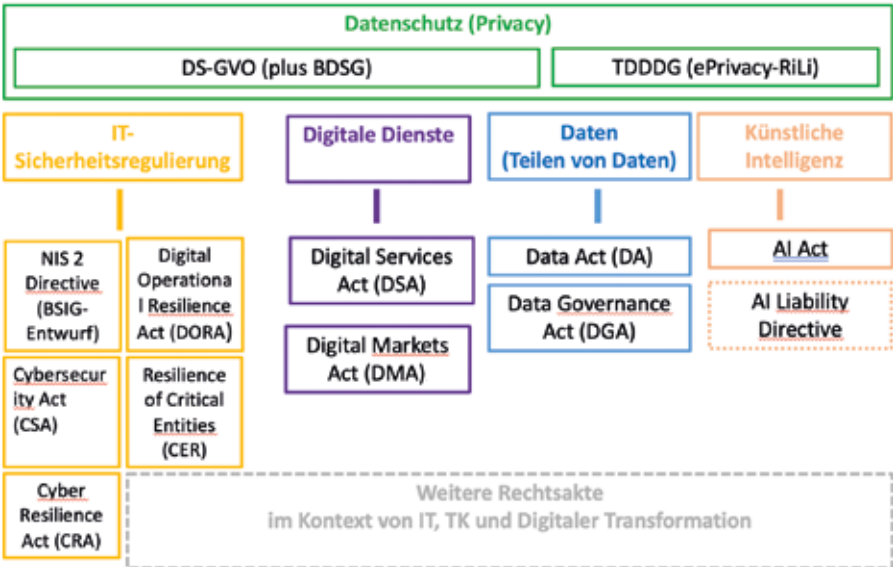
II. First Things First – achten Sie auf den Zeitstrahl!

Der Umfang der Rechtsakte in der Gesamtschau erfordert es, dass Sie sich auch unter zeitlichen Gesichtspunkten vergegenwärtigen, was drängender ist. Keine der Pflichten lässt sich aus dem Stegreif erfüllen. Dennoch könnte es ein Fehler sein, sich zunächst mit Regelungen zu befassen, die erst in Monaten in Kraft treten, während bereits Regelungen, deren Geltung kurz bevorsteht oder die sogar schon gelten, unbeachtet bleiben.

Bis 31.12.2024	2025
NIS-2-Richtlinie: Umsetzungsfrist bis 17.10.2024	Umsetzung der Vorgaben der NIS-2-Richtlinie – v. a. im BSIG: unklar, voraussichtlich nicht vor Ende 2025
DORA: Inkrafttreten im Januar 2023	Anwendungsbeginn: 17.01.2025
Cyber Resilience ACT (CRA): Inkrafttreten im Dezember 2024	
Digital Services Act (DSA): Inkrafttreten im November 2022 Anwendungsbeginn (jedenfalls): 17.02.2024	
Digital Markets Act (DM): Inkrafttreten im November 2022 Anwendungsbeginn (jedenfalls): 02.05.2023	➤ **genereller Anwendungsbeginn: 12.09.2025** (z. B. Regelungen über das „Cloud Switching" in Kapitel VI). ➤ **Geltung des Kapitel III** nur in Bezug auf Datenbereitstellungspflichten nach dem Unionsrecht oder nach im Einklang mit Unionsrecht erlassenen nationalen **Rechtsvorschriften, die nach dem 12.09.2025 in Kraft treten**. ➤ **Geltung des Kapitel IV** nur für **Verträge, die nach dem 12.09.2025 geschlossen wurden.**
Data Act (DA): Inkrafttreten im Januar 2024	
Data Governance Act (DGA): Inkrafttreten im Juni 2023 Anwendungsbeginn: 24.09.2023	
AI Act: Inkrafttreten: Mitte 2024	Ab 02.02.2025: Anwendung der Kapitel I und II Ab 02.08.2025 Kapitel III Abschnitt 4 u. Kapitel V u. Kapitel VII u. Kapitel XII u. Artikel 78 – mit Ausnahme von Art. 101 AI Act
Hinweis: Anwendungsbeginn bedeutet, vereinfacht gesagt, dass ab diesem Zeitpunkt müssen. Die Vorbereitung zur Erfüllung der Pflichten muss also davor erfolgt sein.	

2026	2027	Nach 01.01.2028
➤ **genereller Anwendungsbeginn: 11.09.2026** ➤ Anwendungsbeginn für Kapitel IV (Artt. 35–51 CRA): 11.06.2026	Anwendungsbeginn für Art. 71 Abs. 2 CRA: 11.12.2027	
Geltung des **Art. 3 Abs. 1 DA** nur für vernetzte Produkte und die mit ihnen verbundenen Dienste, die nach dem **12.09.2026** in Verkehr gebracht wurden.		
Ab 02.08.2026 Anwendungsbeginn (aber: Bestandsschutzregelungen nach Art. 111 AI Act)	Ab 02.08.2027: Hochrisiko-KI-Systeme nach Art. 6 Abs. 1 AI Act	Bestandsschutzregelungen (Art. 111 AI Act)

die Regelungen gelten und ab diesem Zeitpunkt die Pflichten eingehalten werden



Die genannten Rechtsakte regeln ihren Geltungs- und Anwendungsbeginn typischerweise in der letzten Regelung des jeweiligen Gesetzes. Also lesen Sie zunächst diese Regelung oder die Übersicht auf der vorherigen Doppelseite.:

Inkrafttreten und Anwendungsbeginn – der Unterschied: Die Rechtsakte unterscheiden zwischen dem Inkrafttreten und dem Anwendungsbeginn. Vereinfacht gesagt: Mit dem Inkrafttreten existieren sie als Gesetz und mit dem Anwendungsbeginn sind sie zu beachten. Damit ergibt sich eine Übergangsfrist zwischen dem Zeitpunkt, in dem klar ist, was getan werden muss, bis es getan werden muss. Der Gesetzgeber trägt damit auch dem Umstand Rechnung, dass die Pflichten nicht aus dem Stegreif erfüllt werden können.

III. Generelles Verhältnis der Rechtsakte zum Datenschutzrecht

Die Digitalrechtsakte der EU sind überwiegend ebenso wie die DS-GVO EU-Verordnungen. Insoweit ergibt sich kein Vorrang der DS-GVO aufgrund der Normhierarchie. Vielmehr müssen die allgemeinen Auslegungsgrundsätze zum Tragen kommen, wonach grundsätzlich der jüngere Rechtsakt bzw. der speziellere Rechtsakt Vorrang hat. Für die DS-GVO würde das bedeuten, dass sich im Fall einer Kolli-

sion der Vorgaben der DS-GVO mit den Vorgaben eines jüngeren Rechtsaktes die Vorgaben des jüngeren Rechtsaktes durchsetzen.

Die in diesem Buch angesprochenen neuen Rechtsakte enthalten jedoch selbst Aussagen bzw. Regelungen zu ihrem Verhältnis zur DS-GVO. Das macht es in der Praxis – wenngleich nur auf den **ersten Blick** – einfacher, weil es explizite Regelungen gibt, die Sie lesen können. **Auf den zweiten Blick** macht es dies jedoch komplizierter, weil jeder der neuen Rechtsakte dies eigenständig regelt. Das bedeutet, dass für jeden Rechtsakt einzeln das Verhältnis zur DS-GVO bestimmt werden muss. Im vorliegenden Buch erfolgt die Darstellung des Verhältnisses zwischen dem neuen Rechtsakt und der DS-GVO daher auch zu jedem Rechtsakt im jeweiligen Kapitel.

Hinweis

Sie müssen für jeden Rechtsakt eigenständig das Verhältnis zur DS-GVO bestimmen.

Auf den dritten Blick: Der Gesetzgeber benennt jedoch nicht konkret (die) Regelungen, die mit der DS-GVO im Konflikt stehen können, sondern regelt das Verhältnis für jeden Rechtsakt recht formelhaft. Die Praxis zeigt, dass gerade die in einigen Rechtsakten verwendete Formulierung des Vorrangs im Konfliktfall das Problem, wie mit Widersprüchen umzugehen ist, in die Praxis verlagert und das Gesetz keine klaren Antworten liefert. Diese Konflikte werden dann in der Praxis durch Auslegung und letztlich durch Gerichte zu klären sein.

Besonderheit NIS-2-Richtlinie

Eine Besonderheit besteht für die NIS-2-Richtlinie. Denn anders als beispielsweise die DORA oder der AI Act ist das keine EU-Verordnung, die in jedem Mitgliedstaat unmittelbar gilt, sondern eine EU-Richtlinie. Eine EU-Richtlinie bedarf eines nationalen Umsetzungsgesetzes, damit sie Wirkung für die Bürger des jeweiligen Mitgliedstaates entfaltet. Das soll in Deutschland nach dem Stand zur Drucklegung dieses Buches durch das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) erfolgen.

Mit anderen Worten: Erst das nationale Umsetzungsgesetz erweckt die Pflichten der NIS-2-Richtlinie zum Leben.

Die DS-GVO hat damit aufgrund ihres Charakters als EU-Verordnung entsprechend der Normhierarchie Vorrang vor dem nationalen Gesetz (z. B. BSI-Gesetz) zur Umsetzung der NIS-2-Richtlinie. Für die Umsetzung der Datenschutzrichtli-

nie für elektronische Kommunikation 2002/58/EG (Stichwort: ePrivacy-Richtlinie) im TDDDG besteht dieselbe Ausgangssituation. Aber für diese ePrivacy-Richtlinie sieht die DS-GVO anders als für die NIS-2-Richtlinie in Art. 95 DS-GVO eine Öffnungsklausel vor. Die NIS-2-Richtlinie stellt auch klar, dass sie keinen Vorrang vor dem Datenschutzrecht hat. In ihrem ErwGr. 14 sieht sie vor, dass das Datenschutzrecht unberührt gelassen wird. In ErwGr. 43 stellt die NIS-2-Richtlinie auf die Erfüllung der Pflichten „im Einklang mit" dem Datenschutzrecht ab.

Zusammenfassung zur Besonderheit der NIS-2-Richtlinie: Die Anforderungen der DS-GVO sind bei der Erfüllung der Pflichten nach dem nationalen Umsetzungsgesetz zu beachten, sofern personenbezogene Daten verarbeitet werden.

IV. Auslegung: Jeder Rechtsakt für sich und aus sich heraus!

Die angesprochenen Rechtsakte (mit Ausnahme der DS-GVO) sind zwar allesamt in einem zeitlichen Zusammenhang verabschiedet worden und sind Bestandteil der EU-Datenstrategie. Das darf jedoch nicht zu dem Irrtum verleiten, dass diese Gesetze gemeinsam und aufeinander abgestimmt entstanden sind. Jedes dieser Gesetze steht im Zweifel für sich allein.

Dementsprechend muss jedes dieser Gesetze aus sich heraus ausgelegt werden. Gerade für die bereits recht vertraute DS-GVO ist zu beachten, dass eine Auslegung dieser EU-Rechtsakte nicht aus der DS-GVO heraus erfolgen darf. Die Formulierung „im Auftrag" in Art. 4 AI Act kann daher nicht im Sinne der Auftragsverarbeitung nach Art. 4 Nr. 8, Art. 28 DS-GVO ausgelegt werden, sondern muss nach ihrem Sinn und Zweck gedeutet werden.

Auch Begriffe eines Rechtsakts dürfen nicht ohne Weiteres anhand von Definitionen eines anderen Rechtsaktes ausgelegt werden. Wenn nicht ein Rechtsakt auf die Definition in einem anderen Rechtsakt verweist, muss im Einzelfall geprüft werden, ob die Definition aus einem anderen Rechtsakt herangezogen werden darf.

A. CYBERSECURITY: NIS-2-UMSETZUNG MIT WEITEREN CYBERSECURITY-RECHTSAKTEN

Unter dem Stichwort Cybersecurity-Regulation werden die aktuellen und bekanntesten Rechtsakte der EU zur Stärkung der Cybersecurity und IT-Security zusammengefasst.

Die **(Umsetzung der) NIS-2-Richtlinie,** der **Digital Operational Resilience Act (DORA),** der **Cybersecurity Act (CSA),** die **Resilience of Critical Entities Directive (CER)** sowie der **Cyber Resilience Act (CRA)** werden nachfolgend behandelt. Diese unterscheiden sich maßgeblich dadurch, dass ein Teil der Rechtsakte Unternehmen aufgrund ihres Tätigkeitsbereichs (z. B. NIS-2 und DORA) adressiert, während andere Regelungen (z. B. CRA) die Herstellung, Bereitstellung und/oder Verwendung bestimmter Produkte durch Unternehmen adressiert. Unter die zuletzt genannte Kategorie ließe sich auch der AI Act fassen, der jedoch nicht nur die IT-Sicherheit in Bezug auf die Nutzung von KI-Systemen adressiert und daher eigenständig behandelt wird.

Der Schwerpunkt der Darstellung ist die (Umsetzung der) NIS-2-Richtlinie.

I. NIS-2-Richtlinie und BSI-Gesetz

NIS steht für Netz- und Informationssysteme. Die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 **(NIS-2-Richtlinie)**[1] zielt auf die Stärkung des Schutzes der Netz- und Informationssysteme. Sie löst die Vorgaben der NIS-Richtlinie ab.

1. Überblick

Netz- und Informationssysteme sind ein zentraler Bestandteil des Alltags und für den grenzüberschreitenden Austausch. Forciert wurde dies durch den schneller werdenden digitalen Wandel und die Vernetzung der Gesellschaft. Mit dieser Ent-

[1] Link: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555 (Stand: 31.01.2025)

wicklung geht jedoch auch die Ausweitung der Cyberbedrohungslage einher. Auch hat die Digitalisierung neue Herausforderungen mit sich gebracht, die in allen Mitgliedstaaten entsprechende koordinierte und innovative Reaktionen erfordern.

Mit Blick auf die Bedrohungslage ist festzustellen, dass die Anzahl, Tragweite, Komplexität, Häufigkeit und Auswirkungen von Vorfällen zunehmen. Sie stellen eine jetzt schon erhebliche, aber kontinuierlich zunehmende Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Sicherheitsvorfälle können die Ausübung wirtschaftlicher Tätigkeiten im Binnenmarkt nachhaltig beeinträchtigen und neben finanziellem Verlust auch das Vertrauen der Nutzer untergraben und damit insgesamt der Wirtschaft und Gesellschaft der EU massiven Schaden zufügen.

Die Cybersicherheit erhält damit eine neue Bedeutung. Ihre Ausgestaltung muss dabei ebenfalls den veränderten technologischen Rahmenbedingungen angepasst werden. Der Schwerpunkt ist in der Vorsorge und Wirksamkeit sowie in der Resilienz zu sehen. Auch der Gesetzgeber hat sich – pointiert formuliert – von der Vorstellung verabschiedet, dass Sicherheitsvorfälle stets verhindert werden können, und daher das Augenmerk expliziter auch (!) auf Maßnahmen zum Umgang mit und der Reaktion auf Sicherheitsvorfälle gerichtet.

Gerade in kritischen Sektoren ist die Cyber- und IT-Security eine entscheidende Voraussetzung, um den digitalen Wandel erfolgreich zu bewältigen und die wirtschaftlichen, sozialen und dauerhaften Vorteile der Digitalisierung voll zu nutzen.

1.1 NIS-2-Richtlinie und Umsetzung im BSI-Gesetz

Die Vorgaben von EU-Richtlinien können grundsätzlich ihre Wirkung nur entfalten, indem sie in einem nationalen Gesetz umgesetzt werden. **Die Stärkung des Schutzes der Netz- und Informationssysteme** erfolgt durch eine EU-Richtlinie, die **NIS-2-Richtline.** Anders als eine EU-Verordnung, wie beispielsweise DSGVO, DSA oder DA, gilt eine Richtlinie nicht unmittelbar in jedem EU-Mitgliedstaat.

In Deutschland sollte die Umsetzung durch das **Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)** erfolgen. Hierbei handelt(e) es sich um ein sog. Artikel-Gesetz. Denn es regelt in seinen verschiedenen Artikeln die Schaffung neuer Gesetze und die Änderung bestehender Gesetze. Der wesentliche Teil der Vorgaben der NIS-2-Richtlinie sollte im **Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informations-**

technik von Einrichtungen (BSI-Gesetz – BSIG) umgesetzt werden. Das bestehende BSIG sollt(e) hierzu grundlegend geändert werden.

Die **Umsetzung der Vorgaben der NIS-2-Richtlinie** musste **bis zum 17.10.2024** erfolgen und das nationale Gesetz hätte ab dem 18.10.2024 gelten müssen (Art. 41 Abs. 1 NIS-2-Richtlinie).

1.1.1 NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG-RegE) vom 02.10.2024 und Ende des Gesetzgebungsverfahrens

Der Gesetzentwurf der Bundesregierung des **NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes** (NIS2UmsuCG-RegE) wurde in seiner Fassung vom 02.10.2024 in das Gesetzgebungsverfahren eingebracht.[2] In seinem Artikel 1 enthält der NIS2UmsuCG-RegE den Regierungsentwurf für das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG) (BSIG-RegE).

Das Gesetzgebungsverfahren endete vor einer Verabschiedung des NIS2UmsuCG-RegE im Januar 2025. Aufgrund des **sog. Grundsatzes der Diskontinuität** muss das Gesetzgebungsverfahren nach der im Februar 2025 stattgefundenen Bundestagswahl erneut begonnen werden.

Aufgrund der konkreten Vorgaben der NIS-2-Richtline sind keine wesentlichen inhaltlichen Abweichungen des nationalen Umsetzungsgesetzes von der NIS-2-Richtlinie zu erwarten. Der deutsche Gesetzgeber ist nicht berechtigt, inhaltlich hinter den Vorgaben der NIS-2-Richtline zurückzubleiben, ist jedoch grundsätzlich nicht daran gehindert, über die Vorgabe der NIS-2-Richlinie hinauszugehen. Denn die NIS-2-Richtlinie sieht nur eine **sog. Mindestharmonisierung** vor (Art. 5 NIS-2-Richtlinie)[3].

Zum Zeitpunkt der Drucklegung wird mit Blick auf die Bundestagswahlen im Februar 2025 und die erforderliche Regierungsbildung mit dem **Inkrafttreten eines Umsetzungsgesetzes nicht vor dem 2. Halbjahr 2025** gerechnet. Ein Umsetzungsgesetz wird erfolgen, auch wenn zum Zeitpunkt der Drucklegung noch nicht sicher ist, wann das geschieht. Denn die EU-rechtliche Pflicht zur Umsetzung der NIS-2-Richtlinie bleibt bestehen.

---

[2] BT-Drs. 20/13184 vom 02.10.2024: Link mit Stand vom 31.01.2025: https://dserver.bundestag.de/btd/20/131/2013184.pdf

[3] „Diese Richtlinie hindert die Mitgliedstaaten nicht daran, Bestimmungen zu erlassen oder beizubehalten, die ein höheres Cybersicherheitsniveau gewährleisten, sofern diese Bestimmungen mit den Pflichten der Mitgliedstaaten nach dem Unionsrecht im Einklang stehen." (Art. 5 NIS-2-Richtlinie).

1.1.2 Was gilt in der Zwischenzeit? Auswirkungen auf die Praxis

EU-Richtlinien haben grundsätzlich keine horizontale unmittelbare Wirkung (EuGH, Urteil vom 05.04.1979, Rs. C-148/78 – Ratti, Urteil vom 04.12.1974, Rs. C-41/74 – van Duyn gegen Homeoffice). Eine horizontale unmittelbare Wirkung würde bedeuten, dass eine Person eine Vorschrift des EU-Rechts gegenüber einer anderen Person zu beachten hat bzw. geltend machen kann.

Mit anderen Worten und vereinfacht: Die Pflichten für die Verpflichteten entstehen nicht bereits mit dem Ablauf der Umsetzungsfrist der NIS-2-Richtlinie, sondern erst mit dem Geltungsbeginn des Umsetzungsgesetzes.



Tipp für die Praxis:
Nutzen Sie die Zeit, um die gesetzlichen Vorgaben umzusetzen.

Verlieren Sie Haftungsrisiken nicht aus dem Auge: Wenngleich keine staatlichen Zwangsmaßnahmen oder Sanktionen zur Durchsetzung der Vorgaben der NIS-2-Richtlinie drohen, kann es nicht mit abschließender Sicherheit ausgeschlossen werden, dass bei einem Vorfall ein Gericht einen Blick auf die Pflichten zum Risikomanagement führt, wenn es um die Bestimmung der Sorgfaltspflichten in einem Schadensersatzanspruch geht. Wenngleich hiergegen gute Argumente sprechen, ist die Entwicklung nicht sicher.

Kurzum: Legen Sie die Hände nicht in den Schoß!

In diesem Buch: Nachfolgend wird in diesem Buch auf das BSIG in der Fassung des Regierungsentwurfs vom 02.10.2024 (BSIG-RegE) abgestellt. Es ist naheliegend, dass im Gesetzgebungsverfahren aufgrund des Standes der Ausarbeitung des Entwurfs, des bestehenden Zeitdrucks zur Umsetzung mit Blick auf die am 17.10.2024 abgelaufene Umsetzungsfrist sowie die starke Ausrichtung des Entwurfs an der NIS-2-Richtlinie keine grundlegenden Änderungen erfolgen. Beachten Sie und verfolgen Sie gleichwohl das Gesetzgebungsverfahren und die Rechtsentwicklung.

1.2 Worum geht es?

Das BSIG-RegE umfasst 55 DIN-A5-Seiten (und die NIS-2-Richtlinie 73 DIN-A4-Seiten) und adressiert in seinen verschiedenen Teilen unterschiedliche Regelungsgegenstände und unterschiedliche Adressaten.

Tipp:
Verlieren Sie nicht den Überblick: Verschaffen Sie sich anhand des nachfolgenden Inhaltsverzeichnisses einen Überblick über das für Sie Wesentliche und Entscheidende!

Teil des BSIG-RegE	Paragraphen des BSIG-RegE	Regelungsinhalt	Anmerkungen
Teil 1	§§ 1–2	Allgemeine Vorschriften	Begriffsbestimmungen in § 2
Teil 2	§§ 3–27	Das Bundesamt	Dieser Teil regelt entsprechend der Bezeichnung des Gesetzes die Errichtung des Bundesamts für Sicherheit in der Informationstechnik.
Teil 3	§§ 28–8	Sicherheit in der Informationstechnik von Einrichtungen	Der Teil 3 regelt die Kernpflichten für die verpflichteten Einrichtungen. Das vorliegende Buch befasst sich daher im Wesentlichen mit diesen Regelungen.
Kapitel 1	§§ 28, 29	Anwendungsbereich	
Kapitel 2	§§ 30–42	Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten	➤ § 30 BSIG-RegE Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen ➤ § 31 BSIG-RegE Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen ➤ § 32 BSIG-RegE Meldepflichten ➤ § 33 BSIG-RegE Registrierungspflicht ➤ § 34 BSIG-RegE Besondere Registrierungspflicht für bestimmte Einrichtungsarten

Kapitel 2	§§ 30–42	Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten	➤ § 35 BSIG-RegE Unterrichtungspflichten ➤ § 36 BSIG-RegE Rückmeldungen des Bundesamts gegenüber meldenden Einrichtungen ➤ § 37 BSIG-RegE Ausnahmebescheid ➤ § 38 BSIG-RegE Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen ➤ § 39 BSIG-RegE Nachweispflichten für Betreiber kritischer Anlagen ➤ § 40 BSIG-RegE Nationale Verbindungsstelle sowie zentrale Melde- und Anlaufstelle für besonders wichtige und wichtige Einrichtungen ➤ § 41 BSIG-RegE Untersagung des Einsatzes kritischer Komponenten ➤ § 42 BSIG-RegE Auskunftsverlangen
Kapitel 3	§§ 43–48	Informationssicherheit der Einrichtungen der Bundesverwaltung	Diese Regelungen enthalten die Pflichten für Einrichtungen der Bundesverwaltung. Wer hierzu verpflichtet ist, ist in § 29 BSIG-RegE geregelt.
Teil 4	§§ 49–51	Datenbanken der Domain-Name-Registrierungsdaten	

Teil 5	§§ 52–55	Zertifizierung, Konformitäts-erklärung und Kennzeichen	
Teil 6	§§ 56–58	Verordnungs-ermächtigungen, Grundrechts-einschränkungen und Berichtspflichten	
Teil 7	§§ 59–64	Aufsicht	
Teil 8	§ 65	Bußgeldvorschriften	
Anlage 1		Sektoren besonders wichtiger und wichtiger Einrichtungen	Diese Anlagen zum Gesetz sind wichtig im Rahmen des § 28 BSIG-RegE zur Bestimmung der Einrichtungen, die die Pflichten nach dem BSIG-RegE einhalten müssen.
Anlage 2		Sektoren wichtiger Einrichtungen	

1.3 Zeitstrahl

Für den zeitlichen Ablauf ist nicht die Umsetzungsfrist der NIS-2-Richtlinie entscheidend (siehe oben Ziffer 1.1), sondern die des NIS2UmsuCG-RegE, die auch die Neuregelung im BSIG-RegE wirksam werden lässt. Art. 33 Abs. 1 NIS2UmsuCG-RegE sieht vor, dass die Regelungen am Tag nach der Verkündung anzuwenden sind und nicht nur in Kraft treten. Das NIS2UmsuCG-RegE sieht für das zukünftige BSIG keine Umsetzungsfrist vor.

Kurzum: Für die Erfüllung der Pflichten gibt es keine Übergangs- oder Umsetzungsfrist im nationalen Recht.

Aus der Begründung des Entwurfs des Umsetzungsgesetzes ergibt sich, dass der deutsche Gesetzgeber eine Übergangs- oder Umsetzungsfrist nicht für geboten hält, weil die verpflichteten Einrichtungen sich bereits seit Veröffentlichung der NIS-2-Richtlinie auf die Pflichten einstellen konnten.[4]

[4] BT-Drs. 20/23184 (Link siehe oben), Seite 178: „Als Inkrafttreten wird der Tag nach Verkündung

Die Befassung mit den Pflichten des BISG-RegE und der NIS-2-Richtlinie zeigt eindeutig, dass eine Vorbereitungszeit erforderlich ist und die Pflichten nicht aus dem Stegreif von „jetzt auf gleich" erfüllt werden können.

Tipp für die Praxis:
Handeln Sie jetzt!

1.4 Begrifflichkeiten und Definition

Der BSIG-RegE enthält in § 2 Begriffsbestimmungen, die – jedenfalls überwiegend – auf den Begriffsbestimmungen in Art. 6 NIS-2-Richtlinie beruhen. Diese Begriffsbestimmungen sind für die Auslegung und Anwendung des Gesetzes von grundlegender Bedeutung.

Sie müssen dabei beachten, dass diese vom allgemeinen oder dem in der IT üblichen Verständnis dieser Begriffe abweichen können. Sowohl der BSIG-RegE als auch die NIS-2-Richtlinie enthalten eine Definition des Begriffs „Cloud-Computing-Dienst" (§ 2 Nr. 4 BSIG-RegE, Art. 6 Nr. 30 NIS-2-Richtlinie) und „Managed Service Provider" (§ 2 Nr. 26 BSIG-RegE) bzw. „Anbieter verwalteter Dienste" (Art 6 Nr. 39 NIS-2-Richtlinie).

Tipp für die Praxis:
Machen Sie sich mit den gesetzlichen Definitionen vertraut. Beachten Sie, dass diese jeweils aus dem jeweiligen Rechtsakt heraus auszulegen sind).

Beachten Sie die Auswirkungen für die Vertragsgestaltung: Diese Definitionen können über das konkrete Gesetz hinaus Bedeutung erlangen. Werden sie beispielsweise in Verträgen verwendet und kommt es bei einem Vertrag zum Streit über das Verständnis des Begriffs, ist es nicht auszuschließen, dass zukünftig ein Gericht eine solche gesetzliche Definition zur Auslegung heranzieht.

2. Verpflichtete

Die Stellung als Verpflichteter regelt § 28 BSIG-RegE für die Privatwirtschaft und § 29 BSIG-RegE für die Bundesverwaltung. Aufgrund der föderalistischen Verteilung der Gesetzgebungskompetenz in Deutschland kann das BSIG-RegE nicht

festgelegt. Im Übrigen sind die für die Verpflichtungen von wesentlichen und besonders wichtigen Einrichtungen maßgeblichen Inhalte der NIS-2-Richtlinie bereits seit dem Kommissionsentwurf vom Dezember 2020 bekannt."

die Verpflichtungen in Bezug auf Einrichtungen der Länder und der Kommunalverwaltung regeln.

2.1 Verpflichtete der §§ 28, 29 BSIG-RegE

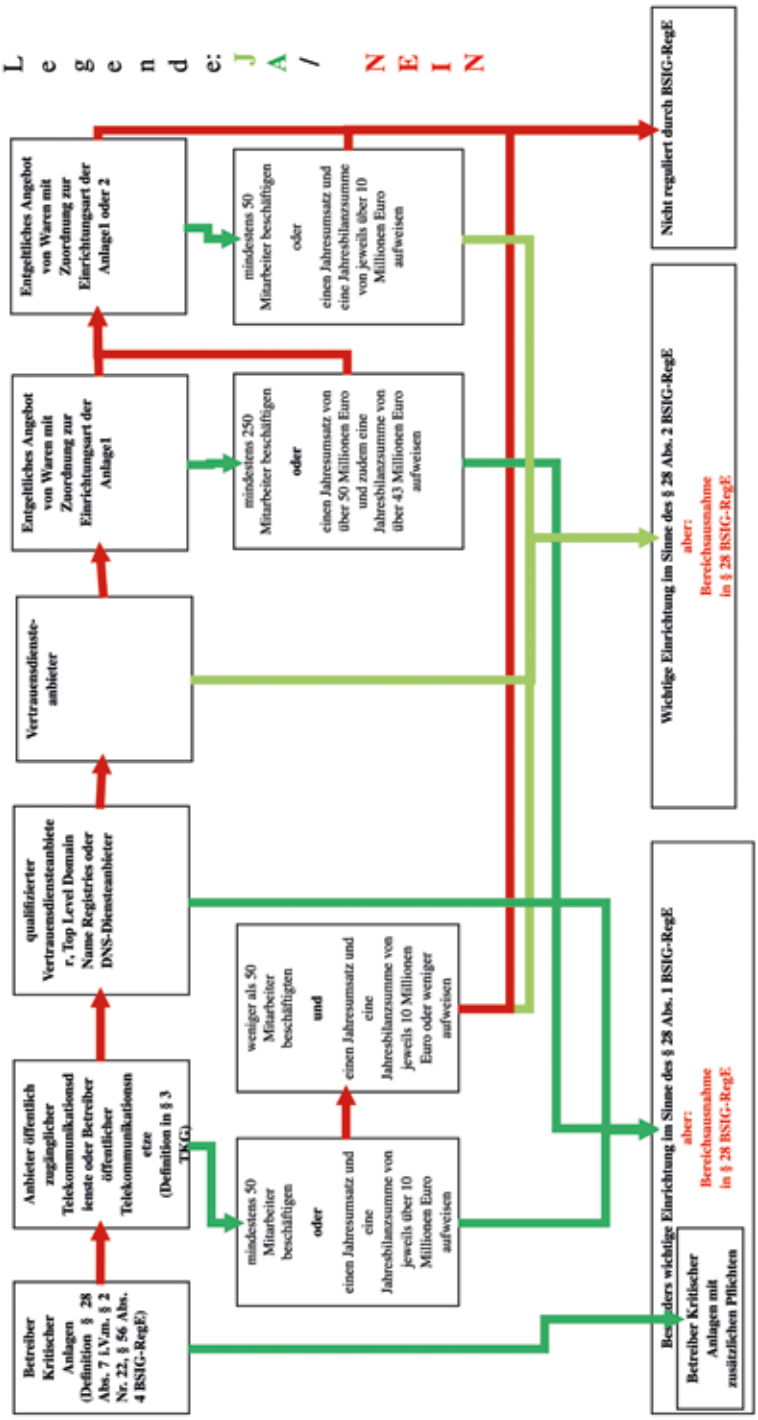
Das bisherige BSIG verpflichtete im Wesentlichen nur die Betreiber kritischer Infrastruktur. Die Neuregelung durch die NIS-2-Richtlinie führt zu einer signifikanten Erweiterung des Kreises der Verpflichteten.

Die Pflichtenstellung in der Privatwirtschaft wird unterschieden in **sog. besonders wichtige Einrichtungen (§ 28 Abs. 1 BSIG-RegE) (sog. wesentliche Einrichtungen, Art. 3 Abs. 1 NIS-2-Richtlinie)** und **sog. wichtige Einrichtungen (§ 28 Abs. 2 BSIG-RegE) (sog. wichtige Einrichtungen, Art. 3 Abs. 2 NIS-2-Richtlinie)**. Die Einzelheiten der Anforderungen ergeben sich aus § 28 BSIG-RegE in Verbindung mit den Anlagen 1 und 2 des BSIG-RegE.

Die Unterscheidung wirkt sich in Bezug auf die Pflichten nach §§ 30 bis 42 BSIG-RegE nicht wesentlich aus. Relevant ist die Unterscheidung in Bezug auf die Höhe der Geldbußen bei Verstößen. Besonders wichtige Einrichtungen werden (jedenfalls teilweise) härter für Verstöße sanktioniert.

Die **„Betreiber kritischer Anlagen“** sind besonders wichtige Einrichtungen gemäß § 28 Abs. 1 Nr. 1 BSIG-RegE. Für sie gelten aber zusätzlich einzelne spezielle Vorgaben (z. B. § 31 BSIG-ReG).

Das nachfolgende Schema soll Ihnen die Bewertung erleichtern. **Aber Achtung:** Ein Übersichtsschema soll nur die Durchführung der Prüfung anleiten, ersetzt aber infolge der damit einhergehenden Vereinfachung nicht die Prüfung anhand des Gesetzes!


Legende: JA / NEIN
Betreiber Kritischer Anlagen (Definition § 28 Abs. 7 i.V.m. § 2 Nr. 22, § 56 Abs. 4 BSIG-RegE)
Anbieter öffentlich zugänglicher Telekommunikationsd ienste oder Betreiber öffentlicher Telekommunikationsn etze (Definition in § 3 TKG)
qualifizierter Vertrauensdiensteanbiete r, Top Level Domain Name Registries oder DNS-Diensteanbieter
Vertrauensdienste-anbieter
Entgeltliches Angebot von Waren mit Zuordnung zur Einrichtungsart der Anlage1
Entgeltliches Angebot von Waren mit Zuordnung zur Einrichtungsart der Anlage1 oder 2
mindestens 50 Mitarbeiter beschäftigen
oder
einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen
weniger als 50 Mitarbeiter beschäftigten
und
einen Jahresumsatz und eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder weniger aufweisen
mindestens 250 Mitarbeiter beschäftigen
oder
einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen
mindestens 50 Mitarbeiter beschäftigen
oder
einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen
Besonders wichtige Einrichtung im Sinne des § 28 Abs. 1 BSIG-RegE
aber:
Bereichsausnahme in § 28 BSIG-RegE
Betreiber Kritischer Anlagen mit zusätzlichen Pflichten
Wichtige Einrichtung im Sinne des § 28 Abs. 2 BSIG-RegE
aber:
Bereichsausnahme in § 28 BSIG-RegE
Nicht reguliert durch BSIG-RegE

Für die Berechnung der Schwellenwerte ist zusätzlich § 28 Abs. 3 BSIG-RegE relevant.

Bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme nach § 28 Abs. 1 und Abs. 2 BSI-RegE ist auf **die der Einrichtungsart zuzuordnende Geschäftstätigkeit abzustellen und** – mit Ausnahme von rechtlich unselbstständigen Organisationseinheiten einer Gebietskörperschaft – die Empfehlung 2003/361/EG[5] mit Ausnahme von Artikel 3 Absatz 4 des Anhangs anzuwenden.

Die **Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung 2003/361/EG**[6] sind **nicht hinzuzurechnen, wenn** das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse unabhängig von seinen Partner- oder verbundenen Unternehmen ist.

2.2 Ausnahmen

Keine Regel ohne Ausnahme! Die Pflichtenstellung besteht nicht uneingeschränkt. In den Absätzen 4 bis 8 des § 28 BSIG-RegE sind Ausnahmen von den Pflichten vorgesehen. Zum Teil werden bestimmte Unternehmen insgesamt von den Pflichten des BSIG-RegE und bestimmte Unternehmen von einzelnen Pflichten des BSIG-RegE ausgenommen.

Nach § 28 Abs. 4 S. 1 BSIG-RegE gelten – abgesehen von der Rückausnahme in § 28 Abs. 4 S. 2 BSIG-RegE[7] – die §§ 30, 31, 32, 35, 36, 38, 39, 61 und 62 BSIG-RegE nicht für folgende besonders wichtige Einrichtungen und wichtige Einrichtungen, die

- ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen;

[5] Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32003H0361 (Stand: 28.10.2024))

[6] Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32003H0361 (Stand: 28.10.2024))

[7] § 28 Abs. 4 S. 2 BSIG-RegE: Satz 1 gilt nicht für die dort aufgeführten besonders wichtigen und wichtigen Einrichtungen, soweit sie über die in Satz 1 Nummer 1 und 2 genannten Anlagen hinaus weitere kritische Anlagen nach § 2 Nummer 22 betreiben oder aufgrund weiterer Tätigkeiten einer der in Anlage 1 oder 2 bestimmten Einrichtungsarten zuzuordnen sind. Satz 2 gilt für alle informationstechnischen Systeme, die für den Betrieb der weiteren kritischen Anlagen erforderlich sind.

- Energieversorgungsnetze oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes[8].

§ 28 Abs. 5 BSIG-RegE regelt für Finanzunternehmen und die Gesellschaft für Telematik nach § 306 Abs. 1 S. 3 des Fünften Buches Sozialgesetzbuch und Betreiber von Diensten der Telematikinfrastruktur Ausnahmen.

Nach § 28 Abs. 8 BSIG-RegE sind rechtlich unselbstständige Organisationseinheiten von Gebietskörperschaften und juristische Personen, an denen ausschließlich Gebietskörperschaften, ausgenommen der Bund, beteiligt sind, wenn sie 1. zu dem Zweck errichtet wurden, im öffentlichen Auftrag Leistungen für Verwaltungen zu erbringen, und 2. durch vergleichbare landesrechtliche Vorschriften unter Bezugnahme auf diesen § 28 Abs. 8 BSIG-RegE reguliert werden, generell ausgenommen.

§ 37 BSIG-RegE sieht zusätzlich vor, dass Unternehmen nach Maßgabe der dortigen Regelungen auf der Grundlage einer behördlichen Entscheidung insgesamt oder teilweise von den Pflichten ausgenommen werden können **(Ausnahmebescheid)**. Die Anforderungen hierfür sind hoch und die Entscheidung erfolgt durch das Bundesministerium des Innern und für Heimat.

2.3 Mittelbar Verpflichtete (Supply Chain)

Eine wesentliche Erweiterung des Kreises derjenigen, die die Pflichten nach dem BSIG-RegE bzw. der NIS-2-Richtlinie (mit-)umsetzen müssen, sind diejenigen, die als Lieferanten oder Dienstleister nach dem BSIG-RegE bzw. der NIS-2-Richtlinie tätig sind. Denn das BSIG-RegE und die NIS-2-Richtlinie zwingen die Verpflichteten dazu, nicht nur eigene Prozesse, sondern auch die Prozesse bei den eingebundenen Dritten zu bewerten.

§ 30 Abs. 2 Nr. 4 BSIG-RegE konkretisiert die nach § 30 Abs. 1 BSIG-RegE erforderlichen Maßnahmen wie folgt: „Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern".

Die Betonung des IKT-Drittparteienrisikos ist in der DORA unverkennbar ausgeprägter. In der Gesamtschau wird aber deutlich, dass der Gesetzgeber dazu zwingen will, dass die Sicherheitsbetrachtung nicht auf das unmittelbar selbst Beherrschte beschränkt bleibt, wodurch der Blick auf die Risiken zu sehr verengt

[8] Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 1 des Gesetzes vom 14. Mai 2024 (BGBl. 2024 I Nr. 161) geändert worden ist

würde. Denn die Auswirkung der Angriffe zeigt, dass diese zunehmend oder vor allem auch an der Lieferkette ansetzen.

Relevanz für die Praxis: Prüfen Sie als Dienstleister, ob Sie für Verpflichtete im Sinne des BSIG-RegE tätig sind, und stellen Sie sich darauf ein, dass Anforderungen an Sie gestellt werden. Sofern Ihr Auftraggeber sich noch nicht an Sie gewendet hat, treten Sie mit ihm in Kontakt, um dessen Pflichtenstellung zu klären sowie das Ob und Wie der Umsetzung der Pflichten abzustimmen.

Parallelität zur DS-GVO?

- Wenngleich sich Parallelen zur Auftragsverarbeitung (Art. 28 DS-GVO) und die Sicherheit der Verarbeitung (Art. 32 Abs. 1 und Abs. 4 DS-GVO) aufdrängen, sollten jedenfalls die Prüfung, die Festlegung und die Dokumentation der Maßnahmen getrennt erfolgen. Denn die DS-GVO und die NIS-2-Richtlinie verfolgen unterschiedliche Schutzziele. Das schließt nicht aus, dass bestimmte Anforderungen nach beiden Rechtsakten durch dieselben Maßnahmen umgesetzt werden können.
- Beachten Sie auch, dass nicht nur Auftragsverarbeiter mit den Pflichten nach Artt. 28, 32 DS-GVO Bestandteil der Lieferkette sein können, sondern auch ein Joint Controller Bestandteil der Lieferkette sein kann. Die Rollenverteilung nach dem BSIG-RegE und der DS-GVO sind nicht gleich.
- Beachten Sie auch, dass der Auftragsverarbeiter nach Art. 32 Abs. 1 DS-GVO unmittelbar und originär zur Sicherheit der Verarbeitung verpflichtet ist, während er dies nach dem BSIG-RegE nicht sein muss.

3. Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

Die Pflicht zum Risikomanagement ist in § 30 BSIG-RegE geregelt.

§ 30 Abs. 1 BSIG-RegE legt fest, dass die nach § 28 BSIG-RegE Verpflichteten geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen ergreifen müssen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten.

Eine Neuerung besteht darin, dass neben der Vermeidung explizit auf Maßnahmen zur Verringerung der Auswirkungen eines Vorfalls abgestellt wird. Auch hierin

wird deutlich, dass der Gesetzgeber davon ausgeht, dass es tatsächlich nicht mehr möglich ist, sicher Sicherheitsvorfälle zu vermeiden. Dementsprechend zwingt § 30 BSIG-RegE die Verpflichteten, sich mit den Auswirkungen von Sicherheitsvorfällen und Maßnahmen zu deren Eindämmung zu befassen und entsprechende Maßnahmen umzusetzen.

§ 30 Abs. 1 BSIG-RegE fordert die Wirksamkeit der Maßnahmen. Das wird dazu führen, dass die Zielerreichung der Maßnahmen ebenfalls zu überprüfen ist. Die Maßnahmen sind am Stand der Technik auszurichten, was sich aus § 30 Abs. 2 BSIG-RegE ergibt.

Die Pflicht steht nach § 30 Abs. 1 BSIG-RegE unter dem Vorbehalt der Verhältnismäßigkeit. Damit ist auch eine Berücksichtigung des Aufwands und der Kosten der Maßnahmen zulässig. § 30 Abs. 1 S. 2 BSIG-RegE konkretisiert diese Bewertung. Danach sind das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen.

§ 30 Abs. 2 BSIG-RegE enthält Konkretisierungen der Pflicht nach Abs. 1. Dabei sind die einschlägigen europäischen und internationalen Normen zu berücksichtigen. Aufgrund der bestehenden, etablierten Normen lässt sich bereits jetzt bestimmen, welche Anforderungen auch ein zukünftiges BSIG vorsehen wird. Die Maßnahmen müssen auch auf einem gefahrenübergreifenden Ansatz beruhen. § 30 Abs. 1 Satz 3 BSIG-RegE stellt klar, dass die Einhaltung der Pflichten zu dokumentieren ist **(Dokumentationspflicht)**. Dabei handelt es sich um eine interne Dokumentation. Diese Dokumentation ist grundsätzlich nicht Bestandteil der Registrierung nach § 33 BSIG-RegE **(Registrierungspflicht)**. § 39 BSIG-RegE sieht jedoch für Betreiber kritischer Anlagen (§ 28 Abs. 1 Nr. 1 BISG-RegE) vor, dass diese die Erfüllung ihrer Pflichten gegenüber dem BSI nachweisen müssen **(Nachweispflicht)**.

§ 30 Abs. 2 BSIG-RegE benennt 10 Mindestanforderungen („zumindest"):

- Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
- Bewältigung von Sicherheitsvorfällen,
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Be-

ziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,

- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik,
- Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen,
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

§ 30 Abs. 3 bis Abs. 9 BSIG-RegE sehen die Möglichkeit zur Konkretisierung insbesondere durch sog. Durchführungsrechtsakte der EU-Kommission vor. Eine Konkretisierung kann jedoch auch durch branchenspezifische Sicherheitsstandards erfolgen.

Die EU-Kommission hat beispielsweise die Durchführungsverordnung mit Durchführungsbestimmungen zur Richtlinie (EU) 2022/2555 im Hinblick auf die technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Präzisierung der Fälle, in denen ein Sicherheitsvorfall in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter als erheblich gilt, erlassen.

§ 30 Abs. 6 BSIG-RegE sieht vor, dass besonders wichtige Einrichtungen und wichtige Einrichtungen gemäß einer nach § 56 Abs. 3 BSIG-RegE erlassenen Rechtsverordnung bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse nur verwenden dürfen, wenn diese über eine Cyber-Sicherheitszertifizierung gemäß

europäischer Schemata nach Artikel 49 der Verordnung (EU) 2019/881 verfügen. Die Begriffe IKT-Produkte, IKT-Dienste und IKT-Prozesse sind in § 2 BSIG-RegE gesetzlich definiert.

4. Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen und Nachweispflichten für Betreiber kritischer Anlagen

Für Betreiber kritischer Anlagen gelten als besonders wichtige Einrichtungen im Sinne des § 28 Abs. 1 Nr. 1 BSIG-RegE alle für diese besonders wichtigen Einrichtungen geltenden Regelungen des BSIG-RegE. Für sie sind jedoch zusätzliche Regelungen insbesondere in §§ 31, 39 BSIG-RegE enthalten.

§ 31 Abs. 1 BSIG-RegE verschiebt das **Maß der Verhältnismäßigkeit** im Sinne des § 30 Abs. 1 BSIG-RegE für die Risikomanagementmaßnahmen. Das Gesetz trägt damit der herausragenden Bedeutung kritischer Anlagen Rechnung.

Durch § 31 Abs. 2 BSIG-RegE werden diese Betreiber auch explizit verpflichtet, **Systeme zur Angriffserkennung** einzusetzen, die geeigneten Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Dabei soll der Stand der Technik eingehalten werden. Der hierfür erforderliche Aufwand soll nach § 31 Abs. 2 S. 5 BSIG-RegE nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage stehen.

Für die Betreiber kritischer Anlagen sieht § 39 BSIG-RegE eine Pflicht zum Nachweis der Risikomanagementmaßnahmen vor **(Nachweispflicht)**. § 39 BSIG-RegE knüpft mit der Nachweispflicht an §§ 30, 31 BSIG-RegE an. Sie haben durch Sicherheitsaudits, Prüfungen oder Zertifizierungen die Umsetzung der Maßnahmen nach §§ 30 Abs. 1 S. 1, 31 Abs. 1, Abs. 2 S. 2 BSIG-RegE nachzuweisen. Der Nachweis muss frühestens nach drei Jahren und danach alle drei Jahre erfolgen. Die sonstigen Verpflichteten müssen sich zwar nach § 33 BSIG-RegE beim BSI registrieren, aber keinen Nachweis der Pflichterfüllung erbringen.

5. Meldepflichten sowie Befugnisse der Aufsichtsbehörde und Pflicht zur Unterstützung

Das BSIG-RegE sieht die Pflicht zur Meldung an das BSI für den Fall eines erheblichen Sicherheitsvorfalls vor. Daneben besteht auch eine Informationspflicht bei Cyberbedrohungen. In bestimmten Fällen müssen auch die Nutzer der betroffenen Dienste informiert werden.

Das BSIG-RegE sieht nur eine Pflicht zur Meldung der verpflichteten Einrichtungen vor. Anders als Art. 33 Abs. 2 DS-GVO besteht jedoch keine Pflicht eines Auftragnehmers der verpflichteten Einrichtung, diese zu informieren. Eine solche muss daher vertraglich vorgesehen werden und sollte Bestandteil des Risikomanagements sein (vgl. § 30 Abs. 2 Nr. 4 BSIG-RegE).

5.1 Meldepflichten

Für die nach § 28 Abs. 1 und Abs. 2 BSIG-RegE verpflichteten Einrichtungen besteht im Fall eines erheblichen Sicherheitsvorfalls die Meldepflicht nach § 32 BSIG-RegE. Die entsprechende Meldestelle wird durch das BSI und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe gemeinsam eingerichtet. Aus § 32 Abs. 1 S. 2 BSIG-RegE ergibt sich, dass die Meldepflicht nach § 32 Abs. 1 S. 1 BSIG-RegE erst ab Einrichtung des Meldewegs besteht.

Auslöser der Meldepflicht ist der **erhebliche Sicherheitsvorfall.** Ein „Sicherheitsvorfall" ist nach § 2 Nr. 40 BSIG-RegE „ein Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt". Achtung: Es kommt nicht darauf an, ob diese Daten personenbezogene Daten sind.

Ein „**erheblicher Sicherheitsvorfall"** ist nach § 2 Nr. 11 BSIG-RegE „ein Sicherheitsvorfall, der a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder b) andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann, sofern durch die Rechtsverordnung nach § 56 Absatz 5 keine konkretisierende Begriffsbestimmung erfolgt".

§ 32 BSIG-RegE sieht anders als § 168 TKG[9] und Artt. 33, 34 DS-GVO eine mehrstufige Meldepflicht vor.

[9] Hierzu: Geppert/Schütze/Eckhardt, TKG 5. Aufl., § 168 Rn. 1 ff.

Auslöser: Kenntniserlangung von einem erheblichen Sicherheitsvorfall			
Reihenfolge	**Zeitpunkt**	**Bezeichnung**	**Inhalt**
1.	unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall	**sog. frühe Erstmeldung** (§ 32 Abs. 1 S. 1 Nr. 1 BSIG-RegE)	Angabe, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte (gemäß § 32 Abs. 1 S. 1 Nr. 1 BSIG-RegE)
2.	unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall	**Meldung über diesen Sicherheitsvorfall** (§ 32 Abs. 1 S. 1 Nr. 2 BSIG-RegE)	Meldung über diesen Sicherheitsvorfall, in der die in Nummer 1 genannten Informationen bestätigt oder aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden (gemäß § 32 Abs. 1 S. 1 Nr. 2 BSIG-RegE)
3.	Verlangen des BSI	**sog. Zwischenmeldung,** **sofern durch BSI angefordert** (§ 32 Abs. 1 S. 1 Nr. 3 BSIG-RegE)	Zwischenmeldung über relevante Statusaktualisierungen (gemäß § 32 Abs. 1 S. 1 Nr. 3 BSIG-RegE)

4.	Dauert der Sicherheitsvorfall zum Zeitpunkt des § 32 Abs. 1 S. 1 Nr. 4 (Zeitpunkt der Abschlussmeldung) noch an	**sog. Fortschrittsmeldung** (§ 32 Abs. 2 BSIG-RegE) **anstatt** **Abschlussmeldung** (§ 32 Abs. 1 S. 1 Nr. 4 BSIG-RegE)	Fortschrittsmeldung (keine inhaltliche Konkretisierung durch § 32 Abs. 2 BSIG-RegE)
5.	spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Nummer 2 oder nach Ende des Sicherheitsvorfalls (§ 32 Abs. 2 BSIG-RegE)	**sog. Abschlussmeldung** (§ 32 Abs. 1 S. 1 Nr. 4 BSIG-RegE)	➤ eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen; ➤ Angaben zur Art der Bedrohung bzw. ihrer zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat; ➤ Angaben zu den getroffenen und laufenden Abhilfemaßnahmen; ➤ gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls. (gemäß § 32 Abs. 1 S. 1 Nr. 4 BSIG-RegE)

Nach § 32 Abs. 4 S. 1 BSIG-RegE legt das Bundesamt die Einzelheiten zur Ausgestaltung des Meldeverfahrens und zur Konkretisierung der Meldungsinhalte nach Anhörung der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe fest, soweit sie möglichen Durchführungsrechtsakten der Europäischen Kommission nicht widersprechen.

Die Informationen nach § 32 Abs. 4 S. 1 BSIG-RegE werden durch das Bundesamt auf dessen Internetseite veröffentlicht (§ 32 Abs. 4 S. 2 BSIG-RegE).

Für Betreiber kritischer Anlagen besteht die **zusätzliche Pflicht**, Angaben zur Art der betroffenen Anlage und der kritischen Dienstleistung sowie zu den Auswirkungen des Sicherheitsvorfalls auf diese Dienstleistung zu übermitteln, wenn ein erheblicher Sicherheitsvorfall Auswirkungen auf die von ihnen betriebene kritische Anlage hat oder haben könnte (§ 32 Abs. 3 BSIG-RegE).

Das **BSI** übermittelt der meldenden Einrichtung unverzüglich und nach Möglichkeit innerhalb von 24 Stunden eine **Bestätigung über den Eingang der Meldung** sowie auf Ersuchen der Einrichtung **Orientierungshilfen oder operative Beratung zu Abhilfemaßnahmen** (nach § 36 Abs. 1 S. 1 BSIG-RegE).

Auf Ersuchen der betreffenden Einrichtung kann das **BSI** zusätzlich auch **technische Unterstützung leisten** (§ 36 Abs. 1 S. 2 BSIG-RegE).

Anders als nach Art. 34 DS-GVO und § 168 TKG besteht nicht per se eine Pflicht, die von dem Sicherheitsvorfall Betroffenen zu unterrichten. **§§ 35, 36 BSIG-RegE sehen die Möglichkeit für das BSI zu entsprechenden Anordnungen vor (siehe unten).**

5.2 Pflicht zur Unterrichtung über eine erhebliche Cyberbedrohung

Für erhebliche Cyberbedrohungen ist in § 35 Abs. 2 BSIG-RegE eine eigenständige Pflicht zur Unterrichtung vorgesehen.

Verpflichtet sind wiederum die **Einrichtungen des § 28 Abs. 1 und 2** BSIG-RegE, aber nur wenn sie den **Sektoren Finanzwesen, Sozialversicherungsträger** sowie **Grundsicherung für Arbeitssuchende, digitale Infrastruktur, Verwaltung von IKT-Diensten** und **Digitale Dienste** angehören.

Für den Begriff **Cyberbedrohung** verweist § 2 Nr. 6 BSIG-RegE auf die Definition in Art. 2 Nr. 8 des Cybersecurity Act (CSA)[10]. Danach bezeichnet „Cyberbedrohung" „einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte". Eine Definition der Erheblichkeit erfolgt nicht. Für das BSIG-RegE kann auf die des § 2 Nr. 11 BSIG-RegE zurückgegriffen werden.

[10] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit, ABl. L 151 vom 7.6.2019, S. 15)

Die potenziell von einer erheblichen Cyberbedrohung betroffenen Empfänger der Dienste der verpflichteten Einrichtungen sind über die erhebliche Cyberbedrohung zu informieren **(Information über erhebliche Cyberbedrohung)** (§ 35 Abs. 1 S. 2 BSIG-RegE). Eine konkrete Betroffenheit muss, wie bereits der Begriff Bedrohung nahelegt, nicht gegeben sein, sondern es genügt die nicht ganz fernliegende Möglichkeit einer Betroffenheit.

Den Empfängern der Dienste der verpflichteten Einrichtungen und dem BSI müssen alle Maßnahmen oder Abhilfemaßnahmen mitgeteilt werden, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können **(Unterrichtung über alle Maßnahmen oder Abhilfemaßnahmen)** (§ 35 Abs. 1 S. 1 BSIG-RegE). Diese Regelung zielt darauf ab, Auswirkungen durch die Nutzer der Dienste (noch) zu verhindern. Die Information bzw. Unterrichtung hat **unverzüglich** zu erfolgen.

Auch für diese Pflichten gilt nach § 35 Abs. 2 S. 3 BSIG-RegE der **Vorbehalt der Verhältnismäßigkeit** („gelten nur dann, wenn in Abwägung der Interessen der Einrichtung und des Empfängers die Interessen des Empfängers überwiegen").

5.3 Anordnungen zur Unterrichtung und zur Information der Öffentlichkeit (§§ 35, 36 BSIG-RegE)

Im Fall eines erheblichen Sicherheitsvorfalls kann das BSI anordnen, dass die meldende Einrichtung die Empfänger ihrer Dienste unverzüglich über den erheblichen Sicherheitsvorfall, der die Erbringung des jeweiligen Dienstes beeinträchtigen könnte, unterrichtet.

§ 36 Abs. 2 BSIG-RegE sieht eine **Verpflichtung zur Information der Öffentlichkeit** vor. Wenn im Fall einer Meldung eines erheblichen Sicherheitsvorfalls eine Sensibilisierung der Öffentlichkeit erforderlich ist, um einen erheblichen Sicherheitsvorfall zu verhindern oder zu bewältigen, oder die Offenlegung des erheblichen Sicherheitsvorfalls anderweitig im öffentlichen Interesse liegt, kann das BSI die betreffende Einrichtung dazu verpflichten, die Öffentlichkeit über den erheblichen Sicherheitsvorfall zu informieren (§ 36 Abs. 2 S. 1 BSIG-RegE).

Stattdessen kann nach § 36 Abs. 2 S. 2 BSIG-RegE unter denselben Voraussetzungen auch durch das BSI eine Unterrichtung der Öffentlichkeit über den Sicherheitsvorfall erfolgen.

5.4 Verhältnis zur Melde- und Benachrichtigungspflicht nach Artt. 33, 34 DS-GVO, § 168 TKG

Die Meldepflichten nach dem BSIG-RegE sind nicht inhaltsgleich mit den Melde- und Benachrichtigungspflichten nach Artt. 33, 34 DS-GVO, § 168 TKG. Die

Schutzziele, die Verpflichteten, die Adressaten der Meldung bzw. Benachrichtigung und die Auslöser sind unterschiedlich. Aber ein Sicherheitsvorfall im Sinne des BSIG-RegE kann, muss aber nicht zugleich eine Verletzung des Schutzes personenbezogener Daten (Art. 4 Nr. 12, Artt. 33, 34 DS-GVO, § 168 TKG) darstellen. **Eine Meldung nach dem einen Gesetz ersetzt nicht die Meldung nach dem anderen Gesetz.** Beides muss daher eigenständig geprüft und bewertet sowie eigenständig an die jeweils zuständige Behörde gemeldet werden.

Tipp für die Praxis:

Eine Meldung nach BSIG-RegE und DS-GVO kann den gleichen tatsächlichen Auslöser haben, muss aber eigenständig geprüft und gemeldet werden.

Das BSI muss bei besonders wichtigen Einrichtungen und Einrichtungen der Bundesverwaltung die zuständigen Datenschutzaufsichtsbehörden unterrichten (§ 61 Abs. 11 BSIG-RegE, § 7 Abs. 8 BSIG-RegE): Stellt das BSI im Zuge der Beaufsichtigung einer Einrichtung oder Durchsetzung einer Maßnahme fest, dass ein Verstoß gegen die Verpflichtungen dieses Gesetzes eine offensichtliche Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DS-GVO zur Folge hat, die gemäß Art. 33 DS-GVO dieser Verordnung zu melden ist, unterrichtet es unverzüglich die zuständigen Aufsichtsbehörden.

6. Registrierungspflicht

§ 33 BSIG-RegE sieht für **besonders wichtige Einrichtungen** und **wichtige Einrichtungen** sowie **Domain-Name-Registry-Diensteanbieter** eine **Registrierungspflicht** vor. Die Pflichtangabe im Rahmen der **Registrierung** legen § 33 Abs. 1 und Abs. 2 BSIG-RegE fest. Ein Nachweis der Erfüllung einer Pflicht nach dem BSIG-RegE ist nicht Gegenstand dieser Registrierung. Wenn die Verpflichteten ihrer Registrierungspflicht jedoch nicht nachkommen, kann das BSI nach § 33 Abs. 3 BSIG-RegE die Registrierung selbst vornehmen. Das BSI und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe richten hierfür gemeinsam eine Registrierungsmöglichkeit ein.

Die Registrierung muss spätestens **drei Monate**, nachdem sie erstmals oder erneut als besonders wichtige Einrichtung und wichtige Einrichtung gelten oder Domain-Name-Registry-Dienste anbieten, erfolgen (**Frist zur Registrierung**).

Die Ausgestaltung des Registrierungsverfahrens erfolgt nach § 33 Abs. 6 BSIG-RegE durch das BSI im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz

und Katastrophenhilfe. Die Festlegung erfolgt durch eine öffentliche Mitteilung auf der Internetseite des Bundesamts.

Die **Vorlage von Nachweisen** kann das BSI nach § 33 Abs. 4 BSIG-RegE verlangen, wenn Tatsachen die Annahme rechtfertigen, dass eine Einrichtung ihre Pflicht zur Registrierung nach § 33 Abs. 1 und Abs. 2 BSIG-RegE nicht erfüllt. Gegenstand der Vorlagepflicht sind „die aus Sicht des Bundesamts für die Bewertung erforderlichen Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen und Auskunft zu erteilen, soweit nicht Geheimschutzinteressen oder überwiegende Sicherheitsinteressen entgegenstehen". Die Festlegung der vorzulegenden Unterlagen liegt danach beim BSI. Sie müssen sich auf die Bewertung der Pflicht zur Registrierung beziehen und umfassen nicht die Einhaltung der Pflichten der Einrichtungen.

§ 33 Abs. 5 BSIG-RegE sieht eine **Pflicht zur Aktualisierung** sowie **entsprechende Fristen** vor.

Eine sog. **besondere Registrierungspflicht** besteht für Einrichtungen der in § 60 Abs. 1 S. 1 BSIG-RegE genannten Einrichtungsart. Das sind **DNS-Diensteanbieter, Top Level Domain Name Registries, Domain-Name-Registry-Dienstleister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Content Delivery Networks, Managed Service Provider, Managed Security Service Provider** sowie für **Anbieter von Online-Marktplätzen, Online-Suchmaschinen** und **Plattformen für Dienste sozialer Netzwerke**. Der Inhalt der Registrierung wird durch § 34 Abs. 1 BSIG-RegE festgelegt. Die Registrierung muss binnen maximal drei Monaten erfolgen. Änderungen müssen unverzüglich, jedoch spätestens innerhalb von drei Monaten ab dem Tag, an dem die Änderung eingetreten ist, gemeldet werden (§ 34 Abs. 2 BSIG-RegE).

7. Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen

Eine Besonderheit ist in § 38 BSIG-RegE vorgesehen. Mit Blick auf eine Verschärfung der Haftung für die Unternehmensleitung wird die Ausgestaltung der Pflicht kontrovers diskutiert.

Für die Geschäftsleitung besonders wichtiger und wichtiger Einrichtungen im Sinne des § 28 BSIG-RegE besteht nach § 38 Abs. 1 BSIG-RegE die Pflicht, die von diesen Einrichtungen nach § 30 BSIG-RegE zu ergreifenden Risikomanagementmaßnahmen im Bereich der Cybersicherheit „umzusetzen und ihre Umsetzung zu überwachen". Der durch diese Regelung umzusetzende Art. 20 Abs. 1 NIS-2-RiLi

fordert (nur), dass die Leitungsorgane die zur Einhaltung des Art. 21 NIS-2-RiLi ergriffenen Risikomanagementmaßnahmen „billigen, ihre Umsetzung überwachen" und für Verstöße gegen Art. 21 NIS-2-RiLi durch die betreffenden Einrichtungen „verantwortlich gemacht werden können". Eine Pflicht zur Umsetzung geht über eine Billigung hinaus und könnte die Verantwortlichkeit verschärfen. Mit Blick auf die Formulierung in der NIS-2-RiLi ist die konkrete Ausgestaltung im Gesetz abzuwarten.

Hinweis für die Praxis: Die konkrete Ausgestaltung der Verantwortlichkeit ändert nichts daran, dass die Pflichten umzusetzen sind und bei einer Nichtumsetzung dennoch eine Haftung und Sanktionen drohen.

In diesem Kontext ist auch zu berücksichtigen, dass eine Haftung der Organe des Unternehmens auch nach bereits geltendem Recht ohnehin besteht (vgl. §§ 93 AktG, 43 GmbHG (analog), §§ 130, 30 OWiG sowie die sog. „Neubürger"-Entscheidung des LG München I (Urt. v. 10.12.2013, 5 HK O 1387/10l)).

§ 38 Abs. 2 S. 1 BSIG-RegE sieht einen Verweis auf die gesetzlichen Haftungsregelungen für die Geschäftsleitung vor (siehe vorstehend). Nach dem BSIG-RegE haftet die Geschäftsleitung nach § 38 Abs. 2 S. 2 BSIG-RegE (nur), wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung im Sinne des § 38 Abs. 1 S. 1 BSIG-RegE enthalten.

Die **Pflicht zur Schulung der Geschäftsleitung** des § 38 Abs. 3 BSIG-RegE Ist eine wesentliche Neuerung. Hierdurch entsteht im Ergebnis eine Verschärfung der Haftung:

> *„Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik und die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste zu erwerben."*

Mit Blick auf diese Schulungspflicht wird bei der Bewertung der Haftung danach zu fragen sein, ob die Geschäftsleitung überhaupt, ausreichend und aktualisiert geschult ist. Im Zweifel werden auch die Inhalte der Schulung und deren Durchführung hinterfragt werden, sodass eine „Feigenblatt-Schulung" ebenfalls ein Risiko darstellen kann.

8. Untersagung des Einsatzes kritischer Komponenten

Das BSIG-RegE sieht in seinem § 41 auch die Möglichkeit, den Betreibern kritischer Anlagen (siehe oben zu § 28 Abs. 1 Nr. 1 BSIG-RegE) den Einsatz kritischer Komponenten zu untersagen.

Eine solche **kritische Komponente** ist ein IKT-Produkt, das die in § 2 Nr. 23 BSIG-RegE genannten Kriterien erfüllt. Wesentliche Voraussetzung ist der Einsatz in einer kritischen Anlage.

Für den Begriff IKT-Produkt verweist § 2 Nr. 15 BSIG-RegE auf die Definition in Art. 2 Nr. 12 CSA (Cyber Security Act / Rechtsakt zur Cybersicherheit. Nach Art. 2 Nr. 12 CSA bezeichnet „IKT-Produkt" „ein Element oder eine Gruppe von Elementen eines Netz- oder Informationssystems".

Dieses muss die folgenden Kriterien des § 2 Nr. 23 Hs. 1 BSIG-RegE erfüllen, um eine sog. kritische Komponente zu sein: IKT-Produkte,

- die in kritischen Anlagen eingesetzt werden,
- bei denen Störungen der Verfügbarkeit, Integrität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit kritischer Anlagen oder zu Gefährdungen für die öffentliche Sicherheit führen können und
- die aufgrund eines Gesetzes unter Verweis auf diese Vorschrift als kritische Komponenten bestimmt werden oder eine aufgrund eines Gesetzes als kritisch bestimmte Funktion realisieren.

§ 2 Nr. 23 Hs. 2 BSIG-RegE sieht ergänzend vor: „Werden für einen der in Nummer 24 genannten Sektoren keine kritischen Komponenten und keine kritischen Funktionen, aus denen kritische Komponenten abgeleitet werden können, aufgrund eines Gesetzes unter Verweis auf diese Vorschrift bestimmt, so gibt es in diesem Sektor keine kritischen Komponenten im Sinne dieser Nummer."

§ 41 BSIG-RegE regelt aber nicht nur die Untersagung, sondern auch die Voraussetzungen, unter denen solche Komponenten überhaupt eingesetzt werden. Denn nicht jede kritische Komponente ist per se verboten, sondern § 40 BSIG-RegE schafft die Grundlage für Verbote durch behördliche Anordnung. Um etwas verbieten zu können, muss die Behörde zunächst Kenntnis erlangen. Dementsprechend ist das Verbot erst in Absatz 3 des § 40 BSIG-RegE geregelt.

Pflicht	Regelung	Inhalt
Anzeigepflicht in Bezug auf kritische Komponenten	§ 41 Abs. 1 BSIG-RegE	**Betreiber kritischer Anlagen** haben den geplanten erstmaligen Einsatz einer kritischen Komponente (§ 2 Nr. 23 BSIG-RegE) dem Bundesministerium des Innern und für Heimat vor ihrem Einsatz anzuzeigen. Die Garantieerklärung nach § 41 Abs. 3 BSIG-RegE muss der Anzeige beigefügt werden (§ 41 Abs. 3 S. 2 BSIG-RegE).
		Erst mit Ablauf einer **Frist von zwei Monaten** nach dieser Anzeige ist der Einsatz der kritischen Komponente gestattet (§ 41 Abs. 2 S. 3 BSIG-RegE). Diese Frist korrespondiert mit der Frist zur Untersagung der kritischen Komponente. Die Frist kann gegenüber der Einrichtung um weitere zwei Monate verlängert werden, wenn die Prüfung durch die Behörde besondere Schwierigkeiten tatsächlicher oder rechtlicher Art aufweist (§ 41 Abs. 2 S. 4 BSIG-RegE).
Garantieerklärung	§ 41 Abs. 3 BSIG-RegE	Kritische Komponenten dürfen nur unter den **Voraussetzungen des § 41 Abs. 3 BSIG-RegE** eingesetzt werden. Grundlegende Voraussetzung ist die Erklärung über seine Vertrauenswürdigkeit **(Garantieerklärung)** (§ 41 Abs. 3 S. 1 BSIG-RegE). Die Inhalte der Garantieerklärung ergeben sich insbesondere nach § 41 Abs. 3 S. 3 BSIG-RegE).
Untersagung	§ 41 Abs. 2 BSIG-RegE	**Nach Maßgabe des § 41 Abs. 3 BSIG-RegE** kann das Bundesministerium des Innern und für Heimat den geplanten erstmaligen Einsatz einer kritischen Komponente gegenüber dem Betreiber kritischer Anlagen bis zum Ablauf von zwei Monaten nach Eingang der Anzeige nach § 41 Abs. 1 BSIG-RegE untersagen oder Anordnungen erlassen.

9. Aufsicht, Kontrolle und Sanktionen

Das BSI ist nach § 59 BSIG-RegE die zuständige Aufsichtsbehörde für die Einhaltung der Vorschriften in Teil 3 (§§ 28–48 BSIG-RegE) durch wichtige und besonders wichtige Einrichtungen, die in der Bundesrepublik Deutschland niedergelassen sind, durch Betreiber kritischer Anlagen, deren kritische Anlagen sich auf dem Hoheitsgebiet der Bundesrepublik Deutschland befinden, und durch Einrichtungen der Bundesverwaltung. Damit wird auch der räumliche Anwendungsbereich bestimmt.

Daneben sieht § 60 BSIG-RegE die **Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten** vor. Für **DNS-Diensteanbieter, Top Level Domain Name Registries, Domain-Name-Registry-Dienstleister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Content Delivery Networks, Managed Service Provider, Managed Security Service Provider** sowie für **Anbieter von Online-Marktplätzen, Online-Suchmaschinen** oder **Plattformen für Dienste sozialer Netzwerke** ist das Bundesamt nach § 60 S. 1 BSIG-RegE nur dann zuständig, wenn diese ihre Hauptniederlassung im Sinne des § 60 Abs. 2 BSIG-RegE in der Europäischen Union in der Bundesrepublik Deutschland haben. Dann ist das BSI für die Einrichtung in der gesamten Europäischen Union zentral zuständig (§ 60 S. 2 BSIG-RegE). Hat eine solche Einrichtung keine Niederlassung in der Europäischen Union, bietet aber Dienste innerhalb der Europäischen Union an, so ist sie verpflichtet, einen Vertreter nach Maßgabe des § 60 Abs. 3 und 4 BSIG-RegE zu benennen.

Für die **Aufsichts- und Durchsetzungsmaßnahmen** unterscheidet das BSIG-RegE die besonders wichtigen Einrichtungen, für die umfangreiche Möglichkeiten in § 61 BSIG-RegE geregelt sind, und wichtige Einrichtungen (§ 62 BSIG-RegE). Für **Zuwiderhandlungen durch Institutionen der sozialen Sicherung** sieht § 64 BSIG-RegE eine Sonderregelung vor. Das sind nach **§ 2 Nr. 19 BSIG-RegE Körperschaften gemäß § 29 des SGB IV, Arbeitsgemeinschaften gemäß § 94 des Zehnten Buches Sozialgesetzbuch, die Deutsche Gesetzliche Unfallversicherung e. V. sowie die Deutsche Post AG, soweit sie mit der Berechnung oder Auszahlung von Sozialleistungen betraut ist.**

§ 65 BSIG-RegE regelt die Bußgelder. § 65 Abs. 1 bis 3 BSIG-RegE regeln die Sanktionen bei **Verstößen gegen die dort genannten Bestimmungen des BSIG-RegE**. § 65 Abs. 4 BSIG-RegE sieht **Geldbußen für Verstöße gegen Art. 55 Abs. 1 und Art. 56 Abs. 8 S. 1 CSA (Cyber Security Act)** vor.

Durch § 65 Abs. 5 BSIG-RegE ist der Bußgeldrahmen in fünf Stufen zwischen 100.000 Euro und 10 Mio. Euro abgestuft, wobei nach § 65 Abs. 5 Nr. 1 für Verstöße gegen § 35 Abs. 1 S. 1 oder § 36 Abs. 2 S. 1, § 30 Abs. 1 S. 1, S. 3, § 32 Abs. 1. S. 1, Abs. 2 S. 2 und § 35 Abs. 2 S. 1, 2 BSIG-RegE zwischen besonders wichtigen (bis zu 10 Mio. Euro nach § 65 Abs. 5 Nr. 1 Buchst. a BSIG-RegE) und wichtigen Einrichtungen (bis zu 7 Mio. Euro nach § 65 Abs. 5 Nr. 1 Buchst. b BSIG-RegE) in Bezug auf den Bußgeldrahmen unterschieden wird.

Bei einem Jahresumsatz von mehr als 500 Mio. Euro kann, abweichend von § 65 Abs. 5 S. 1 Nr. 1 BSIG-RegE, in den Fällen des § 65 Abs. 2 Nr. 1 Buchst. d, Nr. 2 bis 5 und 9 BSIG-RegE, bei besonders wichtigen Einrichtungen mit einer Geldbuße bis zu 2 % des Jahresumsatzes und bei wichtigen Einrichtungen mit einer Geldbuße bis zu 1,4 % des Jahresumsatzes geahndet werden (§ 65 Abs. 6, 7 BSIG-RegE).

Der Jahresumsatz ist der gesamte weltweit getätigte Umsatz des Unternehmens, dem die besonders wichtige Einrichtung oder die wichtige Einrichtung angehört, der in dem Geschäftsjahr erzielt wurde, das dem Verstoß vorangeht (§ 65 Abs. 8 BSIG-RegE). Zuständig ist das BSI (§ 65 Abs. 9 BSIG-RegE).

§ 65 Abs. 10 BSIG-RegE regelt das **Verhältnis zu Sanktionen nach der DS-GVO**. Verhängen die Datenschutzaufsichtsbehörden nach Art. 58 Abs. 2 lit. i DS-GVO ein Bußgeld, darf ein Bußgeld für einen Verstoß nach dem BSIG-RegE, der sich aus demselben Verhalten ergibt, nicht verhängt werden.

§ 56 BSIG-RegE enthält in seinen sechs Absätzen **Ermächtigungen** des Bundesministeriums des Innern und für Heimat **zum Erlass von Rechtsverordnungen** zur Konkretisierung verschiedener Aspekte des BSIG-RegE.

10. Verhältnis zur DS-GVO

Nach Erwägungsgrund 14 NIS-2-Richtlinie lässt die NIS-2-Richtlinie das Datenschutzrecht unberührt und ihre Pflichten müssen nach Erwägungsgrund 43 NIS-2-Richtlinie im Einklang mit dem Datenschutzrecht erfüllt werden.

Vorrang der DS-GVO: Soweit zur Erfüllung der Pflicht der NIS-2-Richtlinie und des nationalen Umsetzungsgesetzes personenbezogene Daten verarbeitet werden, müssen alle Vorgaben der DS-GVO eingehalten werden.

Beachten Sie in diesem Zusammenhang vor allem auch die Transparenzpflichten nach Artt. 12, 13, 14, 15 DS-GVO.

Für die Rechtsgrundlagen nach der DS-GVO ergeben sich Anhaltspunkte aus Erwägungsgrund 121 NIS-2-Richtlinie:

- ErwGr. 121 S. 1 NIS-2-RiLi sieht vor, dass Verarbeitung personenbezogener Daten durch die Verpflichteten „in dem zur Gewährleistung der Sicherheit von Netz- und Informationssystemen erforderlichen und verhältnismäßigen Umfang […] auf der Grundlage als rechtmäßig angesehen werden [kann], dass diese Verarbeitung einer rechtlichen Verpflichtung entspricht, der der Verantwortliche gemäß Artikel 6 Absatz 1 Buchstabe c und Artikel 6 Absatz 3 der Verordnung (EU) 2016/679 unterliegt". Wenngleich damit begründet werden kann, dass Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO die Rechtsgrundlage ist, ist zu beachten, dass die Verhältnismäßigkeit der Verarbeitung der konkreten personenbezogenen Daten zur Erreichung des Zwecks geprüft werden muss.
- Nach ErwGr. 121 S. 2 der NIS-2-RiLi „könnte" die Verarbeitung personenbezogener Daten auch für berechtigte Interessen der Verpflichteten sowie von Anbietern von Sicherheitstechnologien und -diensten, die im Namen der Verpflichteten handeln, erforderlich sein, „gemäß Artikel 6 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 wahrgenommen werden, auch wenn eine solche Verarbeitung für Vereinbarungen über den Informationsaustausch im Bereich der Cybersicherheit oder die freiwillige Mitteilung relevanter Informationen gemäß dieser Richtlinie erforderlich ist" (Zitat aus ErwGr. 121 S. 2 der NIS-2-RiLi). In seinem Urteil vom 04.10.2024, Rs. C-21/23, hat der EuGH instruktiv die Anforderungen an diese Abwägung der Interessen ausgeführt.

II. Digital Operational Resilience Act (DORA)

Die zunehmende Digitalisierung und Vernetzung verstärken das Risiko, für das Finanzsystem „Opfer" von Cyberbedrohungen oder IKT-Störungen zu werden (vgl. Erwägungsgrund 1 DORA). Während die allgegenwärtige Nutzung von IKT-Systemen und die hohe Digitalisierung und Konnektivität heute grundlegende Merkmale der Tätigkeiten von Finanzunternehmen der Union sind, muss ihre digitale Resilienz erst noch besser angegangen und in ihre allgemeinen operativen Rahmen integriert werden (Erwägungsgrund 1 DORA). Diesem Umstand tragen die Regelungen der DORA Rechnung.

1. Überblick

Mit der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor

und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 erfolgt eine Regelung der Cyber- und IT-Security im Bereich der Finanzwirtschaft.[11]

Im vorliegenden Buch wird die englische Bezeichnung *Digital Operational Resilience Act* (DORA) verwendet, um Missverständnisse in Bezug auf den deutschen Rechtsbegriff „Verordnung" zu vermeiden. DORA ist – anders als die NIS-2-Richtlinie – eine EU-Verordnung und gilt daher unmittelbar in jedem EU-Mitgliedstaat. Ein nationales Umsetzungsgesetz, wie beispielsweise das BSI-Gesetz, ist nicht erforderlich.

Die DORA wird in Deutschland durch das Gesetz über die Digitalisierung des Finanzmarktes (Finanzmarktdigitalisierungsgesetz – FinmadiG) ergänzt. Es enthält die im nationalen Recht auszuführenden Maßgaben der DORA und flankiert diese. Anders als das BISG ist dies **kein Umsetzungsgesetz** in Bezug auf die DORA. Denn die DORA gilt als EU-Verordnung direkt unmittelbar in jedem EU-Mitgliedstaat. FinmadiG insgesamt darüber der zusammengefassten Durchführung bzw. Umsetzung der Europäischen Verordnung MiCA (Markets in Crypto Assets, Verordnung (EU) 2023/1114), der Neufassung der EU-Geldtransferverordnung (Transfer of Funds Regulation, Verordnung (EU) 2023/1113) sowie des europäischen **DORA-Pakets (Digital Operational Resilience Act, Verordnung (EU) 2022/2554 und Richtlinie (EU) 2022/2556)**.

Für die Umsetzung der Vorgaben der DORA sind die **Delegierten Rechtsakte** und **Durchführungsstandards zu DORA** sowie **gemeinsamen Leitlinien (Level 2 und 3)** von entscheidender praktischer Bedeutung. Diese entwickeln sich stetig fort. Einen Überblick erhalten Sie auf den **Internetseiten der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)** und insbesondere hier: https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html (Link mit Stand: 07.02.2025)

1.1 Worum geht es?

Der DORA besteht aus 64 Artikeln und 106 Erwägungsgründen und hat einen Textumfang von 79 DIN-A4-Seiten. Der DORA adressiert in seinen verschiedenen Teilen unterschiedliche Regelungsgegenstände und unterschiedliche Adressaten. Die EU-Rechtsakte haben – anders als typischerweise deutsche Gesetze – kein Inhaltsverzeichnis, was eine schnelle Orientierung erschwert.

[11] Quelle: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554 (Link mit Stand: 30.01.2025)

Ausgehend von der Bezeichnung der Verordnung (siehe vorstehend Ziffer 1) lässt sich anhand der Definition zentraler Begriffe das Regelungsziel verdeutlichen:

Das wesentliche **Ziel, die „digitale operationale Resilienz",** wird in Art. 3 Nr. 1 DORA definiert als „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-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".

Es soll dem **IKT-Risiko** begegnet werden. Als „IKT-Risiko" definiert Art. 3 Nr. 5 DORA „jeden vernünftigerweise identifizierbaren Umstand im Zusammenhang mit der Nutzung von Netzwerk- und Informationssystemen, der bei Eintritt durch die damit einhergehenden nachteiligen Auswirkungen im digitalen oder physischen Umfeld die Sicherheit der Netzwerk- und Informationssysteme, jeglicher technologieabhängiger Instrumente oder Prozesse, von Geschäften und Prozessen oder der Bereitstellung von Diensten beeinträchtigen kann".

Um ein hohes gemeinsames Niveau an digitaler operationaler Resilienz zu erreichen, werden in der DORA einheitliche Anforderungen für die Sicherheit von Netzwerk- und Informationssystemen, die die Geschäftsprozesse von Finanzunternehmen unterstützen, wie folgt festgelegt (Art. 1 Abs. 1 DORA):

Tipp

Verlieren Sie nicht den Überblick: Verschaffen Sie sich anhand des nachfolgenden Inhaltsverzeichnisses einen Überblick über das für Sie Wesentliche und Entscheidende!

Kapitel der DORA	Artikel der DORA	Regelungsinhalt	Anmerkungen
I	Artt. 1–4	Allgemeine Bestimmungen	
II	Artt. 5–16	IKT-Risikomanagement	ACHTUNG: Pflicht des Leitungsorgans des Finanzunternehmens (Art. 5 Abs. 2 DORA)
	Art. 5	Abschnitt I	Governance und Organisation
	Artt. 6–16	Abschnitt II	IKT-Risikomanagementrahmen
III	Artt. 17–23	Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle	
IV	Artt. 24–27	Testen der digitalen operationalen Resilienz	
V	Artt. 28–44	Management des IKT-Drittparteienrisikos	
	Artt. 28–30	Abschnitt I	Schlüsselprinzipien für ein solides Management des IKT-Drittparteienrisikos
	Artt. 31–44	Abschnitt II	Überwachungsrahmen für kritische IKT-Drittdienstleister
VI	Art. 45	Vereinbarungen über den Austausch von Informationen	
VII	Artt. 46–56	Zuständige Behörden	
VIII	Art. 57	Delegierte Rechtsakte	
IX	Artt. 58–64	Übergangs- und Schlussbestimmungen	
	Art. 58	Abschnitt I	Überprüfungsklausel
	Artt. 59–64	Abschnitt II	Änderungen

1.2 Zeitstrahl

Inkrafttreten	Anwendungsbeginn
Januar 2023	17.01.2025 (Art. 64 DORA)

1.3 Begrifflichkeiten und Definitionen

Die DORA enthält in ihrem Art. 3 Begriffsbestimmungen. Diese Begriffsbestimmungen sind für die Auslegung und Anwendung des Gesetzes von grundlegender Bedeutung. Die DORA nimmt zum Teil auch Bezug auf Definitionen in anderen EU-Rechtsakten (z. B. in Art. 3 Nr. 2 DORA für den Begriff „Netzwerk- und Informationssystem" auf Artikel 6 Nr. 1 NIS-2-Richtlinie).

Sie müssen dabei beachten, dass diese vom allgemeinen oder in der IT üblichen Verständnis dieser Begriffe abweichen können. Die DORA enthält beispielsweise eine Definition des Begriffs „Cyberangriff" in Art. 3 Nr. 14 DORA und benennt diesen als „einen böswilligen IKT-bezogenen Vorfall, der auf den Versuch eines Angreifers zurückgeht, einen Vermögenswert zu zerstören, freizulegen, zu verändern, zu deaktivieren, zu entwenden oder auf unberechtigte Weise auf diesen Vermögenswert zuzugreifen oder ihn auf unberechtigte Weise zu nutzen".

Tipp für die Praxis

Machen Sie sich mit den gesetzlichen Definitionen vertraut. Beachten Sie, dass diese jeweils aus dem jeweiligen Rechtsakt heraus auszulegen sind.

Beachten Sie die Auswirkungen für die Vertragsgestaltung: Diese Definitionen können über das konkrete Gesetz hinaus Bedeutung erlangen. Werden sie beispielsweise in Verträgen verwendet und kommt es für den Vertrag zum Streit über das Verständnis des Begriffs, ist es nicht auszuschließen, dass zukünftig ein Gericht eine solche gesetzliche Definition zur Auslegung heranzieht.

2. Verpflichtete

Der Anwendungsbereich und der Kreis der Verpflichteten werden durch Art. 2 DORA festgelegt. Verpflichtete sind Finanzunternehmen (Art. 2 Abs. 2 i. V. m. Abs. 1 lit. a bis lit. t DORA) sowie IKT-Drittdienstleister (Art. 2 Abs. 1 lit. u DORA).

Nach **Art. 2 Abs. 2 DORA** werden die in Art. 2 Abs. 1 lit. a bis lit. t DORA genannten Unternehmen in der DORA unter dem Begriff **Finanzunternehmen zusammengefasst.** Erfasst sind nicht nur Banken, sondern auch Versicherungen und weitere Unternehmen.

Im Einzelnen sind das (Art. 2 Abs. 1 lit. a bis lit. t DORA): a) Kreditinstitute, **b)** Zahlungsinstitute, einschließlich gemäß der Richtlinie (EU) 2015/2366 ausgenommene Zahlungsinstitute, **c)** Kontoinformationsdienstleister, **d)** E-Geld-Institute, einschließlich gemäß der Richtlinie 2009/110/EG ausgenommene E-Geld-Institute, **e)** Wertpapierfirmen, **f)** Anbieter von Krypto-Dienstleistungen, die gemäß einer Verordnung des Europäischen Parlaments und des Rates über Märkte von Krypto-Werten und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937 (im Folgenden „Verordnung über Märkte von Krypto-Werten") zugelassen sind, und Emittenten wertreferenzierter Token, **g)** Zentralverwahrer, **h)** zentrale Gegenparteien, **i)** Handelsplätze, **j)** Transaktionsregister, **k)** Verwalter alternativer Investmentfonds, **l)** Verwaltungsgesellschaften, **m)** Datenbereitstellungsdienste, **n)** Versicherungs- und Rückversicherungsunternehmen, **o)** Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, **p)** Einrichtungen der betrieblichen Altersversorgung, **q)** Ratingagenturen, **r)** Administratoren kritischer Referenzwerte, **s)** Schwarmfinanzierungsdienstleister und **t**) Verbriefungsregister.

Die nach Art. 2 Abs. 1 lit. u DORA verpflichteten **IKT-Drittdienstleister** sind in **Art. 3 Nr. 19 DORA** definiert als **„**Unternehmen, die IKT-Dienstleistungen bereitstellen". Solche „**IKT-Dienstleistungen**" sind nach **Art. 3 Nr. 21 DORA** „digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen, wozu auch technische Unterstützung durch den Hardwareanbieter mittels Software- oder Firmware-Aktualisierungen gehört, mit Ausnahme herkömmlicher analoger Telefondienste".

Achtung – Unterschied zur NIS-2-Richtlinie und BSIG-RegE: Die DORA nimmt die „IKT-Drittdienstleister" selbst in die Pflicht und sieht eigenständige Pflichten vor. Die Lieferkette wird durch die NIS-2-Richtlinie und BSIG-RegE nur mittelbar in die Pflicht genommen.

Art. 2 Abs. 3 DORA regelt Ausnahmen von der DORA. Nach Art. 2 Abs. 3 lit. e DORA gilt die DORA beispielsweise nicht für Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, bei denen es sich um Kleinstunternehmen oder kleine oder mittlere Unternehmen handelt.

Hinweis

Prüfen Sie sorgfältig anhand von Art. 2 DORA, ob die DORA einschlägig ist. Denn einerseits ist der Anwendungsbereich in Abs. 1 weiter, als vielleicht erwartet wird, und andererseits können Unternehmen durch Abs. 3 ausgenommen sein, die nach dem weiten Anwendungsbereich des Abs. 1 eigentlich einbezogen werden. Kurzum: Beachten Sie das Regel-Ausnahme-Schema des Art. 2 DORA.

Die Verpflichteten können zugleich auch in den Anwendungsbereich der NIS-2-Richtlinie bzw. des BSIG-RegE fallen. Durch **§ 28 Abs. 5 Nr. 1 BSIG-RegE** sind für Finanzunternehmen im Sinne des Art. 2 Abs. 2 DORA und für Unternehmen, für die die Anforderungen der DORA aufgrund von § 1a Abs. 2 des Kreditwesengesetzes (KWG) oder § 293 Abs. 5 des Versicherungsaufsichtsgesetzes (VAG) gelten, **Ausnahmen von einzelnen Regelungen des BSIG-RegE** vorgesehen – nicht anzuwenden sind demnach §§ 30, 31, 32, 35, 36, 38 und 39 BSIG-RegE.

3. Pflichten zum IKT-Risikomanagement

Die Maßgaben der DORA zum IKT-Risikomanagement lassen sich in fünf Elemente zur Zielerreichung zusammenfassen. Der Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen nach Art. 45 DORA regelt zusätzlich die freiwillige Möglichkeit zum Austausch von Informationen über Cyberbedrohungen.

Die DORA und die NIS-2-Richtlinie verfolgen beide das Ziel, die Cyber Security und IT Security vor allem mit Blick auf eine Resilienz zu stärken. Die **DORA ist im Vergleich zur NIS-2-Richtlinie** umfassender und detailtiefer geregelt. Das bedeutet einerseits zwar weniger Spielräume bei der Erfüllung der Vorgaben andererseits auch weitergehende Klarheit für die Umsetzung der Pflichten.

3.1 Governance und Organisation (Art. 5 DORA)

Finanzunternehmen müssen über einen internen **Governance- und Kontrollrahmen** verfügen, der ein wirksames und umsichtiges Management von IKT-Risiken gewährleistet, um ein hohes Niveau an digitaler operationaler Resilienz zu erreichen (Art. 5 Abs. 1 DORA). Art. 5 DORA verweist darauf, dass dieser im Einklang mit Art. 6 Abs. 4 DORA (IKT-Risikomanagementrahmen) stehen muss.

Die DORA betont die **Verpflichtung und Verantwortung der Leitungsorgane** für die Einhaltung der Vorgaben der DORA. Das Leitungsorgan des Finanzunternehmens – so Art. 5 Abs. 2 UAbs. 1 DORA wörtlich definiert – genehmigt, überwacht und verantwortet die Umsetzung aller Vorkehrungen im Zusammenhang

mit dem IKT-Risikomanagementrahmen nach Artikel 6 Absatz 1. Der Begriff Leitungsorgan ist in Art. 3 Nr. 30 DORA unter Bezugnahme auf weitere EU-Richtlinien definiert. Art. 5 Abs. 2 UAbs. 2 DORA konkretisiert dies mit neun konkreten Anforderungen an das Leitungsorgan, die letztlich die in der DORA im Weiteren festgelegten Anforderungen aufgreifen.

Art. 16 DORA sieht Ausnahmen für kleinere und nicht verflochtene Finanzunternehmen vor (hierzu nachfolgend bei Artt. 6 bis 16 DORA).

3.2 IKT-Risikomanagementrahmen (Artt. 6–16 DORA)

Finanzunternehmen müssen über einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen verfügen. Dieser muss Teil ihres Gesamtrisikomanagementsystems sein und es ihnen ermöglichen, IKT-Risiken schnell, effizient und umfassend anzugehen und ein hohes Niveau an digitaler operationaler Resilienz zu gewährleisten (Art. 6 Abs. 1 DORA).

<table>
<tr><td colspan="2">Art. 6 Abs. 1 DORA steckt mit seinen Vorgaben die Pflichten und Maßgaben ab.</td></tr>
<tr><td rowspan="9">Die Konkretisierung erfolgt in Artt. 6–16 DORA:</td><td>IKT-Risikomanagementrahmen (Art. 6 DORA)</td></tr>
<tr><td>IKT-Systeme, -Protokolle und -Tools (Art. 7 DORA)</td></tr>
<tr><td>Identifizierung (Art. 8 DORA)</td></tr>
<tr><td>Schutz und Prävention (Art. 9 DORA)</td></tr>
<tr><td>Erkennung (Art. 10 DORA)</td></tr>
<tr><td>Reaktion und Wiederherstellung (Art.11 DORA)</td></tr>
<tr><td>Richtlinie und Verfahren zum Backup sowie Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung (Art. 12 DORA)</td></tr>
<tr><td>Lernprozesse und Weiterentwicklung (Art. 13 DORA)</td></tr>
<tr><td>Kommunikation (Art. 14 DORA)</td></tr>
<tr><td>Harmonisierung von Tools, Methoden, Prozessen und Richtlinien für IKT-Risikomanagement (Art. 15 DORA)</td></tr>
<tr><td colspan="2">Art. 16 DORA sieht für die dort genannten kleineren und nicht verflochtenen Finanzunternehmen die Befreiung von Artt. 5–15 DORA vor. Art. 16 Abs. 1 UAbs. 2 DORA legt für diese ausgenommenen Finanzunternehmen eigenständig acht Maßgaben zum IKT-Risikomanagement vor.</td></tr>
</table>

Der **IKT-Risikomanagementrahmen** umfasst nach **Art. 6 Abs. 2 DORA** mindestens Strategien, Leit- und Richtlinien, Verfahren sowie IKT-Protokolle und -Tools, die erforderlich sind, um alle Informations- und IKT-Assets, einschließlich Computer-Software, Hardware und Server, ordnungsgemäß und angemessen zu schützen sowie um alle relevanten physischen Komponenten und Infrastrukturen, wie etwa Räumlichkeiten, Rechenzentren und ausgewiesene sensible Bereiche, zu schützen, damit der angemessene Schutz aller Informations- und IKT-Assets vor Risiken, einschließlich der Beschädigung und des unbefugten Zugriffs oder der unbefugten Nutzung, gewährleistet ist.

Der **IKT-Risikomanagementrahmen** muss nach **Art. 6 Abs. 5 DORA** mindestens einmal jährlich bzw. im Fall von Kleinstunternehmen regelmäßig sowie bei Auftreten schwerwiegender IKT-bezogener Vorfälle und nach aufsichtsrechtlichen Anweisungen oder Feststellungen, die sich aus einschlägigen Tests der digitalen operationalen Resilienz oder Auditverfahren ergeben, dokumentiert und überprüft werden. Der Rahmen wird auf der Grundlage, der bei Umsetzung und Überwachung gewonnenen Erkenntnisse kontinuierlich verbessert. Der zuständigen Behörde wird auf deren Anfrage ein Bericht über die Überprüfung des IKT-Risikomanagementrahmens vorgelegt.

Art. 6 Abs. 8 DORA adressiert die **Umsetzung der definierten Maßnahmen**: Der IKT-Risikomanagementrahmen umfasst eine Strategie für die digitale operationale Resilienz, in der dargelegt wird, wie der Rahmen umgesetzt wird. Zu diesem Zweck schließt die Strategie für die digitale operationale Resilienz Methoden, um IKT-Risiken anzugehen und spezifische IKT-Ziele zu erreichen, ein. Hierzu werden in Art. 6 Abs. 8 DORA acht Maßnahmen vorgegeben.

3.3 Behandlung, Klassifizierung und Berichterstattung von IKT-Vorfällen (Artt. 17–23 DORA)

Die Artt. 17–23 DORA regeln die Reaktion und den Umfang auf mit **IKT-bezogene Vorfälle** und **Cyberbedrohungen**. Die Regelungen sind deutlich umfangreicher und ausgeprägter als in der NIS-2-Richtlinie bzw. dem BSIG-RegE und der DS-GVO.

Die zentrale Pflicht kommt in Art. 17 Abs. 1, Abs. 2 DORA zum Ausdruck. Finanzunternehmen bestimmen einen Prozess für die Behandlung IKT-bezogener Vorfälle, richten diese ein und wenden sie an, um IKT-bezogene Vorfälle zu erkennen, zu behandeln und zu melden (Art. 17 Abs. 1 DORA). Finanzunternehmen erfassen alle IKT-bezogenen Vorfälle und erheblichen Cyberbedrohungen. Finanzunternehmen richten angemessene Verfahren und Prozesse ein, um die kohärente und integrier-

te Überwachung, Handhabung und Weiterverfolgung IKT-bezogener Vorfälle zu gewährleisten, um sicherzustellen, dass Ursachen ermittelt, dokumentiert und angegangen werden, um das Auftreten solcher Vorfälle zu verhindern (Art. 17 Abs. 2 DORA). Die weiteren Ausprägungen erfolgen durch die weiteren Regelungen in Artt. 17 bis 23 DORA.

Ein solcher „IKT-bezogener Vorfall" ist nach Art. 3 Nr. 8 DORA ein von dem Finanzunternehmen nicht geplantes Ereignis bzw. eine entsprechende Reihe verbundener Ereignisse, das bzw. die die Sicherheit der Netzwerk- und Informationssysteme beeinträchtigen und nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder auf die vom Finanzunternehmen erbrachten Dienstleistungen haben. Das Abstellen auf ein nicht geplantes Ereignis zeigt deutlich, dass die Pflicht niederschwelliger ist als in der NIS-2-Richtlinie bzw. dem BSIG-RegE und der DS-GVO.

Art. 17 Abs. 2 S. 1 DORA nimmt auch erhebliche Cyberbedrohungen in Bezug. Diese werden in den Artt. 17–23 DORA nicht den IKT-bezogenen Vorfällen gleichgestellt. Art. 2 Nr. 12 DORA nimmt für die Bestimmung des Begriffs „Cyberbedrohung" auf Art. 2 Nr. 8 CSA (Verordnung (EU) 2019/881) Bezug und nicht auf die NIS-Richtlinie.

Danach bezeichnet „Cyberbedrohung" „einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte". Eine „erhebliche Cyberbedrohung" ist nach Art. 3 Nr. 13 DORA „eine Cyberbedrohung, deren technische Merkmale darauf hindeuten, dass sie das Potenzial haben könnte, einen schwerwiegenden IKT-bezogenen Vorfall oder einen schwerwiegenden zahlungsbezogenen Betriebs- oder Sicherheitsvorfall zu verursachen".

3.4 Test der digitalen operationalen Resilienz (Artt. 24–27 DORA)

Nach Art. 24 DORA muss ein solides und umfassendes Programm für das Testen der digitalen operationalen Resilienz als integraler Bestandteil des in Artikel 6 DORA genannten IKT-Risikomanagementrahmens gepflegt und überprüft werden.

Dies muss erfolgen, um die Vorbereitung auf die Handhabung IKT-bezogener Vorfälle zu bewerten, Schwächen, Mängel und Lücken in Bezug auf die digitale operationale Resilienz zu erkennen und Korrekturmaßnahmen umgehend umzusetzen (Art. 24 Abs. 1 DORA). Die nachfolgenden Artikel der DORA konkretisieren diese Pflicht und gestalten sie aus.

3.5 Management des IKT-Drittparteienrisikos (Artt. 28–44 DORA)

Ein Schwerpunkt der DORA im Vergleich zu Vorgängerregelungen ist die Betrachtung und die Einbeziehung des sog. IKT–Drittparteienrisikos in die Maßnahmen zum IT-Risikomanagement. Die Vorgaben sind im Kapitel V der DORA (Artt. 28–44 DORA) geregelt. Das ist rund ein Viertel des Textumfangs der DORA (rund 20 der 79 DIN-A4-Seiten), was den Schwerpunkt ebenfalls verdeutlicht.

Ein solches IKT-Drittparteienrisiko ist nach Art. 3 Nr. 18 DORA ein IKT-bezogenes Risiko, das für ein Finanzunternehmen im Zusammenhang mit dessen Nutzung von IKT-Dienstleistungen entstehen kann, die von IKT-Drittdienstleistern oder deren Unterauftragnehmern, einschließlich über Vereinbarungen zur Auslagerung, bereitgestellt werden. IKT-Dienstleistungen definiert Art. 3 Nr. 21 DORA als digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen, wozu auch technische Unterstützung durch den Hardwareanbieter mittels Software- oder Firmware-Aktualisierungen gehört, mit Ausnahme herkömmlicher analoger Telefondienste. Ein Unternehmen, das IKT-Dienstleistungen bereitstellt, ist nach Art. 3 Nr. 19 DORA der „IKT-Drittdienstleister".

Die Artt. 28 ff. DORA regeln Schlüsselprinzipien für ein solides Management des IKT-Drittparteienrisikos.

Finanzunternehmen müssen das IKT-Drittparteienrisiko als integralen Bestandteil des IKT-Risikos innerhalb ihres IKT-Risikomanagementrahmens nach Art. 6 Abs. 1 DORA handhaben. Art. 28 Abs. 1 DORA legt die dafür geltenden Prinzipien wie folgt fest:

- Finanzunternehmen, die vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen für die Ausübung ihrer Geschäftstätigkeit getroffen haben, bleiben jederzeit in vollem Umfang für die Einhaltung und Erfüllung aller Verpflichtungen nach dieser Verordnung und nach dem anwendbaren Finanzdienstleistungsrecht verantwortlich.
- Beim Management des IKT-Drittparteienrisikos tragen Finanzunternehmen dem Grundsatz der Verhältnismäßigkeit Rechnung, wobei Folgendes zu berücksichtigen ist: die Art, das Ausmaß, die Komplexität und die Relevanz IKT-bezogener Abhängigkeiten sowie die Risiken infolge vertraglicher Vereinbarungen über die Nutzung von IKT-Dienstleistungen, die mit IKT-Drittdienstleistern geschlossen wurden, wobei die Kritikalität oder Relevanz der jeweiligen Dienstleistungen, Prozesse oder Funktionen sowie die potenziellen

Auswirkungen auf die Kontinuität und Verfügbarkeit von Finanzdienstleistungen und -tätigkeiten auf Einzel- und Gruppenebene zu berücksichtigen sind.

Art. 30 DS-GVO regelt **formale und inhaltliche Anforderungen an den Vertrag zur Beauftragung von IKT-Drittparteien.** Art. 30 Abs. 2 DORA gibt neun Mindestinhalte eines solchen Vertrags vor. Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen müssen zusätzlich die sechs Mindestinhalte des Art. 28 Abs. 2 DORA umfassen.

Hinweis

Die Verträge von Finanzunternehmen oder mit Finanzunternehmen über die Erbringung von IKT-Drittdienstleistungen müssen nach Maßgabe des Art. 30 DORA geprüft und überarbeitet werden.

Den **Überwachungsrahmen für kritische IKT-Drittdienstleister regeln die Artt. 31 ff. DORA.**

3.6 Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen (Art. 45 DORA)

Finanzunternehmen können auf freiwilliger Basis Informationen und Erkenntnisse über Cyberbedrohungen untereinander austauschen, einschließlich Indikatoren für Beeinträchtigungen, Taktiken, Techniken und Verfahren, Cybersicherheitswarnungen und Konfigurationstools (Art. 45 DORA). Art. 45 Abs. 1 DORA regelt drei Maßgaben für einen solchen Austausch. Staatliche Instanzen müssen dabei nicht zwingend beteiligt sein (vgl. Art. 45 Abs. 2 DORA). Die sich beteiligenden Finanzunternehmen müssen ihre Beteiligung der für sich zuständigen Behörde – auch das Ende einer solchen Beteiligung – mitteilen (Art. 45 Abs. 3).

Aus Erwägungsgrund 34 DORA ergibt sich als Hintergrund, dass Finanzunternehmen ermutigt werden sollen, Informationen und Erkenntnisse zu Cyberbedrohungen untereinander auszutauschen und ihre individuellen Kenntnisse und praktischen Erfahrungen auf strategischer, taktischer und operativer Ebene gemeinsam zu nutzen, damit sich ihre Fähigkeit verbessert, Cyberbedrohungen angemessen zu bewerten, zu überwachen, abzuwehren und auf sie zu reagieren, indem sie an Vereinbarungen über den Austausch von Informationen teilnehmen.

Gleichzeitig wird in Erwägungsgrund 34 DORA und Art. 45 Abs. 1 lit. c DORA klargestellt, dass dieser Informationsaustausch mit den Regelungen gegen Wettbewerbsbeschränkungen und dem Datenschutzrecht in Einklang stehen muss.

Mit anderen Worten: Diese Zielsetzung des Informationsaustausches ist kein „Freifahrtschein".

4. Sanktionen

Die DORA regelt selbst nicht direkt Geldbußen bei Verstößen gegen die Pflichten. In Art. 35 DORA ist der Rahmen für Zwangsgelder zur Erzwingung der Erfüllung der Pflichten vorgesehen. Zwangsgelder sind jedoch Maßnahmen der Vollstreckung und nicht der Sanktionierung. Das ist relevant, weil klassisch rechtlich vertreten wird, dass Zwangsgelder eine (zusätzliche) Sanktion nicht ausschließen. Durch nationales Recht können insbesondere strafrechtliche Sanktionen vorgesehen werden (Art. 50 ff. DORA). Die weitergehenden Sanktionen sind in den nationalen Durchführungsrechtsakten (siehe oben Ziffer 1) vorgesehen.

5. Verhältnis zur DS-GVO

Die DORA enthält keine generelle Aussage zum Verhältnis zum Datenschutzrecht. Lediglich beim freiwilligen Informationsaustausch zur Abwehr von Cyberbedrohungen (Art. 45 Abs. 1 lit. c DORA) und für die Datenverarbeitung durch die ESA und die zuständigen Behörden (Art. 56 Abs. 1 S. 2 DORA) wird klargestellt, dass dies im Einklang mit der DS-GVO erfolgen muss.

Die DS-GVO wird damit nicht generell verdrängt und muss natürlich beachtet werden. Gerade Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO kommt als Rechtsgrundlage für die Verarbeitung personenbezogener Daten in Betracht. Wenn es dennoch im Einzelfall zu einem nicht auflösbaren Konflikt zwischen DS-GVO und DORA kommt, wird sich (vermutlich) die DORA als jüngere EU-Rechtsverordnung durchsetzen. Dieses Verhältnis ist jedoch bei Weitem noch nicht abschließend geklärt, sodass die Rechtsprechung hierzu abzuwarten ist.



© WrightStudio – Adobe Stock.com

Trotz DORA bleibt die DSGVO relevant – wie sich beide Regelwerke zueinander verhalten, ist jedoch noch nicht abschließend geklärt.

III. Cyber Resilience ACT (CRA)

1. Überblick

Mit der Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung) erfolgt eine Regelung der Cybersicherheit in Bezug auf digitale Produkte.

Im vorliegenden Buch wird die englische Bezeichnung **Cyber Resilience Act** oder **CRA** verwendet, um Missverständnisse mit Blick auf den deutschen Rechtsbegriff „Verordnung" zu vermeiden.

1.1 Worum geht es?

Der CRA besteht aus 71 Artikeln, 130 Erwägungsgründen sowie 8 Anhängen und hat einen Textumfang von 81 DIN-A4-Seiten.

Der CRA ist – anders als die NIS-2-Richtlinie – eine EU-Verordnung und gilt daher unmittelbar und direkt in jedem EU-Mitgliedstaat. Ein Umsetzungsgesetz wie etwa das BSIG bedarf es nicht. Gleichwohl können Durchführungsrechtsakte im nationalen Recht erfolgen wie zum Beispiel die Festlegung der nationalen Aufsichtsbehörde.

Der CRA regelt die Bereitstellung von Produkten mit digitalen Elementen, um die Cybersicherheit solcher Produkte zu gewährleisten, grundlegende Cybersicherheitsanforderungen an die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Produkte hinsichtlich der Cybersicherheit, grundlegende Cybersicherheitsanforderungen an die von den Herstellern festgelegten Verfahren zur Behandlung von Schwachstellen, um die Cybersicherheit von Produkten mit digitalen Elementen während der erwarteten Nutzungsdauer der Produkte zu gewährleisten, sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Verfahren und die Marktüberwachung, einschließlich Überwachung, und die Durchsetzung der in diesem Artikel genannten Vorschriften und Anforderungen.

Die EU-Rechtsakte haben – anders als typischerweise deutsche Gesetze – kein Inhaltsverzeichnis, was eine schnelle Orientierung erschwert.

Tipp

Verlieren Sie nicht den Überblick: Verschaffen Sie sich anhand des nachfolgenden Inhaltsverzeichnisses einen Überblick über das für Sie Wesentliche und Entscheidende!

Kapitel	Artikel des CRA	Regelungsinhalt	
I	Artt. 1–12 CRA	Allgemeine Bestimmungen	
II	Artt. 13–26 CRA	Pflichten der Wirtschaftsakteure und Bestimmungen in Bezug auf freie und quelloffene Software	
III	Artt. 27–34 CRA	Konformität des Produkts mit digitalen Elementen	
IV	Artt. 35–51 CRA	Notifizierung von Konformitätsbewertungstellen	
V	Artt. 52–60 CRA	Marktüberwachung und Durchsetzung	
VI	Art. 61–62 CRA	Übertragene Befugnisse und Ausschussverfahren	
VII	Artt. 63–65 CRA	Vertraulichkeit und Sanktionen	Art. 65 CRA regelt die Verbandsklage bei Verstößen gegen den CRA.
VIII	Art. 66–71 DORA	Übergangs- und Schlussbestimmungen	

1.2 Zeitstrahl

Inkrafttreten	Anwendungsbeginn		
Dezember 2024	11.09.2026 für Art. 14 CRA	11.06.2026 für Kapitel IV (Artt. 35–51 CRA)	11.12.2027 (Art. 71 Abs. 2 CRA)

1.3 Begrifflichkeiten und Definitionen

Der CRA enthält in seinem Art. 3 Begriffsbestimmungen. Diese Begriffsbestimmungen sind für die Auslegung und Anwendung des Gesetzes von grundlegender Bedeutung.

Sie müssen dabei beachten, dass diese vom allgemeinen oder in der IT üblichen Verständnis dieser Begriffe abweichen können. Der Art. 3 Nr. 2 CRA enthält beispielsweise eine Definition des Begriffs „Datenfernverarbeitung", Art. 3 Nr. 3 CRA eine Definition des Begriffs „Cybersicherheit" und Art. 3 Nr. 7 CRA eine Definition des Begriffs „elektronisches Informationssystem".

Tipp für die Praxis

Machen Sie sich mit den gesetzlichen Definitionen vertraut. Beachten Sie, dass diese jeweils aus dem jeweiligen Rechtsakt heraus auszulegen sind.

Beachten Sie die Auswirkungen für die Vertragsgestaltung: Diese Definitionen können über das konkrete Gesetz hinaus Bedeutung erlangen. Werden sie beispielsweise in Verträgen verwendet und kommt es für den Vertrag zum Streit über das Verständnis des Begriffs, ist es nicht auszuschließen, dass zukünftig ein Gericht eine solche gesetzliche Definition zur Auslegung heranzieht.

2. Anwendungsbereich

Der CRA gilt für auf dem Markt bereitgestellte Produkte mit digitalen Elementen, deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt (Art. 1 Abs. 1 CRA). Der CRA ist – letztlich wie der AI Act – Produktsicherheitsrecht.

Die zentrale Relevanz für die Bestimmung der Anwendung des CRA ist das „**Produkt mit digitalen Elementen**". Das sind nach der Definition in Art. 3 Nr. 1 CRA „ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden".

In den Absätzen 2 bis 8 des Art. 2 CRA wird umfassend aufgelistet, für welche Produkte mit digitalen Elementen der CRA nicht, sondern andere Rechtsakte zur Anwendung kommen.

Hinweis

Prüfen Sie grundlegend den Anwendungsbereich des Art. 2 Abs. 1 CRA und vor allem auch seine Ausnahmen in den Absätzen 2 bis 8 des Art. 2 CRA.

3. Allgemeine Bestimmungen (Artt. 1–12 CRA)

Die allgemeinen Bestimmungen in Artt. 1–12 CRA regeln nicht nur Zweck, Anwendungsbereich und Begriffsbestimmungen des CRA, sondern enthalten auch grundlegende Regelungen.

3.1 Produkte mit digitalen Elementen

Die grundlegende Regelung ist in Art. 6 CRA enthalten: **Produkte mit digitalen Elementen** werden nur dann auf dem Markt bereitgestellt, wenn

- sie den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I genügen und unter der Bedingung, dass sie ordnungsgemäß installiert, gewartet und bestimmungsgemäß oder unter vernünftigerweise vorhersehbaren Umständen verwendet werden sowie gegebenenfalls die erforderlichen Sicherheitsaktualisierungen installiert wurden;
- die vom Hersteller festgelegten Verfahren den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil II entsprechen.

Für sog. **wichtige Produkte mit digitalen Elementen** enthält Art. 7 CRA weitere Regelungen. Produkte mit digitalen Elementen, die die Kernfunktionen einer in Anhang III aufgeführten Produktkategorie aufweisen, gelten als wichtige Produkte mit digitalen Elementen (Art. 7 Abs. 1 CRA).

Art. 8 CRA adressiert sog. **kritische Produkte mit digitalen Elementen**.

3.2 Hochrisiko-KI-Systeme (Art. 12 CRA)

Art. 12 CRA enthält eine Sonderregelung zu Art. 15 AI Act für Produkte mit digitalen Elementen, die in den Anwendungsbereich des CRA fallen und die gemäß Art. 6 AI Act als Hochrisiko-KI-Systeme eingestuft werden.

4. Pflichten der Wirtschaftsakteure und Bestimmungen in Bezug auf freie und quelloffene Software (Artt. 13–26 CRA)

Der CRA nimmt die gesamte Wertschöpfungskette der Produkte mit digitalen Elementen in die Pflicht. Art. 3 Nr. 12 CRA definiert den Begriff „Wirtschaftsakteure" und zeigt damit den Kreis der Verpflichteten auf. „Wirtschaftsakteur" bezeichnet danach den Hersteller, den Bevollmächtigten, den Einführer, den Händler oder jede andere natürliche oder juristische Person, die Verpflichtungen im Zusammenhang mit der Herstellung von Produkten mit digitalen Elementen oder der Bereitstellung auf dem Markt von Produkten mit digitalen Elementen im Einklang mit dieser Verordnung unterliegt.

Die Artt. 13–26 CRA legen dann für den jeweiligen Wirtschaftsakteur entsprechend seiner Stellung in der Wertschöpfungskette Pflichten auf. Besondere Pflichten der Verwalter quelloffener Software regelt Art. 24 CRA.

Zentrale Adresse der Pflichten ist der Hersteller. „Hersteller" ist nach Art. 3 Nr. 13 CRA eine natürliche oder juristische Person, die Produkte mit digitalen Elementen entwickelt oder herstellt oder die Produkte mit digitalen Elementen konzipieren, entwickeln oder herstellen lässt und sie unter ihrem Namen oder ihrer Marke vermarktet, sei es gegen Bezahlung, zur Monetarisierung oder unentgeltlich.

Artt. 21 und 22 CRA regeln Konstellationen, in denen andere Wirtschaftsakteure ebenfalls die für Händler geltenden Pflichten zu beachten haben. Eine ähnliche Regelung enthält Art. 25 AI Act.

5. Sanktionen

Die Sanktion im Fall von Verstößen gegen den CRA regelt sein Art. 64.

Der CRA enthält gestufte Geldbußen:	
Nichteinhaltung der in Anhang I festgelegten grundlegenden Cybersicherheitsanforderungen oder **Verstoß gegen die in den Artt. 13 und 14 CRA** festgelegten Pflichten	Geldbußen bis zu 15 Mio. Euro oder im Fall von Unternehmen von bis zu 2,5 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher Betrag höher ist, möglich (Art. 64 **Abs. 2** CRA)
Verstößen gegen die Pflichten der Artt. 18–23, Art. 28, Art. 30 Abs. 1–4, Art. 31 Abs. 1–4, Art. 32 Abs. 1, 2 und 3, Art. 33 Abs. 5 und Artt. 39, 41, 47, 49 und 53 CRA	Geldbußen bis zu 10 Mio. Euro oder im Fall von Unternehmen von bis zu 2 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher Betrag höher ist, möglich (Art. 64 **Abs. 3** CRA)

falsche, unvollständige oder irreführende **Angaben gegenüber notifizierten Stellen und Marktüberwachungsbehörden** auf deren Auskunftsverlangen	Geldbußen bis zu 5 Mio. Euro oder im Fall von Unternehmen von bis zu 1 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher Betrag höher ist, möglich (Art. 64 **Abs. 4** CRA)

EXKURS: Auch wenn es keine Sanktion ist, ist darauf hinzuweisen, dass **Art. 65 CRA** die **Verbandsklage bei Verletzung der Pflichten des CRA** vorsieht: Richtlinie (EU) 2020/1828 über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der Richtlinie 2009/22/EG findet Anwendung auf Verbandsklagen gegen Zuwiderhandlungen durch Wirtschaftsakteure gegen Bestimmungen dieser Verordnung, die die Kollektivinteressen der Verbraucher beeinträchtigen oder zu beeinträchtigen drohen.

6. Verhältnis zur DS-GVO

Erwägungsgrund 32 verweist darauf, dass durch den Schutz von Verbrauchern und Organisationen vor Cybersicherheitsrisiken, die im CRA festgelegten grundlegenden Cybersicherheitsanforderungen auch dazu beitragen sollen, den Schutz personenbezogener Daten und den Schutz der Privatsphäre natürlicher Personen zu verbessern.

Im Übrigen ist in Erwägungsgrund 32 CRA jedoch ausgeführt, dass der CRA unbeschadet der DS-GVO gilt. Die DS-GVO wird damit nicht generell verdrängt und muss natürlich beachtet werden. Gerade Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO kommt als Rechtsgrundlage für die Verarbeitung personenbezogener Daten in Betracht. Wenn es dennoch im Einzelfall zu einem nicht auflösbaren Konflikt zwischen DS-GVO und CRA kommt, wird sich (vermutlich) die DORA als jüngere EU-Rechtsverordnung durchsetzen. Dieses Verhältnis ist jedoch bei Weitem noch nicht abschließend geklärt, sodass die Rechtsprechung hierzu abzuwarten ist.

B. DIGITAL SERVICES ACT MIT DIGITAL MARKETS ACT

Der Digital Services Act (DSA) und der Digital Markets Act (DMA) adressieren die Anbieter von Digital Services.

I. DIGITAL SERVICES ACT

Ziel des DSA ist es, durch die Festlegung harmonisierter Vorschriften für ein sicheres, vorhersehbares und vertrauenswürdiges Online-Umfeld, in dem Innovationen gefördert und die in der Charta verankerten Grundrechte, darunter der Grundsatz des Verbraucherschutzes, wirksam geschützt werden, einen Beitrag zum reibungslosen Funktionieren des Binnenmarkts für Vermittlungsdienste zu leisten (Art. 1 Abs. 1 DSA).

1. Überblick

Mit der Verordnung (EU) **2022/2065** des Europäischen Parlaments und des Rates vom **vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste)** erfolgt eine Regelung der Dienste der Informationsgesellschaft, damit das Online-Umfeld sicher, berechenbar und vertrauenswürdig ist und in der EU einheitlich geregelt ist.

Im vorliegenden Buch wird die englische Bezeichnung **Digital Services Act** oder **DSA** verwendet, um Missverständnisse mit Blick auf den deutschen Durchführungsrechtsakt in Gestalt des Digitale-Dienste-Gesetz (DDG) zu vermeiden.

Der DSA ist – anders als etwa die NIS-2-Richtlinie – eine EU-Verordnung und gilt daher unmittelbar und direkt in jedem EU-Mitgliedstaat. Ein Umsetzungsgesetz bedarf es also nicht. Gleichwohl können Durchführungsrechtsakte im nationalen Recht erfolgen wie zum Beispiel die Festlegung der nationalen Aufsichtsbehörde:

Das **deutsche Digitale-Dienste-Gesetz (DDG)** ist die Nachfolgeregelung zum alten Telemediengesetz (TMG-alt). Der DSA ersetzt die bisherigen Regelungen über die Haftung für Inhalte im TMG, sodass diese im TMG-alt obsolet wurden. Weitere Regelungen wie beispielsweise die Impressumspflicht, die in TMG-alt enthalten waren und auf der sog. E-Commerce-Richtlinie beruhen, müssen im nationalen Recht weiterhin geregelt werden. Auch dies erfolgt im DDG. Darüber hinaus hat sich der deutsche Gesetzgeber von dem Begriff Telemediendienst ver-

abschiedet und stellt EU-rechtskonform auf „digitaler Dienst" im Sinne des Art. 1 Abs. 1 lit. b der Richtlinie (EU) 2015/153 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft ab. Eine **Folgeänderung** war die Änderung des Telekommunikations-Telemedien-Datenschutz-Gesetzes (TTDSG) in **Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG)**. Eine materielle Änderung der Regelungen ist dadurch nicht erfolgt. Durch das Abstellen auf digitale Dienste anstatt auf die nur in Deutschland definierten Telemedien ergeben sich jedoch Änderungen im Anwendungsbereich.

1.1 Worum geht es?

Der DSA besteht aus 93 Artikeln und 156 Erwägungsgründen und hat einen Textumfang von 102 DIN-A4-Seiten. Der DSA adressiert in seinen verschiedenen Teilen unterschiedliche Regelungsgegenstände und unterschiedliche Adressaten. Die EU-Rechtsakte haben – anders als typischerweise deutsche Gesetze – kein Inhaltsverzeichnis, was eine schnelle Orientierung erschwert.

Der DSA hat ein umfangreiches Regelungsspektrum insbesondere: Schutz vor missbräuchlicher Verwendung der Plattform, Transparenzpflichten bei Empfehlungssystemen, Pflicht zur Löschung illegaler Inhalte „im Internet", Anzeigepflicht bei schweren Straftaten, Schadensersatz bei DSA-Verstößen, Transparenz in Bezug auf Monetarisierung von Daten, Verbot von personalisierter Werbung mit Daten von Minderjährigen sowie Profiling von Minderjährigen und Verboten von personalisierter Werbung mittels besonderer Kategorien personenbezogener Daten.

Der DSA hat Folgendes zum Gegenstand (Art. 1 Abs. 2 DSA):

- „Rechtsrahmen für die bedingte Haftungsbefreiung der Anbieter von Vermittlungsdiensten;
- besondere Sorgfaltspflichten, die auf bestimmte Kategorien von Anbietern von Vermittlungsdiensten zugeschnitten sind;
- Vorschriften über die Durchführung und Durchsetzung dieser Verordnung, einschließlich der Zusammenarbeit und Koordinierung zwischen den zuständigen Behörden."

Tipp

Verlieren Sie nicht den Überblick: Verschaffen Sie sich anhand des nachfolgenden Inhaltsverzeichnisses einen Überblick über das für Sie Wesentliche und Entscheidende!

Kap.	Artikel des DSA	Regelungs-inhalt	Erläuterung zur Differenzierung der Verpflichteten
I	Artt. 1–3 DSA	Allgemeine Bestimmungen	
II	Artt. 4–10 DSA	Haftung der Anbieter von Vermittlungsdiensten	In Bezug auf die Haftung wird zwischen Durchleitungsdiensten, Caching-Leistungen und Hostingdiensten unterschieden.
III	Artt. 11–48 DSA	Sorgfaltspflichten für ein transparentes und sicheres Onlineumfeld	
	Artt. 11–15 DSA	Abschnitt 1	Geltung für **Anbieter von Vermittlungsdiensten**
	Artt. 16–18 DSA	Abschnitt 2	Geltung für Hostingdiensteanbieter, einschließlich Online-Plattformen
	Artt. 19–28 DSA	Abschnitt 3	Geltung für Anbieter von Online-Plattformen
	Artt. 29–32 DSA	Abschnitt 4	Geltung für Anbieter von Online-Plattformen, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglichen
	Artt. 33–43 DSA	Abschnitt 5	Geltung für Anbieter von sehr großen Online- Plattformen und sehr großen Online-Suchmaschinen
	Artt. 44–48 DSA	Abschnitt 6	Sonstige Bestimmungen über Sorgfaltspflichten
IV	Artt. 49–88 DSA	Umsetzung, Zusammenarbeit, Sanktionen und Durchsetzung	
V	Artt. 89–93 DSA	Schlussbestimmungen	

1.2 Zeitstrahl

Inkrafttreten	Anwendungsbeginn	
November 2022	Seit dem **16.11.2022**: Artikel 24 Absätze 2, 3 und 6, Artikel 33 Absätze 3–6, Artikel 37 Absatz 7, Artikel 40 Absatz 13 und Kapitel IV Abschnitte 4, 5 und 6 DSA	**17.02.2024** (Art. 93 DSA)

1.3 Begrifflichkeiten und Definition

Der DSA enthält in seinem Art. 3 Begriffsbestimmungen. Diese Begriffsbestimmungen sind für die Auslegung und Anwendung des Gesetzes von grundlegender Bedeutung.

Sie müssen dabei beachten, dass diese vom allgemeinen oder in der IT üblichen Verständnis dieser Begriffe abweichen können. Der DSA enthält beispielsweise eine Definition des Begriffs „Nutzer" (Art. Art. 3 lit. b DSA), der auch juristische Personen einschließt. Auch werden die Begriffe „Verbraucher" und „Unternehmer" in Art. 3 DSA definiert, für die das Bürgerliche Gesetzbuch (BGB) bereits mit Blick auf die Verbraucherschutzbestimmungen Definitionen enthält. Ebenso wird der Begriff „allgemeine Geschäftsbedingungen" eigenständig definiert.

Der **Begriff „Online-Schnittstelle"** ist in Art. 3 lit. m DSA definiert als „eine Software, darunter auch Websites oder Teile davon sowie Anwendungen, einschließlich Mobil-Apps".

Eine Besonderheit besteht auch darin, dass der **Begriff „Werbung"** in Art. 3 lit. r DSA als „Informationen, die dazu bestimmt sind, die Botschaft einer juristischen oder natürlichen Person zu verbreiten, unabhängig davon, ob damit gewerbliche oder nicht gewerbliche Zwecke verfolgt werden, und die von einer Online-Plattform auf ihrer Online-Schnittstelle gegen Entgelt speziell zur Bekanntmachung dieser Informationen dargestellt werden" definiert ist**. Dieses Begriffsverständnis weicht vom Gesetz gegen unlauteren Wettbewerb (UWG) ab und gilt daher wohl nur für den DSA.**

Für „kommerzielle Kommunikation" wird in Art. 3 lit. w DSA auf die Definition in Art. 2 lit. f der Richtlinie 2000/31/EG (Richtlinie über den elektronischen Geschäftsverkehr) verwiesen.

Ein **„Empfehlungssystem"** ist im Rahmen des DSA „ein vollständiges oder teilweise automatisiertes System, das von einer Online-Plattform verwendet wird,

um auf ihrer Online-Schnittstelle den Nutzern bestimmte Informationen vorzuschlagen oder diese Informationen zu priorisieren, auch infolge einer vom Nutzer veranlassten Suche, oder das auf andere Weise die relative Reihenfolge oder Hervorhebung der angezeigten Informationen bestimmt" (Art. 3 lit. s DSA).

Tipp für die Praxis

Machen Sie sich mit den gesetzlichen Definitionen vertraut. Beachten Sie, dass diese jeweils aus dem jeweiligen Rechtsakt heraus auszulegen sind.

Beachten Sie die Auswirkungen für die Vertragsgestaltung: Diese Definitionen können über das konkrete Gesetz hinaus Bedeutung erlangen. Werden sie beispielsweise in Verträgen verwendet und kommt es für den Vertrag zum Streit über das Verständnis des Begriffs, ist es nicht auszuschließen, dass zukünftig ein Gericht eine solche gesetzliche Definition zur Auslegung heranzieht.

2. Verpflichtete und Anwendungsbereich

Der DSA regelt in seinen verschiedenen Kapiteln unterschiedliche Aspekte der Erbringung von Digital Services. Der zentrale Begriff zur Festlegung des Anwendungsbereichs ist „Vermittlungsdienst". Hierbei handelt es sich um einen Oberbegriff. Für einzelne Ausprägungen des Vermittlungsdiensts enthält der DSA im Kontext der Haftungsbegrenzung differenzierte Regelungen sowie für sog. Online-Plattformen und sog. Online-Suchmaschinen weitere rechtliche Anforderungen.

Verpflichtet ist der Anbieter eines Vermittlungsdienstes. **Der Vermittlungsdienst ist der Oberbegriff.**

Seine Definition in Art. 3 lit. g DSA nimmt Bezug auf den Begriff „**Dienstleistungen der Informationsgesellschaft**", womit diese zum wesentlichen Merkmal wird. Art. 3 lit. a DSA definiert diesen als „einen Dienst im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535".

> *„Dienstleistungen der Informationsgesellschaft" sind nach Art. 3 lit. a DSA i. V. m. Art. 1 Abs. 1 lit. b Richtlinie (EU) 2015/1535 des europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft*[12]*: „jede in der Regel gegen Entgelt elektronisch im*

[12] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015L1535 (Stand: 28.10.2024)

Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung". Im Sinne dieser Definition bezeichnet der Ausdruck

i) „im Fernabsatz erbrachte Dienstleistung" eine Dienstleistung, die ohne gleichzeitige physische Anwesenheit der Vertragsparteien erbracht wird;

ii) „elektronisch erbrachte Dienstleistung" eine Dienstleistung, die mittels Geräten für die elektronische Verarbeitung (einschließlich digitaler Kompression) und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen wird und die vollständig über Draht, über Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen wird;

iii) „auf individuellen Abruf eines Empfängers erbrachte Dienstleistung" eine Dienstleistung die durch die Übertragung von Daten auf individuelle Anforderung erbracht wird."

Eine beispielhafte Nennung solcher Dienste ist in Anhang I dieser Richtlinie (EU) 2015/1535 erfolgt.

„Vermittlungsdienst" ist nach Art. 3 lit. g DSA eine der folgenden Dienstleistungen der Informationsgesellschaft (siehe vorstehend), womit der **Begriff Vermittlungsdienst weitergehend konkretisiert wird** und damit nicht gleichbedeutend ist mit Dienstleistungen der Informationsgesellschaft:

„ *„i) eine **„reine Durchleitung",** die darin besteht, von einem Nutzer bereitgestellte Informationen in einem Kommunikationsnetz zu übermitteln oder den Zugang zu einem Kommunikationsnetz zu vermitteln,*

*ii) eine **„Caching"-Leistung,** die darin besteht, von einem Nutzer bereitgestellte Informationen in einem Kommunikationsnetz zu übermitteln, wobei eine automatische, zeitlich begrenzte Zwischenspeicherung dieser Informationen zu dem alleinigen Zweck erfolgt, die Übermittlung der Informationen an andere Nutzer auf deren Anfrage effizienter zu gestalten,*

*iii) ein **„Hosting"-Dienst,** der darin besteht, von einem Nutzer bereitgestellte Informationen in dessen Auftrag zu speichern".*

Die Differenzierung dieser Dienste ist insbesondere für die unterschiedliche Ausprägung der Haftung der Anbieter von Vermittlungsdiensten (Kapitel II) entscheidend.

Für **„Online-Plattformen“** und **„Online-Suchmaschinen“** sowie für deren sehr große Versionen sieht der DSA Sonderregelungen vor. Diese Begriffe sind wie folgt definiert:

> *„Online-Plattform“ bezeichnet nach Art. 3 lit. i DSA einen „Hostingdienst, der im Auftrag eines Nutzers Informationen speichert und öffentlich verbreitet, sofern es sich bei dieser Tätigkeit nicht nur um eine unbedeutende und reine Nebenfunktion eines anderen Dienstes oder um eine unbedeutende Funktion des Hauptdienstes handelt, die aus objektiven und technischen Gründen nicht ohne diesen anderen Dienst genutzt werden kann, und sofern die Integration der Funktion der Nebenfunktion oder der unbedeutenden Funktion in den anderen Dienst nicht dazu dient, die Anwendbarkeit dieser Verordnung zu umgehen“.*

Die „Online-Plattform“ ist kraft Definition ein Hostingdienst, sodass für diese die Haftungsbegrenzungsregelungen für Hostingdienste gelten.

„Online-Suchmaschine“ bezeichnet nach Art. 3 lit. j DSA

> *„einen Vermittlungsdienst, der es Nutzern ermöglicht, in Form eines Stichworts, einer Spracheingabe, einer Wortgruppe oder einer anderen Eingabe Anfragen einzugeben, um prinzipiell auf allen Websites oder auf allen Websites in einer bestimmten Sprache eine Suche zu einem beliebigen Thema vorzunehmen und Ergebnisse in einem beliebigen Format, in dem Informationen im Zusammenhang mit dem angeforderten Inhalt zu finden sind, angezeigt zu bekommen“.*

Der Begriff und die entsprechenden Regelungen sind erst recht spät im Gesetzgebungsverfahren in den DSA aufgenommen worden. Es ist definitorisch nicht klargestellt, ob es sich hierbei um einen Hostingdienst handelt, was jedoch für die Bewertung der Haftung für Inhalte von zentraler Bedeutung ist.

Hinweis

Die exakte Unterscheidung dieser Dienste ist für die Anwendung der Regelungen des DSA von entscheidender Bedeutung. Denn der DSA regelt anhand dieser Begriffe die Anwendung der unterschiedlichen Regelungen.

Die Regelungen des DSA gelten nach seinem **Art. 2 Abs. 1 DSA** für Vermittlungsdienste, die für Nutzer mit Niederlassungsort oder Sitz in der Union angeboten werden, ungeachtet des Niederlassungsortes des Anbieters dieser Vermittlungsdienste (**Marktortprinzip**).

Ausnahmen für Kleinst- und Kleinunternehmen im Sinne der Empfehlung 2003/361/EG sehen die Artt. 19 und 29 DSA vor.

3. Haftung der Anbieter von Vermittlungsdiensten (Kapitel II, Artt. 4–10 DSA)

Der grundlegende Ansatz der Regelungen ist, dass die Anbieter nicht haften sollen, wenn sie sich in Bezug auf den Inhalt neutral verhalten. Die Haftungsausschlüsse sollen daher nicht gelten, wenn der Anbieter sich nicht darauf beschränkt, die Dienstleistungen auf neutrale Weise und durch die bloße technische und automatische Verarbeitung der vom Nutzer bereitgestellten Informationen zu erbringen, sondern dahingehend eine aktive Rolle einnimmt, dass er Wissen oder Kontrolle über diese Informationen erhält (Erwägungsgrund 18 DSA). Diese Ausschlüsse sollten dementsprechend nicht für die Haftung im Zusammenhang mit Informationen gelten, die nicht vom Nutzer bereitgestellt werden, sondern vom Anbieter des Vermittlungsdienstes selbst, auch wenn diese Informationen im Rahmen der redaktionellen Verantwortung dieses Anbieters entwickelt wurden (Erwägungsgrund 18 DSA).

Wenn ein Anbieter von Vermittlungsdiensten bewusst mit einem Nutzer zusammenarbeitet, um rechtswidrige Tätigkeiten auszuüben, stellt dies keine neutrale Erbringung der Dienstleistung dar, sodass kein Haftungsausschluss greift. Dies sollte – so Erwägungsgrund 20 DSA – beispielsweise dann der Fall sein, wenn der Anbieter seine Dienstleistung hauptsächlich zu dem Zweck anbietet, rechtswidrige Tätigkeiten zu erleichtern, indem er etwa seinen Zweck – die Erleichterung rechtswidriger Aktivitäten – klar zum Ausdruck bringt und seine Dienstleistungen für diesen Zweck geeignet sind. Allein die Tatsache, dass ein Dienst verschlüsselte Übertragungen oder ein anderes System anbietet, mit dem die Identifizierung des Nutzers unmöglich wird, sollte für sich genommen nicht als Erleichterung rechtswidriger Tätigkeiten gelten.

Die Regelungen sollen – wie sich aus Erwägungsgrund 17 DSA ergibt – jedoch nicht haftungsbegründend wirken: Mit den in dieser Verordnung festgelegten Vorschriften über die Haftung der Anbieter von Vermittlungsdiensten sollte nur festgelegt werden, wann der betreffende Anbieter von Vermittlungsdiensten im Zusammenhang mit von den Nutzern bereitgestellten rechtswidrigen Inhalten nicht

haftbar gemacht werden kann. Die Vorschriften sollten nicht so ausgelegt werden, dass sie eine positive Grundlage dafür darstellen, festzustellen, wann ein Anbieter haftbar gemacht werden kann; dies ist nach den geltenden Vorschriften des Unionsrechts oder des nationalen Rechts zu bestimmen. Zudem sollten die in dieser Verordnung festgelegten Haftungsausschlüsse für jegliche Art der Haftung im Zusammenhang mit jeglicher Art von rechtswidrigen Inhalten gelten, unabhängig von dem genauen Gegenstand oder der Art dieser Rechtsvorschriften.

Mit Blick auf die unterschiedlichen **Tätigkeiten „reine Durchleitung", „Caching" und „Hosting" sowie der unterschiedlichen Position**en und Fähigkeiten der Anbieter der betreffenden Dienste ist es erforderlich, die für diese Tätigkeiten geltenden Vorschriften insofern zu unterscheiden, als sie nach dieser Verordnung anderen Anforderungen und Bedingungen unterliegen, und ihr Geltungsbereich nach der Auslegung des Gerichtshofs der Europäischen Union variiert (Erwägungsgrund 19 DSA).

Die Artt. 4–10 DSA enthalten Regelungen zur Haftung der Anbieter von Vermittlungsdiensten. Bei genauer Betrachtung zeigt sich jedoch, dass es sich hierbei um Regelungen zur Begrenzung der Haftung der Vermittlungsdienste handelt, soweit diese auf den Inhalt keinen Einfluss nehmen. Denn Erwägungsgrund 17 DSA stellt klar, dass diese Regelungen des DSA nicht eine Haftung begründen sollen, die nicht ohnehin schon gesetzlich besteht.

Anbietern von Vermittlungsdiensten wird keine allgemeine Verpflichtung auferlegt, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hindeuten (Art. 8 DSA).

Die Haftung bzw. Haftungsbegrenzung differenziert wie folgt:

➤ **Haftungsbegrenzung bei „reiner Durchleitung" (Art. 4 Abs. 1 DSA):**

„ *„Bei der Durchführung eines Dienstes der Informationsgesellschaft, der darin besteht, von einem Nutzer bereitgestellte Informationen in einem Kommunikationsnetz zu übermitteln oder Zugang zu einem Kommunikationsnetz zu vermitteln, haftet der Diensteanbieter nicht für die übermittelten oder abgerufenen Informationen, sofern er*

a) die Übermittlung nicht veranlasst,

b) den Adressaten der übermittelten Informationen nicht auswählt und

c) die übermittelten Informationen nicht auswählt oder verändert."

➤ **Haftungsbegrenzung bei „Caching" (Art. 5 Abs. 1 DSA):**

„ *„Bei der Durchführung eines Dienstes der Informationsgesellschaft, der darin besteht, von einem Nutzer bereitgestellte Informationen in einem Kommunikationsnetz zu übermitteln, haftet der Diensteanbieter nicht für die automatische, zeitlich begrenzte Zwischenspeicherung, die dem alleinigen Zweck dient, die Übermittlung der Informationen an andere Nutzer auf deren Anfrage effizienter oder sicherer zu gestalten, sofern seitens des Anbieters folgende Voraussetzungen erfüllt sind:*

a) er verändert die Informationen nicht,

b) er beachtet die Bedingungen für den Zugang zu den Informationen,

c) er beachtet die Regeln für die Aktualisierung der Informationen, die weithin in der Branche anerkannt und verwendet werden,

d) er beeinträchtigt die zulässige Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Informationen, die weithin in der Branche anerkannt und verwendet werden, nicht und

e) er handelt zügig, um von ihm gespeicherte Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald er tatsächliche Kenntnis davon erhält, dass die Informationen am ursprünglichen Ausgangsort der Übermittlung aus dem Netz entfernt wurden oder der Zugang zu ihnen gesperrt wurde oder eine Justiz- oder Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat."

➤ Haftungsbegrenzung bei „Hosting" (Art. 6 Abs. 1 DSA):

„ *„Bei der Durchführung eines Dienstes der Informationsgesellschaft, der in der Speicherung der von einem Nutzer bereitgestellten Informationen besteht, haftet der Diensteanbieter nicht für die im Auftrag eines Nutzers gespeicherten Informationen, sofern er*

a) keine tatsächliche Kenntnis von einer rechtswidrigen Tätigkeit oder rechtswidrigen Inhalten hat und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder rechtswidrige Inhalte offensichtlich hervorgeht, oder

b) sobald er diese Kenntnis oder dieses Bewusstsein erlangt, zügig tätig wird, um den Zugang zu den rechtswidrigen Inhalten zu sperren oder diese zu entfernen."

Für Hostingdiensteanbieter ist jedoch aufgrund ihrer Nähe zum Inhalt ein Verfahren zur Reaktion auf Hinweise auf Rechtswidrigkeit von Inhalten vorgesehen. Das sog. „Notice & Take Down" ist in Artt. 16–18 DSA geregelt. Danach sind diese verpflichtet, nach einem Hinweis den Inhalt zu prüfen und hierauf zu reagieren.

Erfasst sind auch **Online-Plattformen**, die kraft Definition ein Hostingsdienst sind. Wie **Online-Suchmaschinen** einzuordnen sind, stellt der DSA nicht klar.

Ein sog. **„Guter-Samariter-Privileg"** sieht Art. 7 DSA vor. Die Anbieter, die freiwillige Untersuchungen auf Eigeninitiative und Einhaltung der Rechtsvorschriften vornehmen, sollen nicht schärfer haften als die Unternehmen, die „die Hände in den Schoß legen".

Das **Vorgehen gegen rechtswidrige Inhalte** und entsprechend staatliche Anordnungen sowie Auskunftsanordnungen regeln **Artt. 9 und 10 DSA**.

4. Sorgfaltspflichten für transparentes und sicheres Online-Umfeld (Kapitel III, Artt. 11–48 DSA)

Dem Kapitel III liegt der Ansatz der abgestuften Sorgfaltspflichten je nach Dienstart im Sinne eines Pyramidenmodells zugrunde. Nachfolgend wird ein Überblick gegeben:

- Es müssen **Kontaktstellen** eingerichtet und durch Anbieter außerhalb der EU gesetzliche **Vertreter** benannt werden (Artt. 11–13 DSA).
- **Vorgaben zur Gestaltung von Allgemeinen Geschäftsbedingungen für Anbieter von Vermittlungsdiensten enthält Art. 14 DSA.** Dieser prägt die Transparenzpflichten über das AGB-Recht hinaus und sieht insbesondere vor:
  - Die Anbieter von Vermittlungsdiensten **machen in ihren allgemeinen Geschäftsbedingungen Angaben** zu etwaigen Beschränkungen in Bezug auf die von den Nutzern bereitgestellten Informationen, die sich die Anbieter im Zusammenhang mit der Nutzung ihres Dienstes selbst auferlegen (mit weiteren Maßgaben in Art. 14 Abs. 1 DSA).
  - Die Anbieter von Vermittlungsdiensten **informieren die Nutzer über etwaige wesentliche Änderungen der allgemeinen Geschäftsbedingungen.**

- Richtet sich ein **Vermittlungsdienst in erster Linie an Minderjährige oder wird er überwiegend von Minderjährigen genutzt**, so erläutert der Anbieter von Vermittlungsdiensten die Bedingungen und jegliche Einschränkungen für die Nutzung des Dienstes so, dass Minderjährige sie verstehen können.
- **Sehr große Online-Plattformen und sehr große Online-Suchmaschinen im Sinne des Art. 33 DSA** veröffentlichen ihre allgemeinen Geschäftsbedingungen in den Amtssprachen aller Mitgliedstaaten, in denen sie ihre Dienste anbieten.

➤ **Art. 15 DSA** sieht für Anbieter von Vermittlungsdiensten **Allgemeine Transparenzberichtspflichten** vor.

➤ **Art. 25 DSA** sieht ein **Verbot von „Dark Pattern"** vor. Anbieter von Online-Plattformen dürfen ihre Online-Schnittstellen (siehe zum Begriff oben bei den Begriffsbestimmungen) nicht so konzipieren, organisieren oder betreiben, dass Nutzer getäuscht, manipuliert oder anderweitig in ihrer Fähigkeit, freie und informierte Entscheidungen zu treffen, maßgeblich beeinträchtigt oder behindert werden.

➤ Für **Werbung** (siehe zum Begriff oben bei den Begriffsbestimmungen) **auf Online-Plattformen** sieht **Art. 26 DSA** zusätzliche Regelungen vor. Insbesondere:

Die Anbieter von Online-Plattformen dürfen nach Art. 26 Abs. 3 DSA Nutzern **keine Werbung anzeigen, die auf Profiling im Sinne des Art. 4 Nr. 4 DS-GVO unter Verwendung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO** beruht. Hiermit besteht **ein über die DS-GVO hinausgehendes Verbot!**

➤ Die **Transparenz der Empfehlungssysteme** wird durch **Art. 27 DSA** geregelt. Anbieter von Online-Plattformen, die Empfehlungssysteme verwenden, müssen **in ihren allgemeinen Geschäftsbedingungen in klarer und verständlicher Sprache die wichtigsten Parameter, die in ihren Empfehlungssystemen verwendet werden,** sowie alle Möglichkeiten für die Nutzer, wie diese wichtigen Parameter zu ändern oder zu beeinflussen sind, darlegen. Die Pflicht wird durch die Absätze 32-seitige 27 DSA weiter konkretisiert.

➤ Den **Online-Schutz Minderjähriger** regelt Art. 28 DSA wie folgt:

Anbieter von Online-Plattformen, die für Minderjährige zugänglich sind, müssen **geeignete und verhältnismäßige Maßnahmen ergreifen, um für ein**

hohes Maß an Privatsphäre, Sicherheit und Schutz von Minderjährigen innerhalb ihres Dienstes zu sorgen.

Anbieter von Online-Plattformen dürfen auf ihrer Schnittstelle **keine Werbung auf der Grundlage von Profiling gemäß Art. 4 Nr. 4 DS-GVO unter Verwendung personenbezogener Daten des Nutzers** darstellen, wenn sie hinreichende Gewissheit haben, dass der betreffende Nutzer minderjährig ist.

Zur Einhaltung der vorstehenden Pflichten sind die Anbieter von Online-Plattformen aber nicht verpflichtet, zusätzliche personenbezogene Daten zu verarbeiten, um festzustellen, ob der Nutzer minderjährig ist. Insofern wird dem Grundsatz der Datenminimierung Rechnung getragen.

Die Kommission kann nach Anhörung des Ausschusses Leitlinien herausgeben, um die Anbieter von Online-Plattformen bei der Anwendung von Absatz 1 zu unterstützen.

➤ **Artt. 29–32 DSA** sehen Bestimmungen für **Anbieter von Onlineplattformen, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmen** ermöglichen. Für Kleinst- und Kleinunternehmen sind Ausnahmen in Art. 29 DSA geregelt. Insbesondere:

- Eine Pflicht zur Überprüfung des Unternehmens zum Schutz der Kunden durch die Anbieter von Onlineplattformen, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmen ermöglichen (sieht Art. 30 DSA vor).
- Art. 31 DSA sieht unter dem Schlagwort Konformität durch Technikgestaltung vor, dass solche Onlineplattformen so gestaltet sind, dass die auf diesen Plattformen anbietenden Unternehmen ihren gesetzlichen Pflichten zum Schutz der Verbraucher nachkommen können.
- Eine Informationspflicht der Anbieter solcher Onlineplattformen, wenn die Anbieter Kenntnis davon erhalten, dass ein rechtswidriges Produkt oder eine rechtswidrige Dienstleistung von einem Unternehmen über ihre Dienste gegenüber Verbrauchern in der EU angeboten wurde, ist in Art. 32 DSA geregelt.

5. Sanktionen (Art. 52 DSA)

Art. 52 DSA sieht den Rahmen für Sanktionen für Verstöße gegen den DSA vor. Anders als in der DS-GVO ist dort jedoch keine unmittelbar geltende Bußgeldbestimmung geregelt. Diese muss durch einen nationalen Durchführungsrechtsakt „zum Leben erweckt" werden.

Die Mitgliedstaaten müssen nach Art. 52 Abs. 3 DSA sicherstellen, dass der Höchstbetrag der Geldbußen, die bei Nichteinhaltung einer in dieser Verordnung festgelegten Verpflichtung verhängt werden können, 6 % des weltweiten Jahresumsatzes des betreffenden Anbieters von Vermittlungsdiensten im vorangegangenen Geschäftsjahr beträgt. Die Mitgliedstaaten stellen sicher, dass der Höchstbetrag der Geldbußen, die bei Bereitstellung unrichtiger, unvollständiger oder irreführender Informationen, beim Versäumnis einer Antwort oder der Berichtigung unrichtiger, unvollständiger oder irreführender Informationen sowie bei der Nichtduldung einer Nachprüfung verhängt werden können, 1 % des weltweiten Jahresumsatzes des betreffenden Anbieters von Vermittlungsdiensten oder der betreffenden Person im vorangegangenen Geschäftsjahr beträgt.

6. Verhältnis zur DS-GVO

Das Verhältnis zum Datenschutz ist in Art. 2 Abs. 4 lit. g DSA und Erwägungsgrund 10 Abs. 2 DSA geregelt:

> *„Diese Verordnung lässt die Vorschriften anderer Rechtsakte der Union unberührt, die andere Aspekte der Erbringung von Vermittlungsdiensten im Binnenmarkt regeln oder diese Verordnung präzisieren und ergänzen, insbesondere folgende: […] g) die Unionsvorschriften zum Schutz personenbezogener Daten, insbesondere die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG, […]"*
>
> *(Art. 2 Abs. 4 lit. g DSA)*
>
> *„Ebenso sollte diese Verordnung im Interesse der Klarheit das Unionsrecht über den Verbraucherschutz – […] – sowie das Unionsrecht über den Schutz personenbezogener Daten – insbesondere die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates – unberührt lassen."*
>
> *(ErwGr. 10 Abs. 2 DSA)*

Die DS-GVO gilt damit ohne Einschränkung durch den DSA, sodass die Regelungen der DS-GVO und des DSA nebeneinander anzuwenden sind. Sollte es zum Konflikt kommen, setzt sich, vereinfacht gesagt, das Datenschutzrecht durch.

II. DIGITAL MARKETS ACT (DMA)

Der Digital Markets Act (DMA) zielt in erster Linie darauf ab, Wettbewerbsverzerrungen im Binnenmarkt zu verhindern. Er lässt sich als spezifische Ergänzung zu den Regelungen gegen Wettbewerbsbeschränkungen verstehen, da er Schutz vor Missbrauch der Machtposition durch große Online-Plattformen bieten soll.

1. Überblick

Mit der Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte) erfolgt eine Regulierung der großen Online-Plattformen. Insofern besteht auch eine Nähe zu den Regelungen des DSA, wenngleich die Zielsetzung unterschiedlich ist.

Im vorliegenden Buch wird die englische Bezeichnung **Digital Markets Act** oder **DMA** verwendet, um Missverständnisse mit Blick auf den deutschen Rechtsbegriff „Verordnung" zu vermeiden.

Der DMA ist – anders als z. B. die NIS-2-Richtlinie – eine EU-Verordnung und gilt daher unmittelbar und direkt in jedem EU-Mitgliedstaat.

1.1 Worum geht es?

Der DMA besteht aus 54 Artikeln und 109 Erwägungsgründen und hat einen Textumfang von 66 DIN-A4-Seiten. Die EU-Rechtsakte haben – anders als typischerweise deutsche Gesetze – kein Inhaltsverzeichnis, was eine schnelle Orientierung erschwert. Der DMA umfasst im Überblick: Verbot von Meistbegünstigungsklauseln, Verbot bestimmter Bindungen und Kopplungen, Auskunftsrecht für Werbetreibende und Verlage, Verbot der Zusammenführung von Nutzerdaten über verschiedene Plattformen des Gatekeepers, Transparenz in Bezug auf Preiszusammenstellungen, Transparenz in Bezug auf Algorithmen der Werbedienste der Gatekeeper.

Um eine Fragmentierung des Binnenmarkts zu vermeiden, sieht Art. 1 Abs. 5 DMA vor, dass die EU-Mitgliedstaaten den Gatekeepern keine weiteren Verpflichtungen im Wege von Rechts- oder Verwaltungsvorschriften auferlegen, um bestreitbare und faire Märkte zu gewährleisten. Der DMA hindert die Mitgliedstaaten jedoch nicht daran, Unternehmen – einschließlich solcher, die zentrale Plattformdienste bereitstellen – für Angelegenheiten, die nicht in den Anwendungsbereich des DMA fallen, Verpflichtungen aufzuerlegen.

Darüber hinaus ist es den nationalen Behörden nach Art. 1 Abs. 7 DMA untersagt, Entscheidungen zu erlassen, die einem von der Kommission nach dieser Verordnung erlassenen Beschluss zuwiderlaufen.

Tipp

Verlieren Sie nicht den Überblick: Verschaffen Sie sich anhand des nachfolgenden Inhaltsverzeichnisses einen Überblick über das für Sie Wesentliche und Entscheidende!

Kap.	Artikel des DMA	Regelungsinhalt	
I	Artt. 1–2 DMA	Gegenstand, Anwendungsbereich und Begriffsbestimmungen	
II	Artt. 3, 4 DMA	Torwächter (= Gatekeeper)	Kriterien der Einordnung als Gatekeeper Benennung durch die EU-Kommission
III	Artt. 5–15 DMA	Unfaire oder die Bestreitbarkeit beschränkende Praktiken von Gatekeeper-Sorgfaltspflichten	
		Art. 5 DMA: Verpflichtungen von Gatekeepern	u. a.: Verbotene Verarbeitungen personenbezogener Daten (Art. 2 Nr. 25 DMA)
		Art. 6 DMA: Verpflichtungen von Gatekeepern, die durch Artikel 8 näher ausgeführt werden	u. a.: Verbot der Nutzung von Daten (Art. 2 Nr. 24 DMA) von gewerblichen Nutzern
		Art. 7 DMA: Verpflichtung von Gatekeepern zur Interoperabilität nummernunabhängiger interpersoneller Kommunikationsdienste	u. a.: Pflicht zur Interoperabilität der Sicherheit (vgl. Art. 7 Abs. 3 DMA)
		„Self-Executing" der Pflichten und Verfahren (Artt. 8–11 DMA)	u. a.: Pflicht zum Nachweis der Einhaltung durch Gatekeeper
		Art. 12 DMA: Aktualisierung der Verpflichtungen der Gatekeeper	Befugnis der EU-Kommission zur Ergänzung der Pflichten nach Artt. 5, 6 und 7 DMA
		Art. 13 DMA: Umgehungsverbot	
		Art. 14 DMA: Verpflichtung zur Unterrichtung über Zusammenschlüsse	

		Art. 15 DMA: Prüfungspflicht	
IV	Artt. 16–19 DMA	Marktuntersuchung	
V	Artt. 20–43 DMA	Untersuchungs-, Durchsetzungs- und Überwachungsbefugnisse	
VI	Art. 44–54 DMA	Schlussbestimmungen	

1.2 Zeitstrahl

Inkrafttreten	Anwendungsbeginn	
November 2022	Seit dem **01.11.2022**: Artikel 3 Absätze 6 und 7 und die Artikel 40, 46, 47, 48, 49 und 50 Seit dem **25.06.2023**: Artikel 42 und 43 gelten ab dem 25. Juni 2023	**02.05.2023** (Art. 54 DMA)

1.3 Begrifflichkeiten und Definitionen

Der DMA enthält in seinem Art. 2 Begriffsbestimmungen. Diese Begriffsbestimmungen sind für die Auslegung und Anwendung des Gesetzes von grundlegender Bedeutung.

Sie müssen dabei beachten, dass diese vom allgemeinen oder in der IT üblichen Verständnis dieser Begriffe abweichen können. Der DMA nimmt beispielsweise für die Begriffe „Online-Vermittlungsdienste“ und „Online-Suchmaschine“ Bezug auf die Definitionen in der Verordnung (EU) 2019/1150 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und **nicht (!)** auf den DSA. Art. 3 Nr. 23 DMA enthält beispielsweise auch eine Definition des Begriffs „Suchergebnisse“.

Tipp für die Praxis

Machen Sie sich mit den gesetzlichen Definitionen vertraut. Beachten Sie, dass diese jeweils aus dem jeweiligen Rechtsakt heraus auszulegen sind.

Beachten Sie die Auswirkungen für die Vertragsgestaltung: Diese Definitionen können über das konkrete Gesetz hinaus Bedeutung erlangen. Werden Sie beispielsweise in Verträgen verwendet und kommt es für den Vertrag zum Streit

über das Verständnis des Begriffs, ist es nicht auszuschließen, dass zukünftig ein Gericht eine solche gesetzliche Definition zur Auslegung heranzieht.

2. Verpflichtete

Der DMA gilt für zentrale Plattformdienste, die Gatekeeper für in der Union niedergelassene gewerbliche Nutzer oder in der Union niedergelassene oder aufhältige Endnutzer bereitstellen oder anbieten (Art. 1 Abs. 1 DMA).

„Torwächter" ist nach Art. 2 Nr. 1 DMA ein Unternehmen, das zentrale Plattformdienste bereitstellt und nach Art. 3 DMA benannt worden ist. In diesem Buch wird jedoch anstatt **„Torwächter" der englische Begriff „Gatekeeper"** verwendet, da er eine klarere Assoziation zur Pflichtenstellung nach dem DMA schafft.

Mit anderen Worten: Erst diese Benennung löst die Pflichten nach dem DMA aus.

Zentrale Plattformdienste sind nach Art. 2 Nr. 2 DMA: Online-Vermittlungsdienste, Online-Suchmaschinen, Online-Dienste sozialer Netzwerke, Video-Sharing-Plattform-Dienste, nummernunabhängige interpersonelle Kommunikationsdienste, Betriebssysteme, Webbrowser, virtuelle Assistenten, Cloud-Computing-Dienste sowie Online-Werbedienste, einschließlich Werbenetzwerken, Werbebörsen und sonstiger Werbevermittlungsdienste, die von einem Unternehmen, das einen der unter den Buchstaben a bis i genannten zentralen Plattformdienste bereitstellt, angeboten werden.

Ergänzend ist Art. 3 Abs. 9 DMA zu beachten. Danach gelten die Pflichten des DMA nicht für alle Dienste des benannten Gatekeepers, sondern die EU-Kommission muss auch den jeweiligen Dienst benennen, **für den die Pflichten des DMA dann gelten**.

Der DMA sieht Ausnahmen für Dienste nach dem TKG vor: Diese Verordnung gilt nicht für Märkte im Zusammenhang mit elektronischen Kommunikationsnetzen im Sinne des Art. 2 Nr. 1 Richtlinie (EU) 2018/1972 über den europäischen Kodex für die elektronische Kommunikation und elektronischen Kommunikationsdiensten im Sinne des Art. 2 Nr. 4 der Richtlinie (EU) 2018/1972 über den europäischen Kodex für die elektronische Kommunikation (Art. 1 Abs. 3 DMA). Die Ausnahme gilt jedoch nicht für **nummernunabhängige interpersonelle Kommunikationsdienste**. Das sind die sog. OTT-1-Dienste, bei denen, vereinfacht gesagt, die Anbieter des Kommunikationsdienstes nicht auch zugleich die dafür erforderliche Infrastruktur betreiben (z. B. Messenger und E-Mail-Dienste, nicht aber SMS). Für die interpersonellen Kommunikationsdienste im Sinne des Art. 2 Nr. 5 der Richtlinie

(EU) 2018/1972 über den europäischen Kodex für die elektronische Kommunikation regelt Art. 1 Abs. 4 DMA lediglich, dass der DMA die Befugnisse und Zuständigkeiten, die den nationalen Regulierungsbehörden und anderen zuständigen Behörden nach Art. 61 dieser RiLi 2018/1972 übertragen sind, nicht berührt werden. Für diese gelten also sowohl der DMA als auch die entsprechenden Regelungen des Telekommunikationsgesetzes (TKG).

Zusammengefasst: Der DMA gilt für die nach Art. 3 DMA benannten zentralen Plattformdienste des Gatekeepers.

Der DMA gilt ungeachtet des Niederlassungsorts und Standorts der Gatekeeper und ungeachtet des sonstigen auf die Erbringung von Dienstleistungen anwendbaren Rechts (Art. 1 Abs. 2 DMA) **(Marktortprinzip).**

3. Benennung als Gatekeeper (Torwächter)

Die Benennung als Gatekeeper regelt Art. 3 DMA. Ein Unternehmen wird nach Art. 3 Abs. 1 DMA als Gatekeeper benannt, wenn es erheblichen Einfluss auf den Binnenmarkt hat, einen zentralen Plattformdienst bereitstellt, der gewerblichen Nutzern als wichtiges Zugangstor zu Endnutzern dient, **und** hinsichtlich seiner Tätigkeiten eine gefestigte und dauerhafte Position innehat oder absehbar ist, dass es eine solche Position in naher Zukunft erlangen wird (Art. 3 Abs. 1 DMA). Art. 3 DMA enthält weitere Konkretisierungen:

- **Art. 3 Abs. 2 DMA:** Vermutungstatbestände für Art. 3 Abs. 1 lit. a, b und c DMA
- **Art. 3 Abs. 3 DMA:** Pflicht des Unternehmens zur Mitteilung der Erfüllung der Kriterien an EU-Kommission
- **Art. 3 Abs. 4 DMA:** (Pflicht zur) Benennung durch EU-Kommission binnen 45 Arbeitstagen
- **Art. 3 Abs. 5 bis 10 DMA:**
  - Verfahren zur Benennung (i. V. m. Art. 17 DMA)
  - Kriterien zur Benennung, unabhängig von Art. 3 Abs. 2 DMA
- **Art. 4 DMA:** Verfahren zur Überprüfung des Gatekeeper-Status

4. Pflichten des Gatekeepers (Torwächters)

Der Gatekeeper hat die Einhaltung der Verpflichtungen aus den Art. 5–7 DMA sicherzustellen und nachzuweisen (Art. 8 Abs. 1 DMA).

- **Art. 5 DMA:** Verpflichtungen von Gatekeepern

- Art. 5 Abs. 1 DMA: Der Gatekeeeper hält alle Verpflichtungen nach diesem Artikel **in Bezug auf jeden seiner zentralen Plattformdienste ein, die im Benennungsbeschluss nach Art. 3 Abs. 9 DMA aufgeführt sind.**
- Art. 5 Abs. 2 DMA: **Verbot bestimmter Verarbeitungen und Zusammenführung personenbezogener Daten**

„ *„Der **Torwächter** darf*

***a)** personenbezogene Daten von Endnutzern, die Dienste Dritter nutzen, welche zentrale Plattformdienste des Torwächters in Anspruch nehmen, nicht zum Zweck des Betriebs von Online-Werbediensten verarbeiten,*

***b)** personenbezogene Daten aus dem betreffenden zentralen Plattformdienst nicht mit personenbezogenen Daten aus weiteren zentralen Plattformdiensten oder aus anderen vom Torwächter bereitgestellten Diensten oder mit personenbezogenen Daten aus Diensten Dritter zusammenführen,*

***c)** personenbezogene Daten aus dem betreffenden zentralen Plattformdienst nicht in anderen vom Torwächter getrennt bereitgestellten Diensten, einschließlich anderer zentraler Plattformdienste, weiterverwenden und umgekehrt und*

***d)** Endnutzer nicht in anderen Diensten des Torwächters anmelden, um personenbezogene Daten zusammenzuführen,*

außer wenn dem Endnutzer die spezifische Wahl gegeben wurde und er im Sinne des Artikels 4 Nummer 11 und des Artikels 7 der Verordnung (EU) 2016/679 eingewilligt hat.

Wurde die für die Zwecke des Unterabsatz 1 gegebene Einwilligung vom Endnutzer verweigert oder widerrufen, so darf der Torwächter sein Ersuchen um Einwilligung für denselben Zweck innerhalb eines Jahres nicht mehr als einmal wiederholen. Dieser Absatz berührt nicht die Möglichkeit des Torwächters, sich gegebenenfalls auf Artikel 6 Absatz 1 Buchstaben c, d und e der Verordnung (EU) 2016/679 zu berufen.“

i **Hinweis für die Praxis**

In der Praxis besteht die Gefahr, dass diese speziellen Vorgaben auch auf andere Unternehmen übertragen werden.

- Art. 5 Abs. 3 DMA: Verbot von Meistbegünstigungsklauseln
- Art. 5 Abs. 4 DMA: Pflicht zur Erlaubnis der Kommunikation an Endnutzer
- Art. 5 Abs. 5 DMA: Pflicht zur Gestattung von Endnutzer-Zugang zu Services etc. von Business-Nutzer

- Art. 5 Abs. 6 DMA: Verbot der Einschränkung der Rechtsbehelfe gegenüber Nutzern
- Art. 5 Abs. 7 DMA: Koppelungsverbot
- Art. 5 Abs. 8 DMA: Verbot der Verpflichtung zur Registrierung bei anderen zentralen Plattformdiensten des Gatekeepers
- Art. 5 Abs. 8 DMA: Pflicht gegenüber Anzeigenkunden (Advertiser) zum Bereitstellen von Informationen zu Werbepreisen
- Art. 5 Abs. 10 DMA: Pflicht gegenüber Herausgebern (Publisher) zum Bereitstellen von Informationen zu Werbepreisen
- Art. 6 DMA: Verpflichtungen von Gatekeepern, die möglicherweise noch durch Artikel 8 näher ausgeführt werden
- Art. 7 DMA: Verpflichtung von Gatekeepern zur Interoperabilität nummernunabhängiger interpersoneller Kommunikationsdienste

5. Sanktionen (Art. 30 DMA)

In einem Nichteinhaltungsbeschluss kann die Kommission gegen den betreffenden Gatekeeper Geldbußen bis zu einem Höchstbetrag von 10 % seines im vorausgegangenen Geschäftsjahr weltweit erzielten Gesamtumsatzes verhängen, wenn sie feststellt, dass der Gatekeeper vorsätzlich oder fahrlässig eine der in Art. 30 Abs. 1 DMA genannten Pflichten nicht einhält (Art. 30 Abs. 1 DMA).

Ungeachtet des Art. 30 Abs. 1 DMA kann die Kommission im Nichteinhaltungsbeschluss gegen einen Gatekeeper Geldbußen in Höhe von bis zu 20 % seines im vorausgegangenen Geschäftsjahr weltweit erzielten Gesamtumsatzes verhängen, wenn sie feststellt, dass der Gatekeeper eine identische oder ähnliche Zuwiderhandlung gegen eine in Art. 5, 6 oder 7 DMA festgelegte Verpflichtung in Bezug auf denselben zentralen Plattformdienst begangen hat wie eine bereits im Wege eines in den vorangegangenen acht Jahren erlassenen Nichteinhaltungsbeschlusses festgestellte von ihm begangene Zuwiderhandlung (Art. 30 Abs. 2 DMA).

Die Kommission kann einen Beschluss erlassen, mit dem gegen Unternehmen, einschließlich gegebenenfalls Gatekeeper, und Unternehmensvereinigungen Geldbußen bis zu einem Höchstbetrag von 1 % ihres im vorausgegangenen Geschäftsjahr weltweit erzielten Gesamtumsatzes verhängt werden, wenn sie vorsätzlich oder fahrlässig eine der in Art. 30 Abs. 3 DMA genannten Pflichten nicht einhält (Art. 30 Abs. 3 DMA).

Art. 32 DMA (**Verjährungsfrist für die Verhängung von Sanktionen**) regelt die fünfjährige Verjährungsfrist und gestaltet diese aus. Art. 33 DMA regelt die **Verjährungsfrist für die Durchsetzung von Sanktionen** und gestaltet diese aus.

6. Verhältnis zur DS-GVO

Art. 8 Abs. 1 Satz 3 DMA regelt das Verhältnis zum Datenschutzrecht wie folgt: *„[…] Der Torwächter stellt sicher, dass diese Maßnahmen im Einklang mit dem anwendbaren Recht, insbesondere der Verordnung (EU) 2016/679, der Richtlinie 2002/58/EG, […].“*

Die DS-GVO kommt also vollständig zur Anwendung und der Gatekeeper wird durch den DMA zusätzlich hierzu verpflichtet.

C. DATA (SHARING): DATA ACT UND HINWEIS AUF DATA GOVERNANCE ACT

Data Act (DA) und Data Governance Act (DGA) regeln den Zugang zu Daten (Ob des Zugangs) und die rechtlichen Rahmenbedingungen zum Zugang (Wie des Zugangs) zu Daten. Allerdings regelt der DA eine Pflicht zum Teilen von Daten (Ob des Zugangs) und die damit korrespondierende Ausgestaltung des Zugangs (Wie des Zugangs). Der DGA enthält hingegen nur Regelungen zur Ausgestaltung des Zugangs (Wie des Zugangs).

Der DA und der DGA sind keine Datenschutzgesetze. Sie regeln den Umgang mit Daten und definieren diesen Begriff eigenständig und unabhängig vom Datenschutzrecht.

Der DA und der DGA sollen Wettbewerbsbeschränkungen verhindern und dementsprechend das Teilen von Daten fördern. Die Regelungen stehen damit grundsätzlich in einem Spannungsverhältnis zum Datenschutzrecht, wenn personenbezogene Daten betroffen sind.

I. DATA ACT (DA) BZW. DATENVERORDNUNG

Die einleitenden Erwägungsgründe des DA beschreiben seinen Regelungsansatz (Auszüge): In den letzten Jahren haben datengetriebene Technologien transformative Wirkung auf alle Wirtschaftssektoren gehabt. Insbesondere die rasche Verbreitung von Produkten, die mit dem Internet vernetzt sind, hat den Umfang und den potenziellen Wert von Daten für Verbraucher, Unternehmen und Gesellschaft erhöht.

Hindernisse bei der Datenweitergabe verhindern jedoch eine optimale Verteilung der Daten zum Nutzen der Gesellschaft. In Sektoren mit zahlreichen Kleinstunternehmen sowie Kleinunternehmen und mittleren Unternehmen mangelt es häufig an digitalen Kapazitäten und Kompetenzen für die Erhebung, Analyse und Nutzung von Daten; zudem ist der Zugang oftmals eingeschränkt, weil ein einziger Akteur im System die Daten hält oder weil Daten oder Datendienste an sich bzw. über Grenzen hinweg nicht interoperabel sind.

Um den Bedürfnissen der digitalen Wirtschaft gerecht zu werden und die Hindernisse für einen reibungslos funktionierenden Binnenmarkt für Daten zu beseitigen, soll der DA einen harmonisierten Rahmen schaffen.

1. Überblick

Mit der Verordnung (EU) **EU) 2023/2854** des Europäischen Parlaments und des Rates **vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung)** erfolgt eine Regelung des Zugangs zu Daten und zum Abbau von Hindernissen in der Nutzung von Daten infolge von faktischen Machtpositionen. **Trotz seiner Bezeichnung ist der Data Act kein Datenschutzgesetz!**

Der DA ist – anders als etwa die NIS-2-Richtlinie – eine EU-Verordnung und gilt daher unmittelbar und direkt in jedem EU-Mitgliedstaat. Ein Umsetzungsgesetz bedarf es also nicht. Gleichwohl können Durchführungsrechtsakte im nationalen Recht erfolgen wie zum Beispiel die Festlegung der nationalen Aufsichtsbehörde.

Im vorliegenden Buch wird die englische Bezeichnung **Data Act** oder **DA** verwendet, um Missverständnisse mit Blick auf den deutschen Rechtsbegriff „Verordnung" zu vermeiden.

1.1 Worum geht es?

Der DA besteht aus 50 Artikeln und 119 Erwägungsgründen und hat einen Textumfang von 71 DIN-A4-Seiten. Der DA adressiert in seinen verschiedenen Teilen unterschiedliche Regelungsgegenstände und unterschiedliche Adressaten. Die EU-Rechtsakte haben – anders als typischerweise deutsche Gesetze – kein Inhaltsverzeichnis, was eine schnelle Orientierung erschwert.

Der DA enthält Regelungen in Bezug auf

- die Bereitstellung von Produktdaten und verbundenen Dienstdaten für den Nutzer des vernetzten Produkts oder verbundenen Dienstes,
- die Bereitstellung von Daten durch Dateninhaber für Datenempfänger,
- die Bereitstellung von Daten durch Dateninhaber für öffentliche Stellen, die Kommission, die Europäische Zentralbank und Einrichtungen der Union, soweit eine außergewöhnliche Notwendigkeit der Nutzung dieser Daten zur Wahrnehmung einer spezifischen Aufgabe von öffentlichem Interesse besteht,
- die Erleichterung des Wechsels zwischen Datenverarbeitungsdiensten,
- die Einführung von Schutzmaßnahmen gegen den unrechtmäßigen Zugang Dritter zu nicht personenbezogenen Daten und
- die Entwicklung von Interoperabilitätsnormen für Daten, die abgerufen, übertragen und genutzt werden sollen.

Hinweise

Damit wird auch deutlich, dass die jeweiligen Kapitel des DA Unterschiedliches regeln.

Tipp

Verlieren Sie nicht den Überblick: Verschaffen Sie sich anhand des nachfolgenden Inhaltsverzeichnisses einen Überblick über das für Sie Wesentliche und Entscheidende!

Kap.	Artikel des Data Acts	Regelungsinhalt	Maßgaben des Art. 1 Abs. 2 DA sowie ergänzende Hinweise zur Geltung der Regelungen
I	Artt. 1–2 DA	Allgemeine Bestimmungen	
II	Artt. 3–7 DA	Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen	Kapitel II gilt für Daten, mit Ausnahme von Inhalten, die die Leistung, Nutzung und Umgebung von vernetzten Produkten und verbundenen Diensten betreffen.
III	Artt. 8–12 DA	Pflichten der Dateninhaber, die gemäß dem Unionsrecht verpflichtet sind, Daten bereitzustellen	Kapitel III gilt für alle Daten des Privatsektors, die rechtlichen Verpflichtungen mit Blick auf die Datenweitergabe unterliegen. Geltung des **Kapitels III** nur in Bezug auf **Datenbereitstellungspflichten** nach dem Unionsrecht oder nach im Einklang mit Unionsrecht erlassenen nationalen Rechtsvorschriften, **die nach dem 12. September 2025 in Kraft treten.**

IV	Art. 13 DA	Missbräuchliche Vertragsklauseln in Bezug auf den Datenzugang und die Datennutzung zwischen Unternehmen	Kapitel IV gilt für alle Daten des Privatsektors, die auf der Grundlage von Verträgen zwischen Unternehmen abgerufen und genutzt werden. Geltung des **Kapitels IV** nur für **Verträge, die nach dem 12. September 2025** geschlossen wurden.
V	Artt. 14–22 DA	Bereitstellung von Daten für öffentliche Stellen, die Kommission, die europäische Zentralbank und Einrichtungen der Union wegen außergewöhnlicher Notwendigkeit	Kapitel V gilt für alle Daten des Privatsektors mit Schwerpunkt auf nicht personenbezogene Daten.
VI	Artt. 23–31 DA	Wechsel zwischen Datenverarbeitungsdiensten	Kapitel VI gilt für alle von Anbietern von Datenverarbeitungsdiensten verarbeiteten Daten und Dienste.
VII	Art. 32 DA	Unrechtmäßiger staatlicher Zugang zu und unrechtmäßige staatliche Übermittlung von nicht-personenbezogenen Daten im unternationalen Umfeld	Kapitel VII gilt für alle nicht personenbezogenen Daten, die in der Union von Anbietern von Datenverarbeitungsdiensten gehalten werden.
VIII	Artt. 33–36 DA	Interoperabilität	
IX	Artt. 37–42 DA	Anwendung und Durchsetzung	
X	Art. 43 DA	Schutzrecht sui Generis nach der Richtlinie 96/9/EG	
KAPITEL XI	Artt. 44–50 DA	Schlussbestimmungen	

1.2 Zeitstrahl

Inkrafttreten	Anwendungsbeginn	
Januar 2024	**generell: 12.09.2025** (Art. 50 DA) (z. B. Regelungen über das „Cloud Switching" in Kapitel VI)	**12.09.2027:** Geltung des Kapitels IV für Verträge, die am oder vor dem 12. September 2025 geschlossen wurden, sofern a) sie unbefristet sind oder b) ihre Geltungsdauer frühestens 10 Jahre nach dem 11. Januar 2024 endet.
	Geltung des **Art. 3 Abs. 1 DA nur** für vernetzte Produkte und die mit ihnen verbundenen Dienste, **die nach dem 12. September 2026 in Verkehr gebracht wurden.**	
	Geltung des **Kapitels III** nur in Bezug auf **Datenbereitstellungspflichten** nach dem Unionsrecht oder nach im Einklang mit Unionsrecht erlassenen nationalen Rechtsvorschriften, **die nach dem 12. September 2025 in Kraft treten.**	
	Geltung des **Kapitels IV** nur für **Verträge, die nach dem 12. September 2025** geschlossen werden.	

1.3 Begrifflichkeiten und Definitionen

Der DA enthält in seinem Art. 2 Begriffsbestimmungen. Diese Begriffsbestimmungen sind für die Auslegung und Anwendung des Gesetzes von grundlegender Bedeutung.

Sie müssen dabei beachten, dass diese vom allgemeinen oder in der IT üblichen Verständnis dieser Begriffe abweichen können. Der Art. 2 Nr. 8 DA enthält bei-

spielsweise eine Definition des Begriffs „Datenverarbeitungsdienst", der für die Regelung über das Cloud-Switching von entscheidender Bedeutung ist.

Beachten Sie trotz der vermeintlichen Nähe die Unterschiede der Begriffsbestimmungen des DA zur DS-GVO:

Der DA regelt sowohl „Daten" als auch „personenbezogene Daten" sowie „nicht personenbezogene Daten". Der Unterschied wird deutlich, wenn die Definitionen und ihre Bezugnahme beachtet werden:

- **„Daten"** bezeichnet nach **Art. 2 Nr. 1 DA** „jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material".

- **„Nicht personenbezogene Daten"** sind nach **Art. 2 Nr. 4 DA** „Daten, die keine personenbezogenen Daten sind". Diese Definition nimmt Bezug auf den Begriff Daten, wie er in Art. 2 Nr. 1 DA definiert ist. Es geht also um diese digitalen Darstellungen, die jedoch keine personenbezogenen Informationen im Sinne der DS-GVO sind.

- Für den **Begriff „personenbezogene Daten"** verweist Art. 2 Nr. 3 DA auf **Art. 4 Nr. 1 DS-GVO.** Danach sind „personenbezogene Daten" „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann".

Der DA definiert weitere Begriffe, die denen der DS-GVO ähneln, aber dennoch eigenständig definiert sind:

- **„Verarbeitung"** bezeichnet nach **Art. 2 Nr. 7 DA** „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit Daten oder Datensätzen, wie etwa das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, der Abruf, das Abfragen, die Nutzung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung".

- **„Datenempfänger“** ist nach **Art. 2 Nr. 14 DA** „eine natürliche oder juristische Person, die zu Zwecken innerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit handelt, ohne Nutzer eines vernetzten Produktes oder verbundenen Dienstes zu sein, und dem vom Dateninhaber Daten bereitgestellt werden, einschließlich eines Dritten, dem der Dateninhaber auf Verlangen des Nutzers oder im Einklang mit einer rechtlichen Verpflichtung aus anderem Unionsrecht oder aus nationalen Rechtsvorschriften, die im Einklang mit Unionsrecht erlassen wurden, Daten bereitstellt“.

Tipp für die Praxis

Machen Sie sich mit den gesetzlichen Definitionen vertraut. Beachten Sie, dass diese jeweils aus dem jeweiligen Rechtsakt heraus auszulegen sind.

Beachten Sie die Auswirkungen für die Vertragsgestaltung: Diese Definitionen können über das konkrete Gesetz hinaus Bedeutung erlangen. Werden sie beispielsweise in Verträgen verwendet und kommt es für den Vertrag zum Streit über das Verständnis des Begriffs, ist es nicht auszuschließen, dass zukünftig ein Gericht eine solche gesetzliche Definition zur Auslegung heranzieht.

2. Verpflichtete

Der DA gilt nach seinem Art. 1 Abs. 3 für

- Hersteller vernetzter Produkte, die in der Union in Verkehr gebracht werden, und Anbieter verbundener Dienste, unabhängig vom Ort der Niederlassung dieser Hersteller oder Anbieter;
- die Nutzer der unter Buchstabe a genannten vernetzten Produkte oder verbundenen Dienste in der Union;
- Dateninhaber, unabhängig vom Ort ihrer Niederlassung, die Datenempfängern in der Union Daten bereitstellen;
- Datenempfänger in der Union, denen Daten bereitgestellt werden;
- öffentliche Stellen, die Kommission, die Europäische Zentralbank und Einrichtungen der Union, die von Dateninhabern verlangen, Daten bereitzustellen, soweit eine außergewöhnliche Notwendigkeit der Nutzung dieser Daten zur Wahrnehmung einer speziellen Aufgabe im öffentlichen Interesse besteht, sowie die Dateninhaber, die solche Daten auf ein solches Verlangen hin bereitstellen;

- Anbieter von Datenverarbeitungsdiensten, unabhängig vom Ort ihrer Niederlassung, die Kunden in der Union solche Dienste anbieten;
- Teilnehmer an Datenräumen und Anbieter von Anwendungen, die intelligente Verträge verwenden, und Personen, deren gewerbliche, geschäftliche oder berufliche Tätigkeit die Einführung intelligenter Verträge für andere im Zusammenhang mit der Durchführung einer Vereinbarung umfasst.

Hinweis

Die Verpflichteten werden im DA nicht einheitlich für alle Kapitel geregelt.

3. Kapitel II – Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen

Die Ziele sind die Auflösung der De-facto-Kontrolle über IoT-Daten durch Hersteller und sonstige Dateninhaber, Erleichterung des Datenzugangs, Teilhabe an „co-generated data" und Förderung von Data-Aftermarket-Services durch Datenportabilität. Die wesentlichen Pflichten sind:

- Pflicht der Zugänglichmachung von Produktdaten und verbundenen Dienstdaten für den Nutzer **(Art. 3 DA): Data Access by Design**, Vorvertragliche Informationspflichten ...
- Rechte und Pflichten von Nutzern und Dateninhabern in Bezug auf den Zugang zu sowie die Nutzung und die Bereitstellung von Produktdaten und verbundenen Dienstdaten **(Art. 4 DA)**: **Recht des Nutzers auf Zugang und Nutzung von Daten i. S. d. Art. 2 Nr. 1 DA – bei Nutzung erzeugte Daten (ErwGr. 14 DA)**
- Recht des Nutzers auf **Weitergabe von Daten an Dritte** (Art. 5 DA)
- **Pflichten Dritter, die Daten auf Verlangen des Nutzers erhalten** (Art. 6 DA): Beschränkung der Nutzung entsprechend Vereinbarung mit Nutzer
- **Umfang der Pflichten zur Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen** (Art. 7 DA): Ausnahme für Klein-/Kleinstunternehmen

Konflikte zum Datenschutzrecht sind offensichtlich, soweit personenbezogene Daten betroffen sind.

4. Kapitel III – Pflichten der Dateninhaber mit Pflicht zur Datenbereitstellung gemäß Unionsrecht

Das Ziel überschneidet sich mit dem des Kapitels III. Die wesentlichen Pflichten sind:

- **Bedingungen, unter denen Dateninhaber Datenempfängern Daten bereitstellen (Art. 8 DA)**
  - Vorgaben für die Ausgestaltung im B2B sind u. a. missbräuchliche Klauseln, FRAND-Bedingung. FRAND steht für die Vorgaben **F**air, **R**easonable and **N**on **D**iscriminatory terms – also, dass die Vereinbarungen fair, angemessen und diskriminierungsfrei sein müssen.
  - Schutz von Geschäftsgeheimnissen
- **Gegenleistung für die Bereitstellung von Daten (Art. 9 DA)**

  „Jede Gegenleistung, die zwischen einem Dateninhaber und einem Datenempfänger für die Bereitstellung von Daten im Rahmen von Geschäftsbeziehungen zwischen Unternehmen vereinbart wird, muss diskriminierungsfrei und angemessen sein, und darf eine Marge enthalten." (Art. 9 Abs. 1)

  - **Streitbeilegung (Art. 10 DA)**
- **Technische Schutzmaßnahmen über die unbefugte Nutzung oder Offenlegung von Daten (Art. 11 DA)** *(„Dateninhaber kann geeignete technische Schutzmaßnahmen, einschließlich intelligenter Verträge und Verschlüsselung, anwenden, um ..." (Abs. 1))*
- **Umfang der Pflichten bei Pflicht zur Bereitstellung nach Unionsrecht (Art. 12 DA)**

5. Kapitel IV – Missbräuchliche Vertragsklauseln

Durch die Regelungen in Kapitel IV werden die Regelungen des allgemeinen AGB-Rechts sektorspezifisch ergänzt. Art. 13 Abs. 1 DA regelt den Grundsatz, der in den weiteren Regelungen konkretisiert wird: *„Vertragsklauseln in Bezug auf den Datenzugang und die Datennutzung oder die Haftung und Rechtsbehelfe bei Verletzung oder Beendigung datenbezogener Pflichten, die ein Unternehmen einem anderen Unternehmen einseitig auferlegt, sind für letzteres Unternehmen nicht bindend, wenn sie missbräuchlich sind."*

6. Bereitstellung von Daten für öffentliche Stellen, die Kommission, die Europäische Zentralbank und Einrichtungen der Union wegen außergewöhnlicher Notwendigkeit (Kapitel V)

Wenn eine öffentliche Stelle, die Kommission, die Europäische Zentralbank oder eine Einrichtung der Union den Nachweis dafür erbringt, dass im Hinblick auf die Erfüllung ihrer rechtlichen Aufgaben im öffentlichen Interesse die außergewöhnliche Notwendigkeit der Nutzung bestimmter Daten – einschließlich der für die Auslegung und Nutzung dieser Daten erforderlichen betreffenden Metadaten – gemäß Artikel 15 besteht, stellen die Dateninhaber, bei denen sich diese Daten befinden und bei denen es sich um andere juristische Personen als öffentliche Stellen handelt, diese Daten auf ordnungsgemäß begründeten Antrag bereit (Art. 14 DA).

Die weiteren Einzelheiten und vor allem, wann eine solche außergewöhnliche Notwendigkeit angenommen werden kann, regeln die Artt. 15–22 DA.

7. Wechsel zwischen Datenverarbeitungsdienst (Cloud Switching) (Kapitel VI)

Das sogenanntes Cloud Switching wird durch Kapitel VI geregelt. Das Ziel ist die Beseitigung von Hindernissen beim Wechsel des Cloud Providers.

In die Pflicht genommen werden „Anbieter von Datenverarbeitungsdiensten". „Datenverarbeitungsdienst" bezeichnet nach Art. 2 Nr. 8 DA „eine digitale Dienstleistung, die einem Kunden bereitgestellt wird und einen flächendeckenden und auf Abruf verfügbaren Netzzugang zu einem gemeinsam genutzten Pool konfigurierbarer, skalierbarer und elastischer Rechenressourcen zentralisierter, verteilter oder hochgradig verteilter Art ermöglicht, die mit minimalem Verwaltungsaufwand oder minimaler Interaktion des Diensteanbieters rasch bereitgestellt und freigegeben werden können".

Leichter verständlich wird der Adressatenkreis anhand von Erwägungsgrund 81 DA:

> *„Der generische Begriff ‚Datenverarbeitungsdienste' umfasst eine beträchtliche Zahl von Diensten mit einer sehr großen Bandbreite an unterschiedlichen Anwendungszwecken, Funktionen und technischen Strukturen. Nach allgemeinem Verständnis von Anbietern und Nutzern und im Einklang mit weit verbreiteten Standards fallen Datenverarbeitungsdienste unter eines oder mehrere der folgenden drei Modelle für die Bereitstellung von Datenverarbeitungsdiens-*

ten, nämlich ***‚Infrastructure-as-a-Service' (IaaS), ‚Platform-as-a-Service' (PaaS) und ‚Software-as-a-Service' (SaaS).*** *[…]"*

Der Wechsel zwischen Datenverarbeitungsdiensten soll erleichtert werden. Die Ausgangsregelung ist Art. 23 DA. Art. 23 S. 1 DA regelt:

> *„Anbieter von Datenverarbeitungsdiensten treffen die in den Artikeln 25, 26, 27, 29 und 30 vorgesehenen Maßnahmen, um es Kunden zu ermöglichen, zu einem Datenverarbeitungsdienst, der die gleiche Dienstart abdeckt, die von einem anderen Anbieter von Datenverarbeitungsdiensten erbracht wird, oder zu IKT-Infrastruktur in eigenen Räumlichkeiten zu wechseln oder gegebenenfalls mehrere Anbieter von Datenverarbeitungsdiensten gleichzeitig in Anspruch zu nehmen."*

Die „gleiche Dienstart" ist nach Art. 2 Nr. 9 DA „eine Reihe von Datenverarbeitungsdiensten, die dasselbe Hauptziel haben und dasselbe Dienstmodell für die Datenverarbeitung sowie dieselben Hauptfunktionen aufweisen".

Anbieter von Datenverarbeitungsdiensten dürfen nach Art. 23 S. 2 DA insbesondere keine vorkommerziellen, gewerblichen, technischen, vertraglichen und organisatorischen Hindernisse aufzwingen und müssen solche Hindernisse beseitigen, wenn sie die Kunden daran hindern,

- den Vertrag über den Datenverarbeitungsdienst nach der maximalen Kündigungsfrist und nachdem der Wechsel gemäß Artikel 25 erfolgreich vollzogen ist, zu kündigen;
- neue Verträge mit einem anderen Anbieter von Datenverarbeitungsdiensten für die gleiche Dienstart zu schließen;
- exportierbare Daten des Kunden und digitale Vermögenswerte zu einem anderen Anbieter von Datenverarbeitungsdiensten oder zu einer IKT-Infrastruktur in eigenen Räumlichkeiten zu übertragen, auch nach Inanspruchnahme eines unentgeltlichen Angebots;
- gemäß Artikel 24 die Funktionsäquivalenz bei der Nutzung des neuen Datenverarbeitungsdienstes in der IKT-Umgebung eines anderen Anbieters von Datenverarbeitungsdiensten, der die gleiche Dienstart abdeckt, zu erreichen;
- die in Artikel 30 Absatz 1 genannten Datenverarbeitungsdienste von anderen von dem Anbieter von Datenverarbeitungsdiensten erbrachten Datenverarbeitungsdiensten zu trennen, soweit dies technisch durchführbar ist.

Artt. 24–31 DA enthalten dann unter folgenden Überschriften auf rund vier DIN-A4-Seiten weitergehende Konkretisierungen der Pflichten:

- Art. 24 DA: Tragweite der technischen Verpflichtungen
- Art. 25 DA: Vertragsklauseln für den Wechsel
- Art. 26 DA: Informationspflicht der Anbieter von Datenverarbeitungsdiensten
- Art. 27 DA: Verpflichtung zum Handeln nach Treu und Glauben
- Art. 28 DA: Vertragliche Transparenzpflichten in Bezug auf den Zugang und die Übermittlung im internationalen Umfeld
- Art. 29 DA: Schrittweise Abschaffung von Wechselentgelten
- Art. 30 DA: Technische Aspekte des Wechsels
- Art. 31 DA: Spezifische Regelung für bestimmte Datenverarbeitungsdienste

8. Sanktionen

Der DA regelt selbst nicht die Sanktionen. Nach Art. 40 Abs. 1 DA haben die EU-Mitgliedstaaten Vorschriften über Sanktionen, die bei Verstößen gegen diese Verordnung zu verhängen sind, zu erlassen und alle für die Anwendung der Sanktionen erforderlichen Maßnahmen zu treffen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

Allerdings legt Art. 40 Abs. 3 DA Kriterien zur Bemessung der Sanktionen im Einzelfall fest.

Das Verhältnis zu den Datenschutzaufsichtsbehörden regelt Art. 40 Abs. 4 DA. Bei Verstößen gegen die Pflichten der Kapitel II, III und V des DA können die für die Überwachung der Anwendung der DS-GVO zuständigen Aufsichtsbehörden innerhalb ihres Zuständigkeitsbereichs Geldbußen im Einklang mit Art. 83 DS-GVO bis zu dem in Art. 83 Abs. 5 DS-GVO genannten Betrag verhängen.

Für Verstöße gegen Kapitel V enthält Art. 40 Abs. 5 DA eine Parallelregelung zugunsten des Europäischen Datenschutzbeauftragten nach Art. 66 Verordnung (EU) 2018/1725 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union.

9. Verhältnis zur DS-GVO

Das Verhältnis zur DS-GVO regelt Art. 1 Abs. 5 DA wie folgt:

> *„Diese Verordnung gilt* ***unbeschadet*** *des Unionsrechts und des nationalen* ***Rechts über den Schutz personenbezogener Daten, die Privatsphäre, die Vertraulichkeit der Kommunikation und die Integrität von Endgeräten, die für personenbezogene Daten gelten, die im Zusammenhang mit den in der vorliegenden Verordnung festgelegten Rechten und Pflichten verarbeitet werden,*** *insbesondere der Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinie 2002/58/EG, einschließlich der Befugnisse und Zuständigkeiten der Aufsichtsbehörden und der Rechte der betroffenen Personen. Soweit Nutzer* ***betroffene Personen sind, ergänzen die in Kapitel II dieser Verordnung festgelegten Rechte das Auskunftsrecht von betroffenen Personen und das Recht auf Datenübertragbarkeit gemäß Artikel 15 bzw. Artikel 20*** *der Verordnung (EU) 2016/679. Im Falle eines Widerspruchs zwischen der vorliegenden Verordnung und dem Unionsrecht in Bezug auf den Schutz personenbezogener Daten bzw. der Privatsphäre oder den im Einklang mit dem Unionsrecht erlassenen nationalen Rechtsvorschriften* ***haben das Unionsrecht oder das nationale Recht zum Schutz personenbezogener Daten bzw. der Privatsphäre Vorrang.“***

Der Erwägungsgrund 7 des DA enthält umfangreich weitergehende Erläuterungen zum Verhältnis zwischen DA und DS-GVO. Aufgrund der Relevanz des Wortlauts und der noch fehlenden abschließenden Auslegung wird der Text nachfolgend wiedergegeben:

> *„Das* ***Grundrecht auf den Schutz personenbezogener Daten wird insbesondere durch*** *die Verordnungen (EU) 2016/679(6) und (EU) 2018/1725(7) des Europäischen Parlaments und des Rates gewahrt. Die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates (8) s****chützt darüber hinaus die Privatsphäre und die Vertraulichkeit der Kommunikation,*** *unter anderem mittels Bedingungen für die Speicherung personenbezogener und nichtpersonenbezogener Daten auf Endgeräten und den Zugang dazu.* ***Diese Gesetzgebungsakte der Union bilden die Grundlage für eine nachhaltige und verantwortungsvolle Datenverarbeitung, auch wenn Datensätze eine Mischung aus personenbezogenen und nicht-personenbezogenen Daten enthalten.*** *Die vorliegende Verordnung* ***ergänzt das Unionsrecht zum Schutz personenbezogener Daten und zum Schutz der Privatsphä-***

re, *insbesondere die Verordnungen (EU) 2016/679 und (EU) 2018/1725 und die Richtlinie 2002/58/EG, und lässt es unberührt.* ***Keine Bestimmung dieser Verordnung sollte dahingehend angewandt oder ausgelegt werden, dass das Recht auf den Schutz personenbezogener Daten oder das Recht auf Privatsphäre und Vertraulichkeit der Kommunikation abgeschwächt oder eingeschränkt wird.*** *Jegliche Verarbeitung personenbezogener Daten nach dieser Verordnung* ***sollte dem Datenschutzrecht der Union entsprechen, einschließlich*** *dem Erfordernis einer gültigen Rechtsgrundlage für die Verarbeitung gemäß Artikel 6 der Verordnung (EU) 2016/679 und gegebenenfalls den Bedingungen des Artikels 9 der genannten Verordnung und des Artikels 5 Absatz 3 der Richtlinie 2002/58/EG. Die* ***vorliegende Verordnung stellt keine Rechtsgrundlage für die Erhebung oder Generierung personenbezogener Daten durch den Dateninhaber dar.*** *Die vorliegende Verordnung verpflichtet die Dateninhaber, Nutzern Dritten seiner Wahl oder auf Anfrage eines Nutzers personenbezogene Daten bereitzustellen.* ***Ein solcher Zugang sollte im Falle personenbezogener Daten gewährt werden, die vom Dateninhaber auf der Grundlage einer der in Artikel 6 der Verordnung (EU) 2016/679 genannten Rechtsgrundlagen verarbeitet*** *werden. Handelt es sich* ***bei dem Nutzer nicht um die betroffene Person, so bietet die vorliegende Verordnung keine Rechtsgrundlage für die Gewährung des Zugangs zu personenbezogenen Daten oder für deren Bereitstellung an Dritte und sollte nicht so verstanden werden, dass sie dem Dateninhaber ein neues Recht auf die Nutzung personenbezogener Daten,*** *die bei der Nutzung eines vernetzten Produkts oder verbundenen Dienstes generiert wurden, verleiht. In diesen Fällen* ***könnte es im Interesse des Nutzers liegen, die Erfüllung der Anforderungen des Artikels 6 der Verordnung (EU) 2016/679 zu ermöglichen.*** *Da die vorliegende Verordnung die Datenschutzrechte der betroffenen Personen nicht beeinträchtigen sollte, kann der Dateninhaber Datenzugangsverlangen in diesen Fällen unter anderem nachkommen,* ***indem er personenbezogene Daten anonymisiert oder, wenn ohne Weiteres verfügbare Daten personenbezogene Daten mehrerer betroffener Personen enthalten, nur personenbezogene Daten des Nutzers übermittelt.“***

Konsequent ist, dass klargestellt wird, dass der DA keine Rechtsgrundlage für die Erhebung bzw. Generierung von Daten ist. Denn der DA regelt deren Weitergabe. Für die Übermittlung personenbezogener Daten bedarf es einer Rechtsgrundlage im Sinne der DS-GVO. Hierfür kommt insbesondere Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO in Betracht. Verfolgen Sie jedoch die Diskussion, ob und gegebenenfalls

welche Regelungen des DA den hierfür geltenden Anforderungen der Art. 6 Abs. 2 und Abs. 3 DS-GVO genügen.

Bei der Ausübung von Rechten der Betroffenen nach dem DA bestehen Parallelitäten zu Artt. 15 und 20 DS-GVO. Jedoch ersetzen sich die Regelungen nicht wechselseitig, sodass die Regelungen nach beiden Rechtsakten jeweils zu beachten sind.

II. Data Governance Act (DGA)

Ziel des DGA ist die Stärkung des Vertrauens in den Datenaustausch, die Stärkung der Mechanismen zur Erhöhung der Datenverfügbarkeit sowie das Überwinden von technischen Hindernissen für die Weiterverwendung von Daten. Verpflichtet werden durch den DGA öffentliche Stellen, Datenintermediäre und Datenaltruistische Unternehmen.

1. Überblick

Mit der Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt) erfolgt eine Regelung zur Art und Weise der Übertragung von Daten. Der DGA regelt jedoch – anders als der DA – nicht (auch) den Zugang zu den Daten.

Im vorliegenden Buch wird die englische Bezeichnung **Data Governance Act** oder **DGA** verwendet, um Missverständnisse mit Blick auf den deutschen Rechtsbegriff „Verordnung" zu vermeiden.

Der DGA ist – anders als z. B. die NIS-2-Richtlinie – eine EU-Verordnung und gilt daher unmittelbar und direkt in jedem EU-Mitgliedstaat. Ein Umsetzungsgesetz bedarf es also nicht. Gleichwohl können durch Durchführungsrechtsakte im nationalen Recht erfolgen wie zum Beispiel die Festlegung der nationalen Aufsichtsbehörde.

1.1 Worum geht es?

Der DGA besteht aus 38 Artikeln und 63 Erwägungsgründen und hat einen Textumfang von 44 DIN-A4-Seiten. Der DGA adressiert in seinen drei Teilen unterschiedliche Regelungsgegenstände und unterschiedliche Adressaten. Die EU-Rechtsakte haben – anders als typischerweise deutsche Gesetze – kein Inhaltsverzeichnis, was eine schnelle Orientierung erschwert.

Zur Erreichung seiner Ziele hat der DGA drei Gestaltungsansätze:

- Weiterverwendung von Daten bestimmter Datenkategorien im Besitz öffentlicher Stellen innerhalb der Union
- Schaffung vertrauenswürdiger sog. Datenvermittlungsdienste
- Datenaltruismus – Steigerung der Datenverfügbarkeit durch freiwillige Datenspenden.

Tipp

Verlieren Sie nicht den Überblick: Verschaffen Sie sich anhand des nachfolgenden Inhaltsverzeichnisses einen Überblick über das für Sie Wesentliche und Entscheidende!

Kap.	Artikel des DGA	Regelungsinhalt
I	Artt. 1–2 DGA	Allgemeine Bestimmungen
II	Artt. 3–9 DGA	Weiterverwendung bestimmter Kategorien geschützter Daten im Besitz öffentlicher Stellen
III	Artt. 10–15 DGA	Anforderungen an Datenvermittlungsdienste
IV	Artt. 16–25 DGA	Datenaltruismus
V	Artt. 26–28 DGA	Zuständige Behörden und Verfahrensvorschriften
VI	Artt. 29, 30 DGA	Europäischer Dateninnovationsrat
VII	Art. 31 DGA	Internationaler Zugang und internationale Übertragung
VIII	Artt. 32, 33 DGA	Delegierung und Ausschussverfahren
IX	Artt. 34–38 DGA	Schluss- und Übergangsbestimmungen

1.2 Zeitstrahl

Inkrafttreten	Anwendungsbeginn
Juni 2023	24.09.2023

1.3 Begrifflichkeiten und Definitionen

Der DGA enthält in seinem Art. 2 Begriffsbestimmungen. Diese Begriffsbestimmungen sind für die Auslegung und Anwendung des Gesetzes von grundlegender Bedeutung.

Es gelten die Ausführungen zum DA entsprechend. Aber der DGA verweist nicht auf den DA, sondern enthält selbst eigenständige Definitionen für insbesondere

„Daten", „personenbezogene Daten" und „nicht personenbezogene Daten" sowie „Verarbeitung".

Mit Blick auf die DS-GVO ist hervorzuheben, dass der Begriff „Weiterverwendung" in Art. 2 Nr. 2 DGA definiert wird als „die Nutzung von Daten, die im Besitz öffentlicher Stellen sind, durch natürliche oder juristische Personen für kommerzielle oder nicht kommerzielle Zwecke, die sich von dem ursprünglichen Zweck im Rahmen des öffentlichen Auftrags, für den die Daten erstellt wurden, unterscheiden, abgesehen vom Austausch von Daten zwischen öffentlichen Stellen ausschließlich im Rahmen der Erfüllung ihres öffentlichen Auftrags".

Als „gemeinsame Datennutzung" definiert Art. 2 Nr. 10 DGA „die entgeltliche oder unentgeltliche Bereitstellung von Daten durch eine betroffene Person oder einen Dateninhaber an einen Datennutzer für die gemeinschaftliche oder individuelle Nutzung dieser Daten auf der Grundlage freiwilliger Vereinbarungen, des Unionsrechts oder des nationalen Rechts, sowohl direkt als auch über einen Mittler, etwa im Rahmen von gebührenpflichtigen oder gebührenfreien offenen oder kommerziellen Lizenzen".

Tipp für die Praxis

Machen Sie sich mit den gesetzlichen Definitionen vertraut. Beachten Sie, dass diese jeweils aus dem jeweiligen Rechtsakt heraus auszulegen sind.

Beachten Sie die Auswirkungen für die Vertragsgestaltung: Diese Definitionen können über das konkrete Gesetz hinaus Bedeutung erlangen. Werden Sie beispielsweise in Verträgen verwendet und kommt es für den Vertrag zum Streit über das Verständnis des Begriffs, ist es nicht auszuschließen, dass zukünftig ein Gericht eine solche gesetzliche Definition zur Auslegung heranzieht.

2. Weiterverwendung bestimmter Kategorien geschützter Daten im Besitz öffentlicher Stellen (Kapitel II, Artt. 3–9 DGA)

Das Kapitel II des DGA gilt nach seinem Art. 3 für Daten, die sich im Besitz öffentlicher Stellen befinden und aus den in Art. 3 Abs. 1 DGA genannten Gründen geschützt sind. Der DGA begründet weder eine Verpflichtung für öffentliche Stellen, die Weiterverwendung von Daten zu erlauben, noch befreit er öffentliche Stellen von ihren Geheimhaltungspflichten nach dem Unionsrecht oder dem nationalen Recht (Art. 1 Abs. 2 DGA).

Das Kapitel II regelt die Rahmenbedingungen für die Weiterverwendung (zum Begriff siehe oben bei den Begriffsbestimmungen des DGA) von Daten im Sinne des Art. 3 DGA (siehe vorstehend).

Wesentlich sind das in Art. 4 DGA geregelte Verbot von Ausschließlichkeitsvereinbarungen und die in Art. 5 DGA geregelten Bedingungen für die Weiterverwendung. Die Bedingungen für die Weiterverwendung müssen nach Art. 5 Abs. 2 DGA in Bezug auf die Datenkategorien, die Zwecke der Weiterverwendung und die Art der Daten, deren Weiterverwendung erlaubt wird, nichtdiskriminierend, transparent, verhältnismäßig und objektiv gerechtfertigt sein. Diese Bedingungen dürfen nicht der Behinderung des Wettbewerbs dienen.

Die Zielsetzung ist vor allem eine Freiheit von Beschränkungen des Wettbewerbs und nicht zum Beispiel der Datenschutz.

3. Anforderungen an Datenvermittlungsdienste (Kapitel III, Artt. 10–15 DGA)

Das Kapitel soll Datenvermittlungsdienste institutionalisieren und hierzu eine neue Marktstufe im Sinne eines funktionierenden Marktes für Datenvermittlungsdienste zum Datenaustausch schaffen.

Eine vergleichbare Überlegung liegt § 26 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) zugrunde, der jedoch nur sog. Anerkannte Dienste zur Einwilligungsverwaltung regelt.

Art. 2 Nr. 11 DGA enthält für den „Datenvermittlungsdienst“ folgende Definition, die auch die Zielsetzung des Kapitels III verdeutlicht:

> *„einen Dienst, mit dem durch technische, rechtliche oder sonstige Mittel Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von betroffenen Personen oder Dateninhabern einerseits und Datennutzern andererseits hergestellt werden sollen, um die gemeinsame Datennutzung, auch für die Zwecke der Ausübung der Rechte betroffener Personen in Bezug auf personenbezogene Daten, zu ermöglichen, und die zumindest Folgendes nicht umfassen:*
>
> **a)** *Dienste, in deren Rahmen Daten von Dateninhabern eingeholt und aggregiert, angereichert oder umgewandelt werden, um deren Wert erheblich zu steigern, und Lizenzen für die Nutzung der resultierenden Daten an die Datennutzer vergeben werden, ohne eine Geschäftsbeziehung zwischen Dateninhabern und Datennutzern herzustellen;*

> **b)** *Dienste, deren Schwerpunkt auf der Vermittlung urheberrechtlich geschützter Inhalte liegt;*
>
> **c)** *Dienste, die ausschließlich von einem Dateninhaber genutzt werden, um die Verwendung von im Besitz dieses Dateninhabers befindlichen Daten zu ermöglichen, oder die von mehreren juristischen Personen in einer geschlossenen Gruppe, einschließlich Lieferanten- oder Kundenbeziehungen oder vertraglich festgelegter Kooperationen, genutzt werden, insbesondere wenn deren Hauptziel darin besteht, Funktionen von Gegenständen und Geräten im Zusammenhang mit dem Internet der Dinge sicherzustellen;*
>
> **d)** *Datenvermittlungsdienste, die von öffentlichen Stellen ohne die Absicht der Herstellung von Geschäftsbeziehungen angeboten werden."*

Der „Dateninhaber" ist nach Art. 2 Nr. 8 DGA „eine juristische Person, einschließlich öffentlicher Stellen und internationaler Organisationen oder einer natürlichen Person, die in Bezug auf die betreffenden Daten keine betroffene Person ist, welche nach geltendem Unionsrecht oder geltendem nationalen Recht berechtigt ist, Zugang zu bestimmten personenbezogenen Daten oder nicht personenbezogenen Daten zu gewähren oder diese Daten weiterzugeben".

Ein „Datennutzer" ist nach Art. 2 Nr. 9 DGA „eine natürliche oder juristische Person, die rechtmäßig Zugang zu bestimmten personenbezogenen oder nicht personenbezogenen Daten hat und im Fall personenbezogener Daten, unter anderem nach der Verordnung (EU) 2016/679, berechtigt ist, diese Daten für kommerzielle oder nichtkommerzielle Zwecke zu nutzen".

Die Regelungen der Artt. 11–15 DGA gelten jedoch nur für Datenvermittlungsdienste im Sinne des Art. 10 DGA. Dieser sieht vor, dass die Erbringung der dort genannten Datenvermittlungsdienste gemäß Artikel 12 DGA erfolgt und einem Anmeldeverfahren unterliegt.

Aufgeführt sind in Art. 10 DGA, womit der Anwendungsbereich der Regelungen weitergehend beschränkt wird:

- Vermittlungsdienste zwischen Dateninhabern und potenziellen Datennutzern, einschließlich Bereitstellung der technischen oder sonstigen Mittel als Voraussetzung solcher Dienste; zu diesen Diensten können auch der zwei- oder mehrseitige Austausch von Daten oder die Einrichtung von Plattformen oder Datenbanken, die den Austausch oder die gemeinsame Nutzung von Daten ermöglichen, sowie die Einrichtung anderer spezieller Infrastrukturen für die Vernetzung von Dateninhabern mit Datennutzern gehören (Art. 10 lit. a DGA);

- Vermittlungsdienste zwischen betroffenen Personen, die ihre personenbezogenen Daten zugänglich machen wollen, oder natürlichen Personen, die nicht personenbezogene Daten zugänglich machen wollen, und potenziellen Datennutzern, einschließlich Bereitstellung der technischen oder sonstigen Mittel als Voraussetzung dieser Dienste, sowie insbesondere Ermöglichung der Ausübung der in der Verordnung (EU) 2016/679 verankerten Rechte betroffener Personen (Art. 10 lit. b DGA);
- Dienste von Datengenossenschaften (Art. 10 lit. c DGA).

Art. 11 DGA regelt das Anmeldeverfahren für diese Dienste. Art. 12 DGA sieht 15 Anforderungen vor, die durch diesen Dienst erfüllt werden müssen.

4. Datenaltruismus (Kapitel IV, Artt. 16–25 DGA)

Kapitel IV DGA regelt schließlich den sog. Altruismus. Wie die anderen Kapitel regelt er nur die Rahmenbedingung für die Bereitstellung von Daten.

Art. 2 Nr. 16 DGA definiert den Begriff des Datenaltruismus. Die Definition macht auch den Regelungsansatz und -gegenstand deutlich: *„die freiwillige gemeinsame Nutzung von Daten auf der Grundlage der Einwilligung betroffener Personen zur Verarbeitung der sie betreffenden personenbezogenen Daten oder einer Erlaubnis anderer Dateninhaber zur Nutzung ihrer nicht personenbezogenen Daten, ohne hierfür ein Entgelt zu fordern oder zu erhalten, das über eine Entschädigung für die ihnen durch die Bereitstellung ihrer Daten entstandenen Kosten hinausgeht, für Ziele von allgemeinem Interesse gemäß dem nationalen Recht, wie die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität, die einfachere Entwicklung, Erstellung und Verbreitung amtlicher Statistiken, die Verbesserung der Erbringung öffentlicher Dienstleistungen, die staatliche Entscheidungsfindung oder die wissenschaftliche Forschung im allgemeinen Interesse“.*

Das Kapitel IV regelt die Anforderungen und Rahmenbedingungen für die Errichtung der anerkannten datenaltruistischen Organisationen.

Nach Art. 16 DGA können die Mitgliedstaaten organisatorische oder technische Regelungen oder beides festlegen, um Datenaltruismus zu erleichtern. Hierzu können die Mitgliedstaaten nationale Strategien für Datenaltruismus festlegen. Diese nationalen Strategien können insbesondere dazu dienen, betroffene Personen dabei zu unterstützen, sie betreffende personenbezogene Daten im Besitz öffentlicher Stellen freiwillig für den Datenaltruismus zur Verfügung zu stellen, und die erforderlichen Informationen festzulegen, die betroffenen Personen in Bezug

auf die Weiterverwendung ihrer Daten im allgemeinen Interesse zur Verfügung gestellt werden müssen. Das Verfahren zur Anerkennung regeln die Art. 17–21 DGA.

Der materiell-rechtliche Vorteil der Anerkennung für die Organisationen besteht darin, dass sie nach Art. 15 DGA von den Regelungen des Kapitels III über die Datenvermittlungsdienste freigestellt sind.

5. Verhältnis zur DS-GVO

Das Verhältnis zur DS-GVO wird durch Art. 1 Abs. 3 DGA wie folgt geregelt:

> *„Das Unionsrecht und das nationale Recht über den Schutz personenbezogener Daten* ***gelten für alle personenbezogenen Daten, die im Zusammenhang mit der vorliegenden Verordnung verarbeitet*** *werden. Insbesondere* ***gilt die vorliegende Verordnung unbeschadet der Verordnungen (EU) 2016/679 und*** *(EU) 2018/1725 und der Richtlinien 2002/58/EG und (EU) 2016/680, einschließlich im Hinblick auf die Befugnisse der Aufsichtsbehörden.* ***Im Fall eines Konflikts zwischen*** *der vorliegenden Verordnung und dem Unionsrecht über den Schutz personenbezogener Daten oder dem entsprechend diesem Unionsrecht erlassenen nationalen Recht soll das* ***einschlägige Unionsrecht bzw. das nationale Recht über den Schutz personenbezogener Daten Vorrang*** *haben. Die* ***vorliegende Verordnung schafft keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten****, noch berührt es die in den Verordnungen (EU) 2016/679 oder (EU) 2018/1725 oder den Richtlinien 2002/58/EG oder (EU) 2016/680 festgelegten Rechte und Pflichten."*
>
> *Der DGA sieht in Erwägungsgrund 4 DGA ergänzende Erläuterungen vor. Aufgrund der Relevanz des konkreten Wortlauts wird dieser nachfolgend wiedergegeben:*

> *„Diese Verordnung sollte die Verordnungen (EU) 2016/679 und (EU) 2018/1725 des Europäischen Parlaments und des Rates sowie die Richtlinien 2002/58/EG und (EU) 2016/680 des Europäischen Parlaments und des Rates und die entsprechenden Bestimmungen des nationalen Rechts unberührt lassen,* ***einschließlich in den Fällen, in denen personenbezogene und nicht personenbezogene Daten in einem Datensatz untrennbar miteinander verbunden sind****. Insbesondere sollte mit dieser Verordnung* ***keine neue Rechtsgrundlage für die Verarbeitung personenbezogener Daten für irgendeine der regulierten Tätigkeiten geschaffen werden bzw. keine Änderung der Informationsanforderungen gemäß der Verordnung (EU) 2016/679 bewirkt***

werden. *Die Durchführung dieser Verordnung sollte der grenzüberschreitenden Datenübertragung* ***im Einklang mit Kapitel V der Verordnung (EU) 2016/679*** *nicht im Wege stehen. Im Fall eines Konflikts zwischen dieser Verordnung und dem Unionsrecht über den Schutz personenbezogener Daten oder dem gemäß diesem Unionsrecht erlassenen nationalen Recht sollte das einschlägige Unionsrecht oder das nationale Recht über den Schutz personenbezogener Daten Vorrang haben. Es sollte möglich sein, Datenschutzbehörden als gemäß dieser Verordnung zuständige Behörden zu betrachten.* ***Wenn andere Behörden als zuständige Behörden gemäß dieser Verordnung handeln, sollten dabei die Aufsichtsbefugnisse und -zuständigkeiten der Datenschutzbehörden gemäß der Verordnung (EU) 2016/679 davon unberührt bleiben.***"

D. KÜNSTLICHE INTELLIGENZ: AI ACT

Der Einsatz von Künstlicher Intelligenz hat seit Mitte 2022 durch ChatGPT eine breite Aufmerksamkeit erfahren. Die Entwicklung und der Einsatz von Künstlicher Intelligenz erfolgen jedoch bereits seit den 1950er Jahren.

1. Überblick

Mit der **Verordnung (EU) 2024/1689** des Europäischen Parlaments und des Rates vom 13.06.2024 zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (**Verordnung über Künstliche Intelligenz)** erfolgt weltweit erstmalig eine Regelung der Herstellung und des Einsatzes von Künstlicher Intelligenz.

Im vorliegenden Buch wird die englische Bezeichnung **Artificial Intelligence Act** oder **AI Act** verwendet, um Missverständnisse mit Blick auf den deutschen Rechtsbegriff „Verordnung" zu vermeiden.

Der AI Act ist **kein „Datenschutz 2.0".** Der AI Act hat nicht den Schutz personenbezogener Daten zum Gegenstand, sondern soll als **Produktsicherheitsrecht** die von KI-Systemen und KI-Modellen mit allgemeinem Verwendungszweck ausgehenden Risiken beherrschbar machen.

1.1 Worum geht es?

Der AI Act soll Rahmenbedingungen für die sichere Entwicklung, den Vertrieb und die Verwendung von KI-Systemen schaffen. Er regelt daher auch die gesamte Wertschöpfungskette. Er verfolgt einen risikobasierten Ansatz, indem der AI Act unterschiedliche Risikostufen definiert und unterschiedliche Regelungen für diese vorsieht. KI-Systeme mit hohem Risiko (Art. 6 AI Act) sind – wie schon der Textumfang zeigt – der Regelungsschwerpunkt des AI Acts. Erst „auf den letzten Metern" des Gesetzgebungsverfahrens sind Regelungen für KI-Modelle mit allgemeinem Verwendungszweck in einem eigenständigen Kapitel eingefügt worden.

Der AI Act besteht aus 113 Artikeln, 180 Erwägungsgründen, 13 Anhängen und hat einen Textumfang von 144 DIN-A4-Seiten. Der AI Act adressiert in seinen verschiedenen Teilen unterschiedliche Regelungsgegenstände und unterschiedliche Adressaten. Die EU-Rechtsakte haben – anders als typischerweise deutsche Gesetze – kein Inhaltsverzeichnis, was eine schnelle Orientierung erschwert.

Tipp

Verlieren Sie nicht den Überblick: Verschaffen Sie sich anhand des nachfolgenden Inhaltsverzeichnisses einen Überblick über das für Sie Wesentliche und Entscheidende!

Kap.	Überschrift der Regelungen	Anmerkungen
I	Allgemeine Bestimmungen (Artt. 1–4 AI Act)	Anwendungsbeginn: 2.2.2025.
II	Verbotene Praktiken im KI-Bereich (Art. 5 AI Act)	Anwendungsbeginn: 2.2.2025.
III	Hochrisiko-KI-Systeme (Artt. 6–49 AI Act)	Hochrisiko-KI-Systeme sind KI-Systeme im Sinne des Art. 3 Nr. 1 AI Act, die Voraussetzungen des Art. 6 AI Act erfüllen.
IV	Transparenzpflichten für Anbieter und Betreiber bestimmter KI-Systeme (Art. 50 AI Act)	Kapitel IV adressiert die generativen KI-Systeme und sieht für sie bestimmte Transparenzpflichten vor.
V	KI-Modelle mit allgemeinem Verwendungszweck (Artt. 51–56 AI Act)	KI-Modelle sind von den vor allem in Kapitel II, III und IV regulierten KI-Systemen zu unterscheiden. Kapitel V erfasst auch nicht alle KI-Modelle, sondern nur solche mit allgemeinem Verwendungszweck (Stichwort: General Purpose AI).
VI	Maßnahmen zur Innovationsförderung (Artt. 57–63 AI Act)	
VII	Governance (Artt. 64–70 AI Act)	Regelungen zur staatlichen Aufsicht.
	Governance auf EU-Ebene (Artt. 64–69 AI Act)	
	Zuständige nationale Behörden (Artt. 70 AI Act)	
VIII	EU-Datenbank für Hochrisiko-KI-Systeme (Art. 71 AI Act)	Die Anbieter müssen die Hochrisiko-KI-Systeme in diese Datenbank melden.

IX	Beobachtung nach dem Inverkehrbringen, Informationsaua-tausch, Marktüberwachung (Artt. 72–94 AI Act)	Hier wird der Charakter des AI Act als Produktsicherheitsrecht besonders deutlich.
X	Verhaltenskodizes und Leitlinien (Artt. 95, 96 AI Act)	
XI	Befugnisübertragung und Ausschussverfahren (Artt. 97–98 AI Act)	
XII	Sanktionen (Artt. 99–101 AI Act)	Vorgaben zur Ausgestaltung der Bußgeldbestimmungen, insbesondere in Bezug auf die Höhe der Bußgelder.
XIII	Schlussbestimmungen (Artt. 102–113 AI Act)	Insbesondere: Regelungen zum Bestandsschutz und Anwendungsbeginn.
Anhänge I–XIII		Insbesondere: Konkretisierung zu Art. 6 durch Anhänge I und II. Konkretisierung zu Art. 5 durch Anhang II.

1.2 Zeitstrahl

Der AI Act ist Mitte 2024 in Kraft getreten und sieht Übergangsfristen bis zu seinem Anwendungsbeginn vor. Grundsätzlich sind die Regelungen des AI Act erst ab dem 02.08.2026 anwendbar. Aber bereits am 02.02.2025 sind die Regelungen in Artt. 1–5 AI Act anwendbar. **Art. 113 AI Act** regelt den **Anwendungsbeginn**. Für bestimmte KI-Systeme ist in **Art.** 111 AI Act ein **Bestandsschutz** geregelt. Verdeutlichen Sie sich das anhand des nachfolgenden Zeitstrahls:

02.02.2025	02.08.2025	02.08.2026	02.08.2027	Bestands-schutz bis 2027 bzw. 2030
Artt. 1–5 AI Act	Kapitel III Abschnitt 4 (Notifizierende Behörden und notifizierte Stellen – Artt. 28–39 AI Act) **Kapitel V (KI-Modelle mit allgemeinem Verwendungszweck (Artt. 51–56 AI Act))** Kapitel VII (Governance (Artt. 64–70 AI Act)) Kapitel XII (Sanktionen (Artt. 99–101 AI Act)) mit Ausnahme des Artikels 101 (Geldbußen für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck) Art. 78 (Vertraulichkeit)	**Alle Regelungen im Übrigen (mit Ausnahme des Art. 6 Abs. 1 AI Act)** (Art. 101 AI Act gilt ebenfalls ab dem 02.08.2026)	Pflichten für Hochrisiko-KI-Systeme im Sinne des Artikels 6 **Abs. 1 AI Act**	**Art. 111 AI Act: Bestandsschutz** für bereits in Verkehr gebrachte oder in Betrieb genommene KI-Systeme, bereits in Verkehr gebrachte KI-Modelle mit allgemeinem Verwendungszweck Ausnahme: Kein Bestandsschutz für verbotene Praktiken im Sinne des Art. 5 AI Act.

1.3 Begrifflichkeiten und Definition

Der AI Act enthält in seinem Art. 3 Begriffsbestimmungen. Diese Begriffsbestimmungen sind für die Auslegung und Anwendung des Gesetzes von grundlegender Bedeutung.

Sie müssen dabei beachten, dass diese vom allgemeinen oder in der IT üblichen Verständnis dieser Begriffe abweichen können. Beispielsweise ist die Definition des Begriffs KI-System in Art. 3 Nr. 1 AI Act nicht deckungsgleich mit dem Begriff Künstliche Intelligenz. Auch werden die für den AI Act wesentlichen Begriffe „Anbieter“ und „Betreiber“ eigenständig und nicht in Übereinstimmung mit dem möglicherweise allgemeinen Sprachgebrauch oder beispielsweise dem Telekommunikationsgesetz (TKG) definiert.

Art. 3 AI Act enthält die Begriffsbestimmungen für die Begriffe, die über die **Anwendung des AI Acts (siehe nachfolgend Ziffer 2)** und die **Pflichtenstellung (siehe nachfolgend Ziffer 3)** entscheiden.

Er enthält aber auch weitere wesentliche Begriffe. Hier tritt besonders der **Begriff „Zweckbestimmung"** hervor. Die Zweckbestimmung ist auch für die Anwendung der DS-GVO von entscheidender Bedeutung (vgl. Art. 5 Abs. 1 lit. b DS-GVO). Gerade deshalb ist es wesentlich, dass Sie deutlich machen, dass die **Begriffe im AI Act und der DS-GVO nicht deckungsgleich** sind.

„Zweckbestimmung" im Sinne des AI Act ist nach Art. 3 Nr. 12 AI Act „die Verwendung, für die ein KI-System laut Anbieter bestimmt ist, einschließlich der besonderen Umstände und Bedingungen für die Verwendung, entsprechend den vom Anbieter bereitgestellten Informationen in den Betriebsanleitungen, im Werbe- oder Verkaufsmaterial und in diesbezüglichen Erklärungen sowie in der technischen Dokumentation". Der Anbieter legt also die Zweckbestimmung fest. Diese Festlegung ist insbesondere für die Regelungen zu Hochrisiko-KI-Systemen in Kapitel III des AI Act sowie für den durch den Autor bildlich bezeichneten „Rollenwechsel" nach Art. 25 AI Act vom Betreiber zum Anbieter entscheidend.

Der **Begriff „Einwilligung"** ist beispielsweise in Art. 3 Nr. 59 AI Act ebenfalls eigenständig und ohne Bezugnahme auf Art. 4 Nr. 11 DS-GVO definiert.

Tipp für die Praxis

Machen Sie sich mit den gesetzlichen Definitionen vertraut. Beachten Sie, dass diese immer aus dem jeweiligen Rechtsakt heraus auszulegen sind.

Beachten Sie die Auswirkungen für die Vertragsgestaltung: Diese Definitionen können über das konkrete Gesetz hinaus Bedeutung erlangen. Werden sie beispielsweise in Verträgen verwendet und kommt es beim Vertrag zum Streit über das Verständnis des Begriffs, ist es nicht auszuschließen, dass zukünftig ein Gericht eine solche gesetzliche Definition zur Auslegung heranzieht.

2. Was regelt der AI Act? – Was sind KI-Systeme und KI-Modelle mit allgemeinem Verwendungszweck?

Der AI Act regelt KI-Systeme und KI-Modelle mit allgemeinem Verwendungszweck. Je nach Tätigkeit treffen die Unternehmen (siehe hierzu nachfolgend Ziffer 3) unterschiedliche Pflichten. **Nur wenn ein KI-System oder** KI-Modell mit

allgemeinem Verwendungszweck **gegeben ist, kommt der AI Act zur Anwendung (vgl. Art. 2 Abs. 1 AI Act).**

Relevanz des Wortlauts des AI Acts für die Praxis: Der Wortlaut der Definitionen des **AI Acts sowie der Beschreibung in den Erwägungsgründen ist wichtig, da deren Verständnis noch nicht eindeutig geklärt ist und jede zukünftige Diskussion sich am Wortlaut auszurichten hat.**

2.1 KI-System

Was ein „KI-System" ist, wird in Art. 3 Nr. 1 AI Act wie folgt definiert:

> *„ein maschinengestütztes System, das für einen in unterschiedlicher Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können".*

Die Definition zeigt zunächst, dass sich der Gesetzgeber von der Diskussion darüber, was Künstliche Intelligenz als solche ist, abgrenzt. Erforderlich ist nach der Definition eine Ergebnisausgabe sowie dass das System über eine hinreichende Autonomie zur Erstellung dieses Ergebnisses verfügen muss. Diese Autonomie hat die Definition mit der Diskussion um den Begriff „Künstliche Intelligenz" gemeinsam.

Bei der Auslegung dieser recht abstrakten Definition hilft Erwägungsgrund 12 AI Act weiter. Folgende Auszüge aus dem Erwägungsgrund 12 AI Act treten hierbei für das Verständnis hervor (Hervorhebung nur hier, nicht auch im AI Act):

- „Darüber hinaus sollte die Begriffsbestimmung auf den wesentlichen Merkmalen der KI beruhen, die sie **von einfacheren herkömmlichen Softwaresystemen und Programmierungsansätzen abgrenzen**, und sollte sich **nicht auf Systeme beziehen, die auf ausschließlich von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen beruhen**."
- *„Ein wesentliches Merkmal von KI-Systemen ist **ihre Fähigkeit, abzuleiten**. Diese Fähigkeit **bezieht sich auf den Prozess der Erzeugung von Ausgaben, wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen, die physische und digitale Umgebungen beeinflussen können, sowie auf die Fähigkeit von KI-Systemen, Modelle oder Algorithmen oder beides aus Eingaben***

oder Daten abzuleiten. *Zu den Techniken, die während der Gestaltung eines KI-Systems das Ableiten ermöglichen, gehören* ***Ansätze für maschinelles Lernen, wobei aus Daten gelernt wird, wie bestimmte Ziele erreicht werden können, sowie logik- und wissensgestützte Konzepte, wobei aus kodierten Informationen oder symbolischen Darstellungen der zu lösenden Aufgabe abgeleitet wird****. Die Fähigkeit eines KI-Systems, abzuleiten,* ***geht über die einfache Datenverarbeitung hinaus, indem Lern-, Schlussfolgerungs- und Modellierungsprozesse ermöglicht werden****."*

- *„Die* ***Bezeichnung ‚maschinenbasiert' bezieht sich auf die Tatsache, dass KI-Systeme von Maschinen betrieben werden****. Durch die Bezugnahme auf explizite oder implizite Ziele wird betont, dass KI-Systeme gemäß explizit festgelegten Zielen oder gemäß impliziten Zielen arbeiten können. Die Ziele des KI-Systems können sich — unter bestimmten Umständen — von der Zweckbestimmung des KI-Systems unterscheiden. Für die Zwecke dieser Verordnung sollten Umgebungen als Kontexte verstanden werden, in denen KI-Systeme betrieben werden, während die von einem KI-System erzeugten Ausgaben verschiedene Funktionen von KI-Systemen widerspiegeln, darunter Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen."*

- ***„KI-Systeme sind mit verschiedenen Graden der Autonomie ausgestattet, was bedeutet, dass sie bis zu einem gewissen Grad unabhängig von menschlichem Zutun agieren und in der Lage sind, ohne menschliches Eingreifen zu arbeiten.*** *Die Anpassungsfähigkeit, die ein KI-System nach Inbetriebnahme aufweisen könnte, bezieht sich auf seine Lernfähigkeit, durch sie es sich während seiner Verwendung verändern kann. KI-Systeme können* ***eigenständig oder als Bestandteil eines Produkts*** *verwendet werden, unabhängig davon, ob das System physisch in das Produkt integriert (eingebettet) ist oder der Funktion des Produkts dient, ohne darin integriert zu sein (nicht eingebettet)."*

Beispiele: ChatGPT ist sicherlich ein sehr bekanntes KI-System, aber auch Microsoft Copilot fällt hierunter. Ebenso können weitere Chatbots hierunter fallen sowie Viren- und Spam-Filter-Systeme und Rechtschreib- und Grammatik-Korrektur-Programme.

Ein **Hochrisiko-KI-System** ist kein eigenständiges KI-System, sondern ein KI-System im vorstehenden Sinn, das die Kriterien des Art. 6 AI Act erfüllt, wodurch es dem risikobasierten Ansatz des AI Act als Hochrisiko-KI-System eingeordnet wird und die Pflichten nach Artt. 8 ff. AI Act zu beachten sind und nicht beispielsweise nicht nur die Transparenzpflichten nach Art. 50 AI Act.

2.2 KI-Modell mit allgemeinem Verwendungszweck

KI-Systeme und KI-Modelle sind nicht nur begrifflich zu unterscheiden, sie unterscheiden sich auch inhaltlich und es kommen unterschiedliche Regelungen des AI Act zur Anwendung. Nur für KI-Modelle gelten die Regelungen in Kapitel V des AI Act. KI-Modelle sind selbst keine KI-Systeme, sondern Bestandteile von KI-Systemen.

Ein „KI-Modell mit allgemeinem Verwendungszweck" ist nach der gesetzlichen Definition in Art. 3 Nr. 63 AI Act

> *„ein KI-Modell – einschließlich der Fälle, in denen ein solches KI-Modell mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert wird –, das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann, ausgenommen KI-Modelle, die vor ihrem Inverkehrbringen für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen eingesetzt werden".*

GPT ist ein Beispiel hierfür. Während ChatGPT ein KI-System ist, ist GPT in der jeweiligen Version das KI-Modell, das zugrunde liegt.

Was ein „KI-Modell" ist, wird in Art. 3 AI Act nicht definiert. Die Erwägungsgründe 97–100 AI Act können jedoch zum besseren Verständnis herangezogen werden. Auszugsweise werden diese nachfolgend wiedergegeben:

- *„(97) Der* ***Begriff „KI-Modelle mit allgemeinem Verwendungszweck" sollte […] vom Begriff der KI-Systeme abgegrenzt werden****, um Rechtssicherheit zu schaffen. Die Begriffsbestimmung sollte auf den wesentlichen funktionalen Merkmalen eines KI-Modells mit allgemeinem Verwendungszweck beruhen, insbesondere* ***auf der allgemeinen Verwendbarkeit und der Fähigkeit, ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen****. Diese Modelle werden* ***in der Regel mit großen Datenmengen durch verschiedene Methoden, etwa überwachtes, unüberwachtes und bestärkendes Lernen, trainiert.*** *[…] Obwohl KI-Modelle wesentliche Komponenten von KI-Systemen sind, stellen sie für sich genommen keine KI-Systeme dar.* ***Damit KI-Modelle zu KI-Systemen werden, ist die Hinzufügung weiterer Komponenten, zum Beispiel einer Nutzerschnittstelle, erforderlich. KI-Modelle sind in der Regel in KI-Systeme integriert und Teil davon.*** *[…]"*

- *„(98) Die allgemeine Verwendbarkeit eines Modells könnte zwar unter anderem auch durch eine bestimmte Anzahl von Parametern bestimmt werden, doch sollten* ***Modelle mit mindestens einer Milliarde Parametern, die mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert werden, als Modelle gelten, die eine erhebliche allgemeine Verwendbarkeit*** *aufweisen und ein breites Spektrum unterschiedlicher Aufgaben kompetent erfüllen."*

- *„(99)* ***Große generative KI-Modelle*** *sind ein typisches Beispiel für ein KI-Modell mit allgemeinem Verwendungszweck, da sie eine flexible Erzeugung von Inhalten ermöglichen, etwa in Form von Text-, Audio-, Bild- oder Videoinhalten, die leicht ein breites Spektrum unterschiedlicher Aufgaben umfassen können."*

- *„(100) Wenn ein* ***KI-Modell mit allgemeinem Verwendungszweck in ein KI-System integriert oder Teil*** *davon ist, sollte dieses System als KI-System mit allgemeinem Verwendungszweck gelten, wenn dieses System aufgrund dieser Integration in der Lage ist, einer Vielzahl von Zwecken zu dienen. Ein KI-System mit allgemeinem Verwendungszweck kann direkt eingesetzt oder in andere KI-Systeme integriert werden."*

Ein „**KI-System mit allgemeinem Verwendungszweck**" ist nach Art. 3 Nr. 66 AI Act „ein KI-System, das auf einem KI-Modell mit allgemeinem Verwendungszweck beruht und in der Lage ist, einer Vielzahl von Zwecken sowohl für die direkte Verwendung als auch für die Integration in andere KI-Systeme zu dienen".

Hinweis für die Praxis

Unterscheiden Sie die Begriffe KI-System (einschließlich KI-System mit allgemeinem Verwendungszweck) einerseits und KI-Modell (einschließlich KI-Modell mit allgemeinem Verwendungszweck) andererseits. Denn vereinfacht gesagt: Für die KI-Modelle mit allgemeinem Verwendungszweck gilt Kapitel V und für die KI-Systeme alle anderen Regelungen.

2.3 Ausnahmen

Ausnahmen von seiner Geltung regelt der AI Act in Art. 2 Abs. 2 bis Abs. 12 AI Act:

- Nach Art. 2 Abs. 2 AI Act gelten für die KI-Systeme, die als **Hochrisiko-KI-Systeme gemäß Art. 6 Absatz 1 eingestuft sind und im Zusammenhang mit Produkten stehen, die unter die in Anhang I Abschnitt B aufgeführten Harmonisierungsrechtsvorschriften der Union fallen**, nur Art. 6 Absatz 1, die Artt. 102–109 und Art. 112. Art. 57 gilt nur, soweit die Anforderungen an

Hochrisiko-KI-Systeme gemäß dieser Verordnung im Rahmen der genannten Harmonisierungsrechtsvorschriften der Union eingebunden wurden.

- Art. 2 Abs. 3 AI Act nimmt den Bereich der **öffentlichen Sicherheit und Verteidigung** aus.
- Ausnahmen für **Behörden in Drittländern und internationale Organisationen** sieht Art. 2 Abs. 4 AI Act vor.
- Art. 2 Abs. 5 AI Act stellt klar, dass Bestimmungen über die **Haftung der Anbieter von Vermittlungsdiensten in Kapitel II des Digital Services Act** von dem AI Act unberührt bleiben.
- Art. 2 Abs. 6 AI Act sieht Ausnahmen für KI-Systeme und KI-Modelle vor, die eigens für den **alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung** entwickelt und in Betrieb genommen werden.
- Art. 2 Abs. 7 AI Act regelt den grundsätzlichen **Vorrang der DS-GVO**.
- Für **Forschungs-, Test- und Entwicklungstätigkeiten zu KI-Systemen oder KI-Modellen** gilt der AI Act nach Art. 2 Abs. 8 AI Act generell nicht, bevor diese in Verkehr gebracht oder in Betrieb genommen werden. Tests unter Realbedingungen sind jedoch nicht ausgenommen, womit der AI Act hierfür gilt.
- Nach Art. 2 Abs. 9 AI bleiben die Vorschriften anderer Rechtsakte der Union zum Verbraucherschutz und zur Produktsicherheit unberührt.
- Das sog. **Haushaltsprivileg** ist in Art. 2 Abs. 10 des AI Acts geregelt. Der AI Act gilt nicht für die Pflichten von Betreibern, die natürliche Personen sind und KI-Systeme im Rahmen einer ausschließlich persönlichen und nicht beruflichen Tätigkeit verwenden. Die Ausnahme besteht jedoch nur für Betreiber, nicht auch für beispielsweise Anbieter.
- Der AI Act hindert die Union oder die Mitgliedstaaten nicht daran, Rechts- oder Verwaltungsvorschriften beizubehalten oder einzuführen, die für die Arbeitnehmer im Hinblick auf den Schutz ihrer Rechte bei der Verwendung von KI-Systemen durch die Arbeitgeber vorteilhafter sind, oder die Anwendung von Kollektivvereinbarungen zu fördern oder zuzulassen, die für die Arbeitnehmer vorteilhafter sind (Art. 2 Abs. 11 AI Act). Dies ließe sich überspitzt als **Vorrang des Arbeitsrechts** umschreiben.
- Die **Nutzung von Open Source** wird durch Art. 22 Abs. 12 AI Act privilegiert. Die Privilegierung gilt nicht für Hochrisiko-KI-Systeme, KI-Systeme, die unter Art. 5 AI Act (verbotene Praktiken) oder Art. 50 AI Act (**Transparenzpflichten für Anbieter und Betreiber bestimmter KI-Systeme**) fallen.

3. Verpflichtete des AI Act

Der AI Act nimmt die gesamte Wertschöpfungskette der KI-Systeme von der Herstellung bis zur Nutzung von KI-Systemen in die Pflicht. Die Unterscheidung ist vor allem deshalb wichtig, weil abhängig von der Rolle in Bezug auf das KI-System unterschiedliche Pflichten – sowohl dem Umfang als auch dem Inhalt nach – bestehen. Die verschiedenen Adressaten werden unter dem Sammelbegriff „Akteur" allesamt adressiert.

Beispiel: Während die Anbieter von Hochrisiko-KI-Systemen die Pflichten nach Artt. 8–22 AI Act treffen, bestehen für den Betreiber die Pflichten nach Art. 26 AI Act.

3.1 Verpflichtete des AI Act

Begriff des AI Act	Definition des AI Act – der Ausdruck bezeichnet	(Räumlicher) Anwendungsbereich im Sinne des Art. 2 Abs. 1 AI Act	Wesentliche Regelungen (keine abschließende Aufzählung)
„Akteur" **(Art. 3 Nr. 8 AI Act)**	*„einen Anbieter, Produkthersteller, Betreiber, Bevollmächtigten, Einführer oder Händler"*	Sammelbegriff	
„Produkthersteller"	*Keine Definition in Art. 3 AI Act*	*„Produkthersteller, die KI-Systeme zusammen mit ihrem Produkt unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringen oder in Betrieb nehmen"* *(Art. 2 Abs. 1 lit. e AI Act)*	

„Einführer“ **(Art. 3 Nr. 6 AI Act)**	*„eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die ein KI-System, das den Namen oder die Handelsmarke einer in einem Drittland niedergelassenen natürlichen oder juristischen Person trägt, in Verkehr bringt“*	*„Einführer und Händler von KI-Systemen“* *(Art. 2 Abs. 1 lit. d AI Act)*	Art. 23 AI Act
„Händler“ **(Art. 3 Nr. 7 AI Act)**	*„eine natürliche oder juristische Person in der Lieferkette, die ein KI-System auf dem Unionsmarkt bereitstellt, mit Ausnahme des Anbieters oder des Einführers;“*	*„Einführer und Händler von KI-Systemen“* *(Art. 2 Abs. 1 lit. d AI Act)*	Art. 24 AI Act
„Anbieter“ **(Art. 3 Nr. 3 AI Act)**	*„eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich“*	*„Anbieter, die **in der Union KI-Systeme in Verkehr bringen oder in Betrieb nehmen** oder **KI-Modelle mit allgemeinem Verwendungszweck in Verkehr bringen**, **unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen sind**“* *(Art. 2 Abs. 1 lit. a AI Act)* *„Anbieter […] **von KI-Systemen**, die **ihren Sitz in einem Drittland haben oder sich in einem Drittland befinden, wenn die vom KI-System hervorgebrachte Ausgabe in der Union verwendet wird**“* *(Art. 2 Abs. 1 lit. c AI Act)*	Artt. 16–21 AI Act Art. 50 Abs. 1, Abs. 2 AI Act

„nachgelagerter Anbieter“ **(Art. 3 Nr. 68 AI Act)**	*„einen Anbieter eines KI-Systems, einschließlich eines KI-Systems mit allgemeinem Verwendungszweck, das ein KI-Modell integriert, unabhängig davon, ob das KI-Modell von ihm selbst bereitgestellt und vertikal integriert wird oder von einer anderen Einrichtung auf der Grundlage vertraglicher Beziehungen bereitgestellt wird“*		
„Betreiber“ **(Art. 3 Nr. 4 AI Act)**	*„eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet“*	*„Betreiber von KI-Systemen, die ihren Sitz in der Union haben oder sich in der Union befinden“* *(Art. 2 Abs. 1 lit. b AI Act)* *„[…] Betreiber von KI-Systemen, die ihren Sitz in einem Drittland haben oder sich in einem Drittland befinden, wenn die vom KI-System hervorgebrachte Ausgabe in der Union verwendet wird“* *(Art. 2 Abs. 1 lit. c AI Act)*	Artt. 26, 27 AI Act Art. 50 Abs. 3, Abs. 4 AI Act
Rollenwechsel		*„In den folgenden Fällen **gelten Händler, Einführer, Betreiber oder sonstige Dritte als Anbieter** eines Hochrisiko-KI-Systems für die Zwecke dieser Verordnung und unterliegen den Anbieterpflichten gemäß Artikel 16: […]“*	Art. 25 AI Act

„Bevollmächtigter“ **(Art. 3 Nr. 5 AI Act)**	*„eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die vom Anbieter eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck schriftlich dazu bevollmächtigt wurde und sich damit einverstanden erklärt hat, in seinem Namen die in dieser Verordnung festgelegten Pflichten zu erfüllen bzw. Verfahren durchzuführen“*	*„Bevollmächtigte von Anbietern, die nicht in der Union niedergelassen sind“* *(Art. 2 Abs. 1 lit. f AI Act)*	Art. 22 AI Act

3.2 Risiko des Rollenwechsels (Art. 25 AI Act)

Art. 25 DS-GVO regelt den sog. Rollenwechsel. Vereinfacht gesagt, steckt hinter der Überlegung folgender Grundsatz: Wer sich wie ein Anbieter verhält, muss auch die Pflichten eines Anbieters erfüllen. Damit wird verhindert, dass die Pflichtenstellung als Anbieter unterlaufen wird.

Vergleich zur DS-GVO: Die DS-GVO kennt eine vergleichbare Regelung für den Auftragsverarbeiter: Exzess des Auftragsverarbeiters nach Art. 28 Abs. 10 DS-GVO. Der Auftragsverarbeiter wird dann behandelt wie ein Verantwortlicher. Nur bei Hochrisiko-KI-Systemen gilt Art. 25 AI Act. Bei Hochrisiko-KI-Systemen sind die Pflichten von Anbietern signifikant umfangreicher als die der anderen Akteure.

Nach Art. 25 Abs. 1 AI Act gelten Händler, Einführer, Betreiber oder sonstige Dritte als Anbieter eines Hochrisiko-KI-Systems und unterliegenden Anbieterpflichten gemäß Art. 16 AI Act:

- *„wenn sie ein bereits in Verkehr gebrachtes oder in Betrieb genommenes Hochrisiko-KI-System mit ihrem Namen oder ihrer Handelsmarke versehen, unbeschadet vertraglicher Vereinbarungen, die eine andere Aufteilung der Pflichten vorsehen“*
- Mit anderen Worten: Wer das Hochrisiko-KI-System zu seinem eigenen macht, muss auch die entsprechenden Pflichten erfüllen.
- *„wenn sie eine wesentliche Veränderung eines Hochrisiko-KI-Systems, das bereits in Verkehr gebracht oder in Betrieb genommen wurde, so vornehmen, dass es weiterhin ein Hochrisiko-KI-System gemäß Artikel 6 bleibt“*

- Mit anderen Worten: Wer in Hochrisiko-KI-Systeme eingreift und damit Abweichungen von den Vorgaben des Anbieters erzeugt, muss sich auch im Übrigen verhalten wie ein Anbieter.

- *„wenn sie die Zweckbestimmung eines KI-Systems, einschließlich eines KI-Systems mit allgemeinem Verwendungszweck, das nicht als hochriskant eingestuft wurde und bereits in Verkehr gebracht oder in Betrieb genommen wurde, so verändern, dass das betreffende KI-System zu einem Hochrisiko-KI-System im Sinne von Artikel 6 wird".*

  Mit anderen Worten: Hier kommt die Zweckbestimmung *ebenfalls zum Tragen. Wer abweichend von der Zweckbestimmung des Anbieters ein einfaches KI-System in einem Hochrisiko-Umfeld einsetzt, muss auch die Anbieterpflichten für dieses Hochrisiko-KI-System erfüllen.*

Hinweis für die Praxis

Es muss im Unternehmen sichergestellt werden, dass es nicht versehentlich oder durch Eigenmächtigkeiten von Mitarbeitern oder Dienstleistern zu einem solchen Rollenwechsel kommt.

4. Risikobasierter Regelungsansatz – das Risiko bestimmt über die Anwendung der Regelungen!

Der AI Act verfolgt einen risikobasierten Ansatz dergestalt, dass er die KI-Systeme in verschiedene Risikokategorien einteilt und entsprechend diesen Risikokategorien bestimmte Pflichten vorsieht.

Innerhalb der jeweiligen Risikokategorie bestehen dann für die Akteure unterschiedliche Pflichten (siehe Ziffer 3.1).

Für KI-Modelle bestehen keine unterschiedlichen Risikokategorien. Der AI Act erfasst in Kapitel V alle KI-Modelle, wobei besondere Anforderungen nur für solche mit systemischem Risiko bestehen.

4.1 Risikokategorisierung des AI Act

Die nachfolgende Übersicht bildet im Ampel-Farbschema die Risikokategorisierung des AI Act ab.

Die darin angedeutete Pyramide bringt in Anlehnung an „A risk-based approach", Europäische Kommission, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai, Link vom 22.09.2024, die vermutete Relevanz der Regelungen in der Praxis zum Ausdruck.



4.2 KI-spezifische Risiken im Überblick

Beim Einsatz von Künstlicher Intelligenz werden vor allem drei spezifische Risiken diskutiert. Diese sind im AI Act nicht definiert.

Sie wirken sich vor allem auch bei einer datenschutzrechtlichen Bewertung im Rahmen der Grundsätze der Fairness, Transparenz und Richtigkeit des Art. 5 Abs. 1 DS-GVO aus und sind damit natürlich auch bei der Zulässigkeitsprüfung und Bewertungen nach Art. 35 DS-GVO (Datenschutz-Folgenabschätzung) zu bewerten.

- **sog. Verzerrungseffekt (BIAS)**

  Der Verzerrungseffekt ist aus der Psychologie bereits bekannt. Dort wird das Phänomen beschrieben, dass Einstellungen oder Stereotype die Wahrnehmung der Umwelt, das Treffen von Entscheidungen sowie die Vornahme von Handlungen – positiv oder negativ – beeinflussen. Ein Fehler im Rahmen der Datenerhebung und/oder -verarbeitung in der Statistik wird hierunter verstanden *(Quelle: https://bias-and-fairness-in-ai-systems.de/grundlagen/ (Link mit Stand: 17.10.2024)).*

  Wenn KI-Systeme, die voreingenommen Ergebnisse liefern, die menschlichen Verzerrungen innerhalb einer Gesellschaft widerspiegeln und aufrechterhalten, einschließlich historischer und aktueller sozialer Ungleichheit, kann von KI-Verzerrungen gesprochen werden. Dies kann sich aus den anfänglichen

Trainingsdaten, dem Algorithmus oder den Vorhersagen, die der Algorithmus generiert, ergeben (Quelle: *https://www.ibm.com/de-de/think/topics/shedding-light-on-ai-bias-with-real-world-examples (Link mit Stand: 17.10.2024) sowie mit Beispielen aus der Praxis*).

- **sog. Halluzination (auch bezeichnet als Konfabulation)**

  Ein überzeugend formuliertes Resultat, das nicht durch Trainingsdaten gerechtfertigt zu sein scheint und objektiv falsch sein kann, wird im Kontext von KI als Halluzination bezeichnet (*Quelle: https://de.wikipedia.org/wiki/Halluzination_(K%C3%BCnstliche_Intelligenz) (Link mit Stand: 17.10.2024)*).

- **Blackbox-Problematik**

  Ein System, dessen innere Abläufe nicht nachvollziehbar oder kaum erklärbar sind, wird als Blackbox bezeichnet. Das Blackbox-Phänomen ergibt sich im Kontext von KI jedoch weniger daraus, dass die Funktionsweise geheim gehalten wird, sondern daraus, dass es für einen Menschen (nicht mehr) verständlich erklärt werden kann.

  Mit Blick darauf, dass anderseits die Autonomie gerade ein Merkmal der Definition eines KI-Systems ist, stellt dieses Risiko möglicherweise einen Zielkonflikt dar. Das Gegenteil ist die sogenannte Explainable AI, also erklärbare KI.

4.3 KI-Kompetenz (Art. 4 AI Act)

Eine Besonderheit des AI Act besteht in der gesetzlichen Pflicht zur „KI-Kompetenz".

Diese Pflicht besteht **unabhängig von der Risikokategorisierung** und gilt bereits **seit dem 02.02.2025**. Art. 4 AI Act formuliert die Pflicht wie folgt:

> *„Die **Anbieter** und **Betreiber** von **KI-Systemen** ergreifen Maßnahmen, um nach besten Kräften sicherzustellen, dass **ihr Personal** und **andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind**, über ein **ausreichendes Maß an KI-Kompetenz verfügen**, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind."*

Folgende **Eckpunkte** ergeben sich aus Art. 4 AI Act:

- Die Pflicht betrifft die Nutzung von KI-Systemen, und zwar unabhängig von der Risikokategorisierung.
- In die Pflicht genommen wird sowohl der Anbieter als auch der Betreiber. Mit der Bezugnahme auf die Betreiber wird deutlich, dass praktisch jedes Unternehmen, bei dem KI zum Einsatz kommt, für die KI-Kompetenz sorgen muss.
- Die Pflicht bezieht sich nicht nur auf das eigene Personal, sondern auch auf Dienstleister. Dienstleister im Sinne dieser Regelung sind nicht nur Auftragsverarbeiter im Sinne der DS-GVO.
- Erfasst sind die Dienstleister nicht nur dann, wenn sie die KI-Systeme für den Auftraggeber nutzen, sondern bereits dann, wenn sie ihm diese zur Nutzung bereitstellen.
- Es besteht die Pflicht, die Kompetenz sicherzustellen, aber nicht „um jeden Preis", sondern nur nach besten Kräften. Das ist gleichwohl eine hohe Anforderung.
- Formal besteht **keine Ausnahme von der Pflicht**. Die Pflicht als solche ist auch nicht risikobasiert. Das bedeutet, dass auch Personal, das nur ein KI-System zur Rechtschreib- und Grammatikkorrektur einsetzt, die KI-Kompetenz vermittelt werden muss. Unterschiede ergeben sich allenfalls in der Detaillierung der Kompetenzvermittlung.

Es muss ein **ausreichendes Maß an KI-Kompetenz** sichergestellt werden. Das Ziel ist die KI-Kompetenz, wie sie in Art. 3 Nr. 56 AI Act definiert ist:

> *„‚KI-Kompetenz' [ist] die Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden."*

Nach Art. 4 AI Act sind bei der Beurteilung des Maßes die technischen Kenntnisse, die Erfahrung, die Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme verwendet werden sollen, zu berücksichtigen. Das bedeutet, dass in einem Unternehmen durchaus unterschiedliche Inhalte vermittelt werden müssen.

Für das Verständnis sind auch die Konkretisierungen in Erwägungsgrund 20 AI Act wichtig:

- *„Um den **größtmöglichen Nutzen aus KI-Systemen zu ziehen und gleichzeitig die Grundrechte, Gesundheit und Sicherheit zu wahren und eine demokratische Kontrolle** zu ermöglichen, sollte die KI-Kompetenz **Anbieter, Betreiber und betroffene Personen mit den notwendigen Konzepten ausstatten, um fundierte Entscheidungen über KI-Systeme zu treffen**."*

- *„Diese Konzepte können **in Bezug auf den jeweiligen Kontext unterschiedlich sein und das Verstehen der korrekten Anwendung technischer Elemente in der Entwicklungsphase des KI-Systems, der bei seiner Verwendung anzuwendenden Maßnahmen und der geeigneten Auslegung der Ausgaben des KI-Systems umfassen sowie im Falle betroffener Personen das nötige Wissen, um zu verstehen, wie sich mithilfe von KI getroffene Entscheidungen auf sie auswirken werden**."*

- *„Im Zusammenhang mit der Anwendung dieser Verordnung sollte die KI-Kompetenz **allen einschlägigen Akteuren der KI-Wertschöpfungskette die Kenntnisse vermitteln, die erforderlich sind, um die angemessene Einhaltung und die ordnungsgemäße Durchsetzung der Verordnung sicherzustellen.**"*

- *„**Darüber hinaus könnten die umfassende Umsetzung von KI-Kompetenzmaßnahmen und die Einführung geeigneter Folgemaßnahmen dazu beitragen, die Arbeitsbedingungen zu verbessern und letztlich die Konsolidierung und den Innovationspfad vertrauenswürdiger KI in der Union unterstützen**."*

Zum Anwendungsbeginn dieser Regelung ist noch nicht klar, wie diese Kompetenzvermittlung inhaltlich auszugestalten und die Vermittlung praktisch umzusetzen ist.

Jedenfalls müssen technische (Technologie und Funktionsweise) und rechtliche Kenntnisse (AI Act, aber auch Datenschutzrecht) sowie die Chancen und Risiken (Nutzen im Unternehmen, aber auch BIAS, Halluzination und Blackbox) vermittelt werden. Diese 3 Bausteine müssen dann anhand der Besonderheiten des konkreten KI-Einsatzes ausgeprägt werden.

Die Detaillierung und der Umfang der Kompetenzvermittlung hängen maßgeblich von dem genutzten KI-System und dessen Einsatzgebiet ab. Es bieten sich dementsprechend unterschiedliche Schulungen an.

Tipp für die Praxis

Die Kompetenzvermittlung kann durch KI-Kompetenzschulungen vermittelt werden.

Achtung!

Ein Verstoß gegen Art. 4 AI Act ist nach dem AI Act nicht bußgeldsanktioniert. Aber wird das grundlegende Einfallstor zur Begründung von Schadensersatzansprüchen sein, wenn die Handelnden nicht über das erforderliche Maß an KI-Kompetenz verfügt haben.

5. Verbotene Praktiken im KI-Bereich (Art. 5 AI Act)

In seinem Art. 5 verbietet der AI Act bestimmte Praktiken. Das ist ein absolutes Verbot; auf eine Risikobewertung kommt es nicht an.

Diese Regelung gilt seit dem 02.02.2025 und ist mit dem mit Abstand höchsten Bußgeldrahmen (bis 37 Mio. Euro oder – im Fall von Unternehmen – von bis zu 7 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres) des AI Act belegt. Der Gesetzgeber macht damit deutlich, wie bedeutend das Verbot ist. Dies ist auch ein Handlungsauftrag an die Aufsichtsbehörden.

Vereinfacht gesagt: Art. 5 AI Act regelt die 8 Todsünden der Nutzung von KI-Systemen.

Verboten ist durch Art. 5 AI Act Folgendes – die nachfolgenden Hervorhebungen dienen nur dem Schnelllesen, entscheidend sind jedoch die Details der Formulierungen:

> *„(1) Folgende Praktiken im KI-Bereich sind verboten:*
>
> *a) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das* ***Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person oder absichtlich manipulative oder täuschende Techniken*** *mit dem Ziel oder der Wirkung einsetzt, das Verhalten einer Person oder einer Gruppe von Personen wesentlich zu verändern, indem ihre Fähigkeit, eine fundierte Entscheidung zu treffen, deutlich beeinträchtigt wird,* ***wodurch sie veranlasst wird, eine Entscheidung zu treffen, die sie andernfalls nicht getroffen hätte, und zwar in einer Weise, die dieser Person, einer anderen Person oder einer Gruppe von Personen erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird****.*

b) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das eine ***Vulnerabilität oder Schutzbedürftigkeit einer natürlichen Person oder einer bestimmten Gruppe von Personen aufgrund ihres Alters, einer Behinderung oder einer bestimmten sozialen oder wirtschaftlichen Situation*** *mit dem Ziel oder der Wirkung ausnutzt,* ***das Verhalten*** *dieser Person oder einer dieser Gruppe angehörenden Person* ***in einer Weise wesentlich zu verändern, die dieser Person oder einer anderen Person erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird****;*

c) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen zur ***Bewertung oder Einstufung von natürlichen Personen oder Gruppen von Personen über einen bestimmten Zeitraum auf der Grundlage ihres sozialen Verhaltens oder bekannter, abgeleiteter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale****, wobei die soziale Bewertung zu einem oder beiden der folgenden Ergebnisse führt:*

- i) Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder Gruppen von Personen in sozialen Zusammenhängen, die in keinem Zusammenhang zu den Umständen stehen, unter denen die Daten ursprünglich erzeugt oder erhoben wurden;
- ii) Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder Gruppen von Personen in einer Weise, die im Hinblick auf ihr soziales Verhalten oder dessen Tragweite ungerechtfertigt oder unverhältnismäßig ist;

d) das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung eines KI-Systems ***zur Durchführung von Risikobewertungen in Bezug auf natürliche Personen, um das Risiko, dass eine natürliche Person eine Straftat begeht,*** *ausschließlich auf der Grundlage des Profiling einer natürlichen Person oder der Bewertung ihrer persönlichen Merkmale und Eigenschaften zu bewerten oder vorherzusagen; dieses Verbot gilt nicht für KI-Systeme, die dazu verwendet werden, die durch Menschen durchgeführte Bewertung der Beteiligung einer Person an einer kriminellen Aktivität, die sich bereits auf objektive und überprüfbare Tatsachen stützt, die in unmittelbarem Zusammenhang mit einer kriminellen Aktivität stehen, zu unterstützen;*

e) das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen, die ***Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen*** *erstellen oder erweitern;*

f) das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen ***zur Ableitung von Emotionen einer natürlichen Person am Arbeitsplatz und in Bildungseinrichtungen****, es sei denn, die Verwendung des KI-Systems soll aus medizinischen Gründen oder Sicherheitsgründen eingeführt oder auf den Markt gebracht werden;*

g) das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von Systemen zur ***biometrischen Kategorisierung, mit denen natürliche Personen individuell auf der Grundlage ihrer biometrischen Daten kategorisiert werden, um ihre Rasse, ihre politischen Einstellungen, ihre Gewerkschaftszugehörigkeit, ihre religiösen oder weltanschaulichen*** **Überzeugungen, ihr Sexualleben oder ihre sexuelle Ausrichtung zu erschließen oder abzuleiten***; dieses Verbot gilt nicht für die Kennzeichnung oder Filterung rechtmäßig erworbener biometrischer Datensätze, wie z. B. Bilder auf der Grundlage biometrischer Daten oder die Kategorisierung biometrischer Daten im Bereich der Strafverfolgung;*

h) die Verwendung ***biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken****, außer wenn und insoweit dies im Hinblick auf eines der folgenden Ziele unbedingt erforderlich ist:*

- i) gezielte Suche nach bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung sowie die Suche nach vermissten Personen;

- ii) Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr eines Terroranschlags;

- iii) Aufspüren oder Identifizieren einer Person, die der Begehung einer Straftat verdächtigt wird, zum Zwecke der Durchführung von strafrechtlichen Ermittlungen oder von Strafverfahren oder der Vollstreckung einer Strafe für die in Anhang II aufgeführten Straftaten, die in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens vier Jahren bedroht ist. Dieses Verbot gilt unabhängig von der Regelung in Art. 9 DS-GVO (Verarbeitung besonderer Kategorien personenbezogener Daten).

Unterabsatz 1 Buchstabe h gilt unbeschadet des Artikels 9 der Verordnung (EU) 2016/679 für die Verarbeitung biometrischer Daten zu anderen Zwecken als der Strafverfolgung.“

Weitergehende Konkretisierungen und Ausnahmen sind in den Abs. 2 bis Abs. 7 des Art. 5 AI Act enthalten.

In Art. 5 Abs. 8 AI Act wird klargestellt, dass durch Art. 5 AI Act die Regelungen in anderen Rechtsvorschriften der Union, die Verbote für solche KI-Praktiken vorsehen, nicht berührt, also nicht eingeschränkt oder verändert werden.

Die Ausnahme des Art. 2 Abs. 12 AI Act für Open Source KI-Systeme gilt nicht für die Praktiken des Art. 5 AI Act.

Hinweis für die Praxis

Im Unternehmen und auch bei Dienstleistern muss sichergestellt sein, dass nicht gegen Art. 5 AI Act verstoßen wird. Dieses Verbot ist daher ein grundlegender Bestandteil jeder unternehmensinternen Vorgabe zum Einsatz von KI.

6. Hochrisiko-KI (Art. 6 AI Act)

Die Hochrisiko-KI ist der Regelungsschwerpunkt – jedenfalls dem inhaltlichen Umfang des AI Act nach. Der Schwerpunkt der materiellen Anforderungen ist in Kapitel III des AI Act – das sind die Artt. 6–49 AI Act – geregelt.

Hinweis

Die Kernaussage ist, dass der Einsatz von Hochrisiko-KI-Systemen zulässig ist, aber bestimmte Anforderungen zur Beherrschung des von ihnen ausgehenden Risikos erfüllt werden müssen.

Das Kapitel III des AI Act ist wie folgt strukturiert:

- Festlegung der Hochrisiko-KI-Systeme (Art. 6 AI Act (zzgl. Art. 7 AI Act))
- Generelle Anforderungen an Hochrisiko-KI-Systeme (Artt. 8–15 AI Act)
- Pflichten der Anbieter und Betreiber von Hochrisiko-KI-Systemen und anderer Beteiligter (Artt. 16 ff. AI Act) und insbesondere
  - Pflichten der Anbieter (Artt. 16–22 AI Act)
  - Pflichten der Betreiber (Artt. 26, 27 AI Act)

Eine detaillierte Darstellung aller Bestimmungen ist im Rahmen des Überblicks in diesem Buch nicht möglich. Es werden Schwerpunkte gesetzt.

6.1 Festlegung der Hochrisiko-KI-Systeme (Art. 6 AI Act)

Ein KI-System wird zum Hochrisiko KI-System, wenn die Voraussetzungen des Art. 6 Abs. 1 AI Act oder die Voraussetzungen des Art. 6 Abs. 2 AI Act gegeben sind.

Diese Unterscheidung entscheidet auch über den Beginn der Pflichten:

- Für Hochrisiko-KI-Systeme nach Art. 6 **Abs. 2** AI Act gelten die Pflichten ab dem 02.08.20**26**.
- Für Hochrisiko-KI-Systeme nach Art. 6 **Abs. 1** AI Act gelten die Pflichten ab dem 02.08.20**27**.

6.1.1 Hochrisiko-KI-System nach Art. 6 Abs. 1 AI Act

Nach Art. 6 Abs. 1 AI Act ist ein KI-System ein Hochrisiko-KI-System, wenn zwei Voraussetzungen gleichzeitig erfüllt sind:

> *„a) das KI-System soll als **Sicherheitsbauteil eines unter die in Anhang I** aufgeführten Harmonisierungsrechtsvorschriften der Union fallenden Produkts verwendet werden oder das **KI-System ist selbst ein solches Produkt**;*
>
> *b) das Produkt, dessen Sicherheitsbauteil gemäß Buchstabe a das KI-System ist, oder das KI-System selbst als Produkt muss einer **Konformitätsbewertung durch Dritte im Hinblick auf das Inverkehrbringen oder die Inbetriebnahme dieses Produkts gemäß den in Anhang I** aufgeführten Harmonisierungsrechtsvorschriften der Union unterzogen werden."*

Für Hochrisiko-KI-Systeme nach Art. 6 **Abs. 1** AI Act gelten die Pflichten ab dem 02.08.20**27**.

6.1.2 Hochrisiko-KI-System nach Art. 6 Abs. 2 AI Act

Die in Anhang III genannten KI-Systeme gelten nach Art. 6 Abs. 2 ebenfalls als hochriskant. Für Hochrisiko-KI-Systeme nach Art. 6 **Abs. 2** AI Act gelten die Pflichten ab dem 02.08.20**26**.

Art. 6 Abs. 3 AI Act regelt **Ausnahmen von der Einstufung als Hochrisiko-KI-System im Sinne des Art. 6 Abs. 2 AI Act. Voraussetzung ist hierfür, dass nach der Bewertungsmaßgabe des Art. 6 Abs. 3 AI Act** kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen gegeben ist. Nach Art. 6 Abs. 3 UAbs. 3 AI Act greift die

Ausnahme nach Art. 6 Abs. 2 nicht **(Rückausnahme)**, wenn das KI-System ein Profiling natürlicher Personen vornimmt. Für den Begriff Profiling gilt aufgrund der Verweisung des Art. 3 Nr. 52 AI Act die Definition in Art. 4 Nr. 4 DS-GVO.

Für Art. 6 Abs. 2 AI Act sieht Art. 6 Abs. 4 AI Act eine **Dokumentationspflicht der Ausnahme vor:** Ein Anbieter, der der Auffassung ist, dass ein in Anhang III aufgeführtes KI-System nicht hochriskant ist, dokumentiert seine Bewertung, bevor (!) dieses System in Verkehr gebracht oder in Betrieb genommen wird (Art. 6 Abs. 4 S. 1 AI Act). Auf Verlangen der zuständigen nationalen Behörden legt der Anbieter die Dokumentation der Bewertung vor (Art. 6 Abs. 4 S. 3 AI Act). Die Registrierungspflicht gemäß Artikel 49 Abs. 2 AI Act besteht ebenfalls dennoch (Art. 6 Abs. 4 S. 2 AI Act).

6.1.3 Leitlinien und Liste praktischer Beispiele für Anwendungsfälle (Art. 6 Abs. 5 AI Act)

Die EU-Kommission stellt nach Konsultation des Europäischen Gremiums für Künstliche Intelligenz spätestens bis zum 02.02.2026 Leitlinien zur praktischen Umsetzung des Art. 6 AI Act und eine umfassende Liste praktischer Beispiele für Anwendungsfälle für KI-Systeme, die hochriskant oder nicht hochriskant sind, bereit.

Tipp für die Praxis: Behalten Sie diese Veröffentlichung im Auge! Sie soll sechs Monate vor dem Anwendungsbeginn der Regelungen für Hochrisiko-KI-Systeme veröffentlicht sein. Aber: Bereits jetzt sind eine Einordnung und Vorbereitung auf die Pflichten möglich.

6.2 Generelle Anforderungen an Hochrisiko-KI-Systeme (Artt. 8–15 AI Act)

Artt. 8–15 AI Act legen Anforderungen fest, die generell für Hochrisiko-KI-Systeme gelten. Diese Pflichten werden in Art. 16 AI Act für den Anbieter des Hochrisiko-KI-Systems wieder adressiert.

Als **grundlegende Maßgabe** regelt **Art. 8 AI Act** die Pflicht zur **Einhaltung der Anforderungen** der Artt. 9–15 AI Act.

Nach Art. 8 Abs. 1 AI Act müssen Hochrisiko-KI-Systeme die in Artt. 8–15 AI Act festgelegten Anforderungen erfüllen, wobei ihrer Zweckbestimmung sowie dem allgemein anerkannten Stand der Technik in Bezug auf KI und KI-bezogene Technologien Rechnung zu tragen ist. Bei der Gewährleistung der Einhaltung dieser Anforderungen ist dem in Art. 9 AI Act genannten Risikomanagementsystem Rechnung zu tragen.

Zentrale Bedeutung für die Pflichten nach dem AI Act hat die Zweckbestimmung des KI-Systems. Sie ist wesentlich für die Festlegung der Pflichten. Sie ist aber auch für den sog. Rollenwechsel nach Art. 25 DS-GVO relevant.

Für den Begriff **Zweckbestimmung** enthält Art. 3 Nr. 12 AI Act folgende **Definition:** „die Verwendung, für die ein KI-System laut Anbieter bestimmt ist, einschließlich der besonderen Umstände und Bedingungen für die Verwendung, entsprechend den vom Anbieter bereitgestellten Informationen in den Betriebsanleitungen, im Werbe- oder Verkaufsmaterial und in diesbezüglichen Erklärungen sowie in der technischen Dokumentation".

Art. 8 Abs. 2 AI Act regelt das **Verhältnis des AI Act zu anderen Harmonisierungsrechtsvorschriften der Union im Sinne des Anhangs I des AI Act**. Vereinfacht gesagt, sind die Anbieter im Sinne des AI Act auch dafür verantwortlich, dass ihr Produkt alle geltenden Anforderungen der geltenden Harmonisierungsrechtsvorschriften der Union vollständig erfüllt.

Die **Pflichten der Artt. 9–15 AI Act** werden nachfolgend benannt und bestimmte Pflichten **im Überblick** besprochen. Diese Pflichten gelten **nur für Hochrisiko-KI-Systeme!**

➤ **Risikomanagementsystem (Art. 9 AI Act)**

Für Hochrisiko-KI-Systeme ist ein **Risikomanagementsystem** einzurichten, anzuwenden, zu dokumentieren und aufrechtzuerhalten (Art. 9 Abs. 1 AI Act). Die Anforderungen werden durch die Abs. 2–10 des Art. 9 AI Act konkretisiert. Das Risikomanagementsystem versteht sich als ein kontinuierlicher iterativer Prozess während des gesamten Lebenszyklus.

➤ **Daten und Daten-Governance (Art. 10 AI Act)**

Hochrisiko-KI-Systeme, in denen Techniken eingesetzt werden, bei denen KI-Modelle mit Daten trainiert werden, müssen mit Trainings-, Validierungs- und Testdatensätzen entwickelt werden, die den in den Art. 9 Abs. 1 bis Abs. 5 AI Act genannten Qualitätskriterien entsprechen.

Art. 10 Abs. 5 AI Act enthält eine Regelung **für besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DS-GVO. Hierbei handelt es sich um eine Regelung zur Zulässigkeit der Verarbeitung personenbezogener Daten, die die Wirkung des Art. 9 DS-GVO einschränkt.**

➤ **Technische Dokumentation (Art. 11 AI Act)**

Die Pflicht zur **Technischen Dokumentation** sowie zur inhaltlichen Ausgestaltung der Technischen Dokumentation regelt **Art. 11 AI Act**. Die technische Dokumentation muss erstellt sein, bevor (!) dieses Hochrisiko-KI-System in Verkehr gebracht oder in Betrieb genommen wird (Art. 11 Abs. 1 UAbs. 1 AI Act).

Erleichterungen in Bezug auf die Technische Dokumentation für kleine und mittlere Unternehmen (**KMU) und Start-ups** sieht Art. 11 Abs. 1 UAbs. 2 Satz 3 AI Act vor.

➤ **Aufzeichnungspflichten (Art. 12 AI Act)**

Nach **Art. 12 AI Act** muss die automatische Aufzeichnung von Ereignissen während des gesamten Lebenszyklus des Systems möglich sein.

➤ **Transparenz und Bereitstellung von Informationen für die Betreiber (Art. 13 AI Act)**

Art. 13 AI Act ist eine **zentrale Regelung des AI Acts für Betreiber.** Denn die Informationspflicht des Anbieters nach Art. 13 AI Act ist zentral für die Erfüllung der Pflichten des Betreibers sowohl nach dem AI Act (Artt. 26, 27 AI Act) als auch nach der DS-GVO. Denn hierdurch erhält er wesentliche Informationen für diese Bewertungen. Insbesondere ergibt sich hieraus auch die Zweckbestimmung des KI-Systems.

Aber: Die Transparenzpflicht gilt nur für Hochrisiko-KI-Systeme und nicht für alle KI-Systeme und auch nicht für KI-Modelle.

Die Konzeption und Entwicklung von Hochrisiko-KI-Systemen muss so erfolgen, dass ihr Betrieb hinreichend transparent ist, damit die Betreiber die Aussagen eines Systems angemessen interpretieren und verwenden können.

Nach Art. 13 Abs. 2 AI Act muss eine Betriebsanleitung bereitgestellt werden. Die Betriebsanleitungen müssen präzise, vollständige, korrekte und eindeutige Informationen in einer für die Betreiber relevanten, barrierefrei zugänglichen und verständlichen Form enthalten. Art. 13 Abs. 3 AI Act legt die Mindestinhalte fest.

➤ **Menschliche Aufsicht (Art. 14 AI Act)**

Der menschlichen Aufsicht kommt insbesondere mit Blick auf die KI-spezifischen Risiken eine besondere Bedeutung zu. Hochrisiko-KI-Systeme müssen der **menschlichen Aufsicht** unterstehen können. Art. 14 AI Act schafft hierfür die Voraussetzungen. Die Regelung korrespondiert mit der Pflicht der Betreiber zur Einrichtung einer menschlichen Aufsicht nach Art. 26 Abs. 2 AI Act.

Den Zweck der menschlichen Aufsicht legt Art. 14 Abs. 2 AI Act fest, der damit auch für Art. 26 Abs. 1 AI Act relevant wird. Die menschliche Aufsicht dient der Verhinderung oder Minimierung der Risiken für Gesundheit, Sicherheit oder Grundrechte, die entstehen können, wenn ein Hochrisiko-KI-System im Einklang mit seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird, insbesondere wenn solche Risiken trotz der Einhaltung anderer Anforderungen dieses Abschnitts fortbestehen.

Art. 14 Abs. 1 AI Act gibt vor, dass Hochrisiko-KI-Systeme so konzipiert und entwickelt werden müssen, dass sie während der Dauer ihrer Verwendung – auch mit geeigneten Instrumenten einer Mensch-Maschine-Schnittstelle – von natürlichen Personen wirksam beaufsichtigt werden können.

Nach **Art. 14 Abs. 3** müssen die **Aufsichtsmaßnahmen** den Risiken, dem Grad der Autonomie und dem Kontext der Nutzung des Hochrisiko-KI-Systems angemessen sein und werden durch die in Abs. 3 genannten Vorkehrungen gewährleistet.

Art. 14 Abs. 4 AI Act stellt den Zusammenhang zur menschlichen Aufsicht beim Betrieb eines Hochrisiko-KI-Systems nach Art. 26 Abs. 2 AI Act her:

> *„Für die Zwecke der Durchführung der Absätze 1, 2 und 3 wird das Hochrisiko-KI-System dem Betreiber so zur Verfügung gestellt, dass die natürlichen Personen, denen die menschliche Aufsicht übertragen wurde, angemessen und verhältnismäßig in der Lage sind,*
>
> *a) die einschlägigen Fähigkeiten und Grenzen des Hochrisiko-KI-Systems angemessen zu verstehen und seinen Betrieb ordnungsgemäß zu überwachen, einschließlich in Bezug auf das Erkennen und Beheben von Anomalien, Fehlfunktionen und unerwarteter Leistung;*
>
> *b) sich einer möglichen Neigung zu einem automatischen oder übermäßigen Vertrauen in die von einem Hochrisiko-KI-System hervorgebrachte Ausgabe („Automatisierungsbias") bewusst zu bleiben, insbesondere wenn Hochrisiko-KI-Systeme Informationen oder Empfehlungen ausgeben, auf deren Grundlage natürliche Personen Entscheidungen treffen;*
>
> *c) die Ausgabe des Hochrisiko-KI-Systems richtig zu interpretieren, wobei beispielsweise die vorhandenen Interpretationsinstrumente und -methoden zu berücksichtigen sind;*

d) in einer bestimmten Situation zu beschließen, das Hochrisiko-KI-System nicht zu verwenden oder die Ausgabe des Hochrisiko-KI-Systems außer Acht zu lassen, außer Kraft zu setzen oder rückgängig zu machen;

e) in den Betrieb des Hochrisiko-KI-Systems einzugreifen oder den Systembetrieb mit einer „Stopptaste" oder einem ähnlichen Verfahren zu unterbrechen, was dem System ermöglicht, in einem sicheren Zustand zum Stillstand zu kommen."

Art. 14 Abs. 5 AI Act regelt einen Sonderfall für die in Anhang III Nr. 1 Buchstabe a genannten Hochrisiko-KI-Systeme, wonach insbesondere eine menschliche Aufsicht durch zwei natürliche Personen gefordert ist.

➤ **Genauigkeit, Robustheit und Cybersicherheit (Art. 15 AI Act)**

Art. 15 AI Act fordert, dass Hochrisiko-KI-Systeme so konzipiert und entwickelt werden, dass sie ein angemessenes Maß an **Genauigkeit, Robustheit und Cybersicherheit** erreichen und in dieser Hinsicht während ihres gesamten Lebenszyklus beständig funktionieren. Die Anforderungen werden in Art. 15 Abs. 2–5 AI Act konkretisiert.

6.3 Pflichten der Anbieter und Betreiber von Hochrisiko-KI-Systemen und anderer Beteiligter (Artt. 16 ff. AI Act)

Artt. 16–27 AI Act regeln die Pflichten in Bezug auf Hochrisiko-KI-Systeme **für die verschiedenen Akteure unterschiedlich.**

Der umfangreichste Pflichtenkatalog trifft den **Anbieter (Artt. 16 bis 22 AI Act einschließlich der Bezugnahmen auf Artt. 8–15 AI Act)**.

Den **Betreiber** treffen „nur" die Pflichten nach **Artt. 26, 27 AI Act**. Art. 26 AI Act enthält mit seinen zwölf Absätzen gleichwohl umfangreiche Pflichten, die mit den Regelungen der Artt. 15–22 AI Act korrespondieren. Die Pflichten des Betreibers sind daher im Kontext dieser Regelungen zu verstehen. Das zeigt sich insbesondere an der Regelung über die menschliche Aufsicht in Art. 26 Abs. 2, Art. 14 AI Act.

Hinweis für die Praxis

Lesen Sie die Pflichten des Betreibers im Kontext der Regelungen nach Artt. 15 22 AI Act.

Dementsprechend muss ein **KI-Beauftragter**, der zur Erfüllung der Pflicht nach Art. 26 Abs. 2 AI Act eingesetzt wird, zumindest auch Kenntnis von den Regelungen in Artt. 8–15 sowie 16–22 AI Act haben.

6.3.1 Pflichten der Anbieter (Artt. 16–22 AI Act)

Art. 16 AI Act ist die zentrale Regelung für die Pflichten des Anbieters von Hochrisiko-KI-Systemen. Hieran wird auch erkennbar, dass diese primär in die Pflicht genommenen sind. Art. 16 AI Act nimmt die Pflichten nach Artt. 8–15 AI Act und nach Art. 17–22 AI Act in Bezug.

Die Pflichten werden nachfolgend benannt. Für **Anbieter von Hochrisiko-KI-Systemen im Kontext von Finanzinstituten** sind jeweils Sonderregelungen vorgesehen, die insbesondere auf eine Harmonisierung mit den Sonderbestimmungen für die Finanzinstitute ausgerichtet sind.

- **Pflichten der Anbieter von Hochrisiko-KI-Systemen (Art. 16 AI Act)**

  Nach Art. 16 Abs. 1 lit. a AI Act hat der Anbieter die Erfüllung der Pflichten nach Artt. 8–15 AI Act **sicherzustellen. Die Pflicht zur Eigenidentifikation sieht Art. 16 Abs. 1 lit. b AI Act vor.** Die Anbieter müssen sich selbst als Anbieter des Hochrisiko-KI-Systems benennen und kennzeichnen.

  Art. 16 Abs. 1 lit. c, d und e sowie lit. j AI Act nehmen die Pflichten nach Artt. 17, 18, 19 und 20 AI Act in Bezug (siehe nachfolgend). Darüber hinaus sind weitere Pflichten des Anbieters geregelt, insbesondere durch Bezugnahmen auf Artt. 43, 47 und 49 Abs. 1 AI Act.

- **Qualitätsmanagementsystem (Art. 17 AI Act)**

  Anbieter von Hochrisiko-KI-Systemen sind verpflichtet, ein **Qualitätsmanagementsystem** einzurichten, das die Einhaltung des AI Act gewährleistet (Art. 17 Abs. 1 Satz 1 AI Act). Art. 17 Abs. 1 Satz 2 AI Act gibt vor, dass das **Qualitätsmanagementsystem** „systematisch und ordnungsgemäß in Form schriftlicher Regeln, Verfahren und Anweisungen dokumentiert" sein muss und mindestens die in Art. 17 Abs. 1 Satz 1 lit. a bis lit. m AI Act genannten Aspekte umfasst.

  Der Grundsatz der Verhältnismäßigkeit wird durch Art. 17 Abs. 2 AI Act adressiert. Die Umsetzung kann in einem angemessenen Verhältnis zur Größe der Organisation des Anbieters erfolgen. In jedem Fall müssen die Anbieter „den Grad der Strenge und das Schutzniveau einhalten, die erforderlich sind, um die Übereinstimmung ihrer Hochrisiko-KI-Systeme mit dieser Verordnung sicherzustellen". Hieraus ergibt sich, dass unter Wirtschaftlichkeitsaspekten keine Unterschreitung der gesetzlich zwingenden Pflichten möglich ist.

- **Aufbewahrung der Dokumentation (Art. 18 AI Act)**

  Art. 18 AI Act sieht eine zehnjährige Pflicht zur **Aufbewahrung** für die in Art. 18 AI Act genannten Dokumentationen vor.

➤ **Pflicht zur Aufbewahrung automatisch erzeugter Protokolle (Art. 19 AI Act)**

Die **Pflicht zur Aufbewahrung automatisch erzeugter Protokolle** nach **Art. 19 AI Act** knüpft an die Pflicht in Art. 12 Abs. 1 AI Act zur automatischen Erzeugung von Protokollen an.

➤ **Korrekturmaßnahmen und Informationspflicht (Art. 20 AI Act)**

Art. 20 AI Act sieht Pflichten des Anbieters eines Hochrisiko-KI-Systems für die Zeit nach dem Inverkehrbringen oder der Inbetriebnahme vor. Auch hieran wird deutlich, dass der AI Act Produktsicherheitsrecht ist. Die Auslöser der in Art. 20 Abs. 1 und Abs. 2 AI Act genannten Pflichten sind:

- Der Anbieter von Hochrisiko-KI-Systemen sind der Auffassung oder haben Grund zu der Annahme, dass eines ihrer Hochrisiko-KI-Systeme nicht dem AI Act entspricht.
- Der Anbieter des Hochrisiko-KI-Systems ist sich bewusst, dass dieses ein Risiko im Sinne des Art. 79 Abs. 1 AI Act birgt. Art. 79 Abs. 1 AI Act nimmt die Risiken für die Gesundheit oder Sicherheit oder Grundrechte von Personen in Bezug.

➤ **Zusammenarbeit mit den zuständigen Behörden (Art. 21 AI Act)**

Der Anbieter eines Hochrisiko-KI-Systems ist nach Maßgabe des Art. 21 AI Act zur Zusammenarbeit mit den zuständigen Behörden verpflichtet. Er ist insbesondere verpflichtet, der zuständigen Behörde sämtliche Informationen und Dokumentationen zur Verfügung zu stellen, die erforderlich sind, um die Konformität des Hochrisiko-KI-Systems mit den in Artt. 8 bis 15 AI Act festgelegten Anforderungen nachzuweisen. Die Pflicht besteht – insoweit anders als nach Art. 31 DS-GVO – nur bei einer begründeten Anfrage.

➤ **Bevollmächtigte der Anbieter von Hochrisiko-KI-Systemen (Art. 22 AI Act)**

Anbieter von Hochrisiko-KI-Systemen, die nicht in einem EU-Mitgliedstaat niedergelassen sind, haben vor (!) der Bereitstellung ihrer Hochrisiko-KI-Systeme auf dem Markt der EU schriftlich einen in der Union niedergelassenen Bevollmächtigten zu benennen (**Bevollmächtigte der Anbieter von Hochrisiko-KI-Systemen)** (Art. 22 Abs. 1 AI Act). Hier besteht der Zusammenhang zum räumlichen Anwendungsbereich des AI Acts, der nicht auf die EU begrenzt ist.

Pflicht zur Beendigung und zur Anzeige (Art. 22 Abs. 4 AI Act): Der Bevollmächtigte hat den Auftrag zu beenden, wenn er der Auffassung ist oder Grund zu der Annahme hat, dass der Anbieter gegen seine Pflichten des AI

Acts verstößt. In diesem Fall hat er auch unverzüglich die betreffende Marktüberwachungsbehörde und gegebenenfalls die notifizierende Stelle über die Beendigung des Auftrags und deren Gründe zu informieren.

6.3.2 Pflichten der Betreiber (Artt. 26, 27 AI Act)

Art. 26 AI Act regelt die Pflichten der Betreiber von Hochrisiko-KI-Systemen in 12 Absätzen recht umfangreich. Diese Pflichten korrespondieren insbesondere mit den Regelungen in Artt. 8–15 AI Act, weshalb die Vorgaben des Art. 26 AI Act im Kontext dieser Regelungen ausgelegt und angewendet werden müssen.

Die Pflicht zur **Grundrechte-Folgenabschätzung für Hochrisiko-KI-Systeme nach Art. 27 AI Act** trifft den Betreiber zusätzlich.

6.3.2.1 Pflichten der Betreiber von Hochrisiko-KI-Systemen (Art. 26 AI Act)

In seinen zwölf Absätzen enthält **Art. 26 Act** verschiedene Pflichten für die Betreiber von Hochrisiko-KI-Systemen:

- **Risikomanagementsystem (Art. 26 Abs. 1 AI Act)**

  Art. 26 Abs. 1 AI Act regelt die grundlegende Pflicht für Betreiber von Hochrisiko-KI-Systemen. Durch geeignete technische und organisatorische Maßnahmen haben sie sicherzustellen, dass sie die Hochrisiko-KI-Systeme entsprechend den den Systemen beigefügten Betriebsanleitungen und gemäß Art. 26 Abs. 3 und 6 AI Act verwenden.

  Es besteht eine Parallelität zur Pflicht der Anbieter nach Art. 9 AI Act. Art. 26 Abs. 1 AI Act belässt jedoch mehr Spielräume zur Gestaltung des Risikomanagementsystems. Eine gedankliche Orientierung an Art. 9 des AI Act kann in Betracht gezogen werden.

  Eine Begrenzung der Pflicht ergibt sich aus der Bezugnahme auf die Betriebsanleitung. Die zentrale Bedeutung der Betriebsanleitung im Sinne des Art. 13 AI Act und der Zweckbestimmung des Anbieters kommt hier zum Ausdruck.

- **4.1.2 Menschliche Aufsicht (Art. 26 Abs. 2 AI Act)**

  Die Pflicht zur **menschlichen Aufsicht** über den Betrieb des Hochrisiko-KI-Systems ergibt sich aus Art. 26 Abs. 2 AI Act. Die Regelung korrespondiert mit Art. 14 AI Act; auf die Ausführungen dort wird Bezug genommen).

  Beachten Sie den Unterschied zur KI-Kompetenz: Die Kompetenz für die menschliche Aufsicht nach Art. 26 Abs. 2 AI Act ist nicht inhaltsgleich mit der KI-Kompetenz nach Art. 4 AI Act. Denn: Jede Person im Unternehmen, die KI verwendet, muss über die KI-Kompetenz des Art. 4 AI Act verfügen. Aber nicht

jede Person muss über die Befähigung zur menschlichen Aufsicht verfügen. Neben diesem inhaltlichen Unterschied kommt hinzu, dass die menschliche Aufsicht gesetzlich nur für Hochrisiko-KI-Systeme vorgesehen ist, während die KI-Kompetenz für jedes KI-System verpflichtend ist.

- **Beachtung der Zweckbestimmung des Hochrisiko-KI-Systems (Art. 26 Abs. 4 AI Act)**

  Die Betreiber von Hochrisiko-KI-Systemen sorgen dafür, dass die Eingabedaten, also die Daten, mit denen sie das Hochrisiko-KI-System verwenden, der Zweckbestimmung des Hochrisiko-KI-Systems entsprechen und ausreichend repräsentativ sind, sofern die Eingabedaten ihrer Kontrolle unterliegen.

- **Überwachung des Betriebs des Hochrisiko-KI-Systems und Informationspflichten (Art. 26 Abs. 5 AI Act)**

  Die Überwachung hat anhand der Betriebsanleitung zu erfolgen, die der Anbieter des Hochrisiko-KI-Systems bereitzustellen hat (Art. 13 AI Act).

  Art. 26 Abs. 5 AI Act regelt in seinen weiteren Sätzen verschiedene Informationspflichten des Betreibers.

- **Aufbewahrung der automatisch erzeugten Protokolle (Art. 26 Abs. 6 AI Act)**

  Betreiber von Hochrisiko-KI-Systemen bewahren die von ihrem Hochrisiko-KI-System automatisch erzeugten Protokolle auf, soweit diese Protokolle ihrer Kontrolle unterliegen. Diese Pflicht korrespondiert mit Artt. 12, 19 AI Act. Die Mindestspeicherdauer beträgt sechs Monate an, sofern im geltenden Unionsrecht, insbesondere im Unionsrecht über den Schutz personenbezogener Daten, oder im geltenden nationalen Recht nichts anderes bestimmt ist.

- **4.1.5 Unterrichtung der Arbeitnehmer und Arbeitnehmervertreter (Art. 26 Abs. 7 AI Act)**

  Arbeitgeber, die Betreiber eines Hochrisiko-KI-Systems am Arbeitsplatz sind, haben nach Art. 26 Abs. 7 AI Act sowohl die Arbeitnehmervertreter als auch die davon betroffenen Arbeitnehmer zu informieren, dass sie der „Verwendung eines Hochrisiko-KI-Systems unterliegen". Die Information muss vor (!) der Inbetriebnahme oder vor der Verwendung erfolgen.

  Art. 26 AI Act regelt jedoch keine Mitbestimmung oder Zustimmungsvorbehalt. Diese können sich jedoch aus dem Kollektivarbeitsrecht und dem Datenschutzrecht ergeben, sofern diese Regelungen anwendbar sind.

Hinweis

Die Informationspflicht nach Artt. 13, 14 DS-GVO wird dadurch nicht eingeschränkt oder verändert. Sie besteht jedoch nur, wenn personenbezogene Daten verarbeitet werden, was jedoch typischerweise der Fall sein dürfte.

- **Organe, Einrichtungen oder sonstige Stellen der Union als Betreiber (Art. 26 Abs. 8 AI Act)**

  Art. 26 Abs. 8 AI Act regelt besondere Pflichten für Betreiber von Hochrisiko-KI-Systemen, die Organe, Einrichtungen oder sonstige Stellen der Union sind: Sie müssen der Registrierung nach Art. 49 AI Act nachkommen. Stellen diese Betreiber fest, dass das Hochrisiko-KI-System, dessen Verwendung sie planen, nicht in der in Art. 71 AI Act genannten EU-Datenbank registriert wurde, sehen sie von der Verwendung dieses Systems ab und informieren den Anbieter oder den Händler.

- **Datenschutz-Folgenabschätzung nach Datenschutzrecht (Art. 26 Abs. 9, 10 AI Act)**

  Die Betreiber von Hochrisiko-KI-Systemen verwenden die gemäß Art. 13 AI Act durch den Anbieter bereitgestellten Informationen zur Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO oder Art. 27 der Richtlinie (EU) 2016/680. Eine Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung im Sinne des Datenschutzrechts wird durch Art. 26 Abs. 9 AI Act nicht geschaffen („gegebenenfalls"). Die Pflicht bestimmt sich allein nach dem Datenschutzrecht. Eine Prüfung, ob eine Datenschutz-Folgenabschätzung durchzuführen ist, muss nach Art. 35 DS-GVO jedenfalls erfolgen.

- **Sonderregelung für Hochrisiko-KI-Systeme zur biometrischen Fernidentifizierung (Art. 26 Abs. 10 AI Act)**

  Art. 26 Abs. 10 AI Act enthält in seinen sieben Unterabsätzen speziellen Anforderungen für Betreiber eines Hochrisiko-KI-Systems zur nachträglichen biometrischen Fernidentifizierung im Rahmen von Ermittlungen zur gezielten Suche einer Person, die der Begehung einer Straftat verdächtigt wird oder aufgrund einer solchen verurteilt wurde.

- **Information natürlicher Personen bei automatisierter und unterstützter Entscheidung (Art. 26 Abs. 11 AI Act)**

Der Betreiber eines Hochrisiko-KI-Systems in Sinne des Anhangs III des AI Act hat gemäß Art. 26 Abs. 11 AI Act die natürlichen Personen zu informieren, wenn dieses KI-System Entscheidungen trifft, welche die natürliche Person betreffen, oder bei solchen Entscheidungen Unterstützung leistet.

- **Pflicht zur Zusammenarbeit mit den Aufsichtsbehörden (Art. 26 Abs. 12 AI Act)**

  „Die Betreiber arbeiten mit den zuständigen Behörden bei allen Maßnahmen zusammen, die diese Behörden im Zusammenhang mit dem Hochrisiko-KI-System zur Umsetzung dieser Verordnung ergreifen" – so Art. 26 Abs. 12 AI Act wörtlich. Es besteht damit eine Pflicht der Betreiber.

- **Sonderregelungen für Finanzinstitute**

  Für Betreiber, die Finanzinstitute sind und gemäß den Rechtsvorschriften der Union über Finanzdienstleistungen Anforderungen in Bezug auf ihre Regelungen oder Verfahren der internen Unternehmensführung unterliegen, gelten Sonderbestimmungen in Art. 26 Abs. 5, Abs. 6 AI Act.

6.3.2.2 Grundrechte-Folgenabschätzung für Hochrisiko-KI-Systeme (Art. 27 AI Act)

Nach Art. 27 AI Act besteht für den Betreiber eines Hochrisiko-KI-Systems die Pflicht zur Grundrechte-Folgenabschätzung.

Die Pflicht besteht **nur für Hochrisiko-KI-Systeme im Sinne des Art. 6 Abs. 2 AI Act**. Im Anwendungsbereich des Art. 6 Abs. 2 AI Act sind zusätzlich die Hochrisiko-KI-Systeme ausgenommen, die in dem in Anhang III Nr. 2 aufgeführten Bereich verwendet werden sollen.

Nicht alle Betreiber von Hochrisiko-KI-Systemen sind verpflichtet, sondern nur solche,

- bei denen es sich um Einrichtungen des öffentlichen Rechts oder
- private Einrichtungen, die öffentliche Dienste erbringen, handelt, oder
- von Hochrisiko-KI-Systemen gemäß Anhang III Nummer 5 Buchstaben b und c des AI Act.

Die Pflicht besteht nach Art. 27 Abs. 2 Satz 1 AI Act für die erste Verwendung eines Hochrisiko-KI-Systems. In ähnlichen Fällen kann sich der Betreiber auf zuvor durchgeführte Grundrechte-Folgenabschätzungen oder bereits vorhandene Folgenabschätzungen, die vom Anbieter durchgeführt wurden, stützen.

Die Betreiber werden daher gut beraten sein, darauf zu drängen, dass ihnen eine solche Folgenabschätzung vom Anbieter zur Verfügung gestellt wird. Denn mit Blick auf die Anforderungen aus Art. 27 AI Act stellt eine solche Grundrechte-Folgenabschätzung einen erheblichen Aufwand dar, der sich bei der Durchführung

durch den Anbieter leichter amortisieren lässt. Die Pflicht zur Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, die typischerweise die Betreiber treffen (sofern personenbezogene Daten verarbeitet werden), kann hingegen nicht delegiert werden.

Der Betreiber hat der Marktüberwachungsbehörde das Ergebnis der Grundrechte-Folgenabschätzung mitzuteilen, sobald diese durchgeführt ist (Art. 27 Abs. 3 AI Act).

Das Verhältnis zur Datenschutz-Folgenabschätzung des Datenschutzrechts (Art. 35 DS-GVO und Artikel 27 der Richtlinie (EU) 2016/680)) adressiert Art. 27 Abs. 4 AI Act: Wenn eine der in Art. 27 AI Act festgelegten Pflichten bereits infolge einer solchen Datenschutz-Folgenabschätzung erfüllt ist, ergänzt die Grundrechte-Folgenabschätzung nach Art. 27 Abs. 1 AI Act diese Datenschutz-Folgenabschätzung.

6.3.3 Pflichten der weiteren Akteure in Bezug auf Hochrisiko-KI-Systeme

Die Pflichten für weitere Akteure sind in Art. 23 AI Act (Einführer) und Art. 24 AI Act (Händler) geregelt.

Achtung: Beachten Sie, dass es nach Art. 25 AI Act zum Rollenwechsel kommen kann. Unter den dort genannten Voraussetzungen gelten Händler, Einführer, Betreiber oder sonstige Dritte als Anbieter eines Hochrisiko-KI-Systems und müssen die entsprechenden Pflichten erfüllen.

7. Transparenzpflichten für Anbieter und Betreiber bestimmter KI-Systeme (Art. 50 AI Act)

Art. 50 nimmt allgemein KI-Systeme in Bezug. In der Risikokategorisierung sind die KI-Systeme mit geringem bzw. mittlerem Risiko adressiert. Die Risikokategorisierung ergibt sich für den Gesetzgeber offensichtlich daraus, dass mittels dieser KI-Systeme Content generiert wird. Diese KI-Systeme werden daher auch generative KI (Generative AI) bezeichnet.

Art. 50 AI Act regelt **vier Arten von KI-Systemen** und nimmt **entweder den Anbieter oder den Betreiber** in die Pflicht.

Die Ausnahme des Art. 2 Abs. 12 AI Act für Open Source KI-Systeme gilt nicht für Art. 50 AI Act.

Die Tabelle gibt einen Überblick über den Regelungsgehalt des Art. 50 AI Act			
KI-Systeme …	**Verpflichteter**	**Primäre Regelung des AI Act**	**Ergänzende Regelungen**
… die für die direkte Interaktion mit natürlichen Personen bestimmt sind,	Anbieter	Art. 50 Abs. 1 AI Act	Art. 50 Abs. 5, 6 AI Act
… mit allgemeinem Verwendungszweck, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen	Anbieter	Art. 50 Abs. 2 AI Act	Art. 50 Abs. 5, 6 AI Act
Emotionserkennungssystems oder eines Systems zur biometrischen Kategorisierung	Betreiber	Art. 50 Abs. 3 AI Act	Art. 50 Abs. 5, 6 AI Act
… das Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert, die ein Deepfake sind	Betreiber	Art. 50 Abs. 4, 5 AI Act	Art. 50 Abs. 5, 6 AI Act
Die Regelung über verbotene Praktiken in Art. 5 AI Act wird durch Art. 50 nicht aufgehoben oder eingeschränkt (Art. 50 Abs. 6 AI Act). **Mit anderen Worten: Was nach Art. 5 AI Act verboten ist, bleibt verboten.** **Transparenzvorschriften nach anderen EU-Rechtsakten, also auch die DS-GVO, werden durch Art. 50 nicht aufgehoben oder eingeschränkt (Art. 50 Abs. 6 AI Act).**			

Für die Aufdeckung, **Verhütung, Ermittlung oder Verfolgung von Straftaten** sind in den Absätzen des Art. 50 AI Act Sonderregelungen enthalten.

Die Informationen nach Art. 50 Abs. 1 bis Abs. 4 AI Act müssen den betreffenden natürlichen Personen spätestens zum Zeitpunkt der ersten Interaktion oder Aussetzung in klarer und eindeutiger Weise bereitgestellt werden (Art. 50 Abs. 5 Satz 1 AI Act). Die Informationen müssen den geltenden Barrierefreiheitsanforderungen entsprechen (Art. 50 Abs. 5 Satz 2 AI Act).

➤ **KI-Systeme, die zur direkten Interaktion mit natürlichen Personen bestimmt sind (Art. 50 Abs. 1 AI Act)**

KI-Systeme, die für die direkte Interaktion mit natürlichen Personen bestimmt sind (z. B. sog. Chatbots), werden durch Art. 50 Abs. 1 AI Act geregelt.

Der Anbieter muss diese KI-Systeme so konzipieren und entwickeln, dass die betreffenden natürlichen Personen informiert werden, dass sie mit einem KI-System interagieren. Diese Pflicht besteht nur dann nicht, wenn dies aus Sicht einer angemessen informierten, aufmerksamen und verständigen natürlichen Person aufgrund der Umstände und des Kontexts der Nutzung offensichtlich ist. Für diese Ausnahme trägt der Anbieter die Beweislast.

Kurzum: Gegenstand der Informationspflicht ist die Offenlegung, dass mit einem KI-System und nicht mit einem Menschen kommuniziert wird.

Mit der Regelung soll dem Risiko in Bezug auf Identitätsbetrug oder Täuschung entgegengewirkt werden (Erwägungsgrund 132 AI Act). Dem Alter oder einer Behinderung der schutzbedürftigen Gruppen, die mit dem KI-System interagieren, soll Rechnung getragen werden (Erwägungsgrund 132 AI Act).

➤ **Transparenzpflichten für Betreiber bestimmter KI-Systeme (Art. 50 Abs. 2 AI Act)**

Art. 50 Abs. 2 AI Act enthält Regelungen für **KI-Systeme, einschließlich KI-Systemen mit allgemeinem Verwendungszweck, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen.** Erfasst sind sowohl vollständig künstlich erzeugte als auch manipulierte Inhalte (Art. 50 Abs. 2 AI Act). Der Begriff „manipuliert" bezeichnet originär echte Inhalte, die verändert wurden.

Die **Anbieter** müssen sicherstellen, dass die Ausgaben des KI-Systems „in einem maschinenlesbaren Format gekennzeichnet und als künstlich erzeugt oder manipuliert erkennbar sind".

Art. 50 Abs. 2 Satz 2 AI Act konkretisiert die Pflicht weitergehend.

Es gibt **Ausnahmen von der Pflicht.** Nach Art. 50 Abs. 2 S. 3 AI Act besteht diese Pflicht nicht …

- „soweit die KI-Systeme eine unterstützende Funktion für die Standardbearbeitung ausführen" oder
- „die vom Betreiber bereitgestellten Eingabedaten oder deren Semantik nicht wesentlich verändern" oder
- „wenn sie zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten gesetzlich zugelassen sind".

➤ **Emotionserkennungssysteme und Systeme zur biometrischen Kategorisierung (Art. 50 Abs. 3 AI Act)**

Art. 50 Abs. 3 AI Act regelt die Transparenz bei Emotionserkennungssystemen sowie Systemen zur biometrischen Kategorisierung.

Art. 3 Nr. 39 AI Act definiert **„Emotionserkennungssystem"** als „ein KI-System, das dem Zweck dient, Emotionen oder Absichten natürlicher Personen auf der Grundlage ihrer biometrischen Daten festzustellen oder daraus abzuleiten". Eine Konkretisierung enthält Erwägungsgrund 18 AI Act: Der Begriff „Emotionserkennungssystem" sollte als ein KI-System definiert werden, das dem Zweck dient, Emotionen oder Absichten natürlicher Personen auf der Grundlage ihrer biometrischen Daten festzustellen oder daraus abzuleiten. In diesem Begriff geht es um Emotionen oder Absichten wie Glück, Trauer, Wut, Überraschung, Ekel, Verlegenheit, Aufregung, Scham, Verachtung, Zufriedenheit und Vergnügen. Dies umfasst nicht physische Zustände wie Schmerz oder Ermüdung, einschließlich beispielsweise Systemen, die zur Erkennung des Zustands der Ermüdung von Berufspiloten oder -fahrern eigesetzt werden, um Unfälle zu verhindern. Es geht dabei auch nicht um die bloße Erkennung offensichtlicher Ausdrucksformen, Gesten und Bewegungen, es sei denn, sie werden zum Erkennen oder Ableiten von Emotionen verwendet. Bei diesen Ausdrucksformen kann es sich um einfache Gesichtsausdrücke wie ein Stirnrunzeln oder ein Lächeln oder um Gesten wie Hand-, Arm- oder Kopfbewegungen oder um die Stimmmerkmale einer Person handeln, wie eine erhobene Stimme oder ein Flüstern.

Art. 3 Nr. 40 AI Act definiert ein **„System zur biometrischen Kategorisierung"** als „ein KI-System, das dem Zweck dient, natürliche Personen auf der Grundlage ihrer biometrischen Daten bestimmten Kategorien zuzuordnen, sofern es sich um eine Nebenfunktion eines anderen kommerziellen Dienstes handelt und aus objektiven technischen Gründen unbedingt erforderlich ist".

Die Betreiber müssen die betroffenen natürlichen Personen über den Betrieb des Systems informieren **(Informationspflicht)** (Art. 50 Abs. 3 Satz 1 AI Act).

Art. 50 Abs. 3 Satz 1 AI Act sieht dabei explizit vor, dass die Betreiber die hiervon betroffenen personenbezogenen Daten gemäß der **DS-GVO bzw. den Verordnungen (EU) 2016/679 und (EU) 2018/1725 bzw. der Richtlinie (EU) 2016/680**[13] zu verarbeiten haben.

Ergänzend ergibt sich aus Erwägungsgrund 132 AI Act: Natürlichen Personen sollte mitgeteilt werden, wenn sie KI-Systemen ausgesetzt sind, die durch die

[13] Die genannten Rechtsakte sind alle Datenschutzrechtsakte jedoch mit unterschiedlichem Anwendungsbereich.

Verarbeitung ihrer biometrischen Daten die Gefühle oder Absichten dieser Personen identifizieren oder ableiten oder sie bestimmten Kategorien zuordnen können. Solche spezifischen Kategorien können Aspekte wie etwa Geschlecht, Alter, Haarfarbe, Augenfarbe, Tätowierungen, persönliche Merkmale, ethnische Herkunft sowie persönliche Vorlieben und Interessen betreffen. Diese Informationen und Mitteilungen sollten für Menschen mit Behinderungen in entsprechend barrierefrei zugänglicher Form bereitgestellt werden.

➤ Bild-, Ton- oder Videoinhalte sowie Texte (Art. 50 Abs. 4 AI Act)

Art. 50 Abs. 4 AI Act regelt die Pflichten in Bezug auf KI-Systeme, die Bild-, Ton- und Videoinhalte, die ein Deepfake sind (Art. 50 Abs. 4 UAbs. 1 AI Act) sowie Texte (Art. 50 Abs. 4 UAbs. 2 AI Act) erzeugen oder manipulieren.

Die Pflicht der **Betreiber besteht neben der Pflicht der Anbieter nach Art. 50 Abs. 2 AI Act**; beide Pflichten sollen sich komplementieren (Erwägungsgrund 134 AI Act).

Für die Auslegung der Regelung mit Blick auf die freie Meinungsäußerung enthält Erwägungsgrund 134 AI Act Maßgaben.

Art. 50 Abs. 4 unterscheidet in seinen beiden Unterabsätzen zwischen einerseits Bild-, Ton- oder Videoinhalten als Deepfakes (Art. 50 Abs. 4 UAbs. 1 AI Act) und andererseits Textinhalten (Art. 50 Abs. 4 UAbs. 2 AI Act):

▸ Bild-, Ton- oder Videoinhalte als Deepfakes (Art. 50 Abs. 4 UAbs. 1 AI Act)

Art. 50 Abs. 4 UAbs. 1 AI Act zwingt dazu, offenzulegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden, wenn Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert werden, die ein Deepfake sind.

Art. 3 Nr. 60 AI Act definiert ein „Deepfake" als „einen durch KI erzeugten oder manipulierten Bild-, Ton- oder Videoinhalt, der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde".

Für den künstlerischen Kontext enthält Art. 50 Abs. 4 UAbs. 1 Satz 3 AI Act eine Abweichung: „Ist der Inhalt Teil eines offensichtlich künstlerischen, kreativen, satirischen, fiktionalen oder analogen Werks oder Programms, so beschränken sich die in diesem Absatz festgelegten Transparenzpflichten darauf, das Vorhandensein solcher erzeugten oder manipulierten Inhalte in geeigneter

Weise offenzulegen, die die Darstellung oder den Genuss des Werks nicht beeinträchtigt".

- **Texte zu Angelegenheiten von öffentlichem Interesse (Art. 50 Abs. 4 UAbs. 2 AI Act)**

  Art. 50 Abs. 4 UAbs. 2 AI Act regelt KI-Systeme, die Texte erzeugen oder manipulieren, die veröffentlicht werden, um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren. Es muss offengelegt werden, dass der Text künstlich erzeugt oder manipuliert wurde.

  Damit sind schon alle Texte erfasst, die mittels KI-System erzeugt werden. Das ist ein wesentlicher Unterschied zu Art. 50 Abs. 4 UAbs. 1 AI Act.

  Die **Ausnahme von der Kennzeichnungspflicht** sieht Art. 50 Abs. 4 UAbs. 2 Satz 2 AI Act vor: Wenn die durch KI erzeugten Inhalte einem Verfahren der menschlichen Überprüfung oder redaktionellen Kontrolle unterzogen wurden und wenn eine natürliche oder juristische Person die redaktionelle Verantwortung für die Veröffentlichung der Inhalte trägt, muss eine Kennzeichnung nach Maßgabe des Art. 50 Abs. 4 UAbs. 2 S. 1 AI Act nicht erfolgen.

8. KI-Modelle mit allgemeinem Verwendungszweck (Artt. 51–56 AI Act)

Das Kapitel V des AI Act ist erst „auf den letzten Metern" des Gesetzgebungsverfahrens eingefügt worden. Es war im Gesetzgebungsverfahren umstritten, ob KI-Modelle bzw. KI-Modelle mit allgemeinem Verwendungszweck überhaupt geregelt werden sollen. Der Streit ist zwar mit der Verabschiedung entschieden worden, aber das Kapitel V ist aufgrund der späten Einfügung nur beschränkt mit den anderen Regelungen harmonisiert und wirkt wie eine „Insel" im AI Act.

Die **KI-Modelle mit allgemeinem Verwendungszweck** werden in Artt. 51 bis 56 AI Act auch unabhängig von einer Risikokategorisierung geregelt. Die Regelungen nehmen nur die **Anbieter, nicht aber weitere Akteure** in die Pflicht.

Das Kapitel V des AI Act adressiert **KI-Modelle mit allgemeinem Verwendungszweck und nicht KI-Systeme.** Spezielle Regelungen enthält Kapitel V für **KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko**. Was ein KI-Modell ist, wird – auch in Abgrenzung zum KI-System – in diesem Buch erläutert.

Die Reihenfolge der Regelung des Kapitel V ist verwirrend:

- **Artt. 53, 54 AI Act** enthalten die Regelungen für **KI-Systeme mit allgemeinem Verwendungszweck**
- **Art. 55 AI Act** enthält die Regelungen für **KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko**. Aber: **Artt. 51, 52 AI Act** regeln die Einstufung eines KI-Modells mit allgemeinem Verwendungszweck als einer mit systemischem Risiko.

Weitere Erläuterungen zum Verständnis und zur Behandlung der KI-Modelle mit allgemeinem Verwendungszweck enthalten die **Erwägungsgründe 97–118 sowie 161–164, 173, 174 und 179 AI Act**.

8.1 KI-Modelle mit allgemeinem Verwendungszweck (Artt. 53, 54 AI Act)

Die **Anforderungen an KI-Modelle mit allgemeinem Verwendungszweck regelt Art. 53 AI Act**. Diese Regelung entsprechen dem Marktortprinzip nicht nur für Anbieter mit Sitz in der EU. Dementsprechend regelt **Art. 54 AI Act die Pflicht zur Benennung eines Bevollmächtigten**.

8.2 KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko (Art. 55 AI Act)

Art. 55 AI Act enthält ergänzende Regelungen zu Art. 53, 54 AI Act, wenn es sich um ein KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko handelt. Wann ein systemisches Risiko anzunehmen ist, regeln die Artt. 51, 52 AI Act.

Das **„systemische Risiko"** ist in **Art. 3 Nr. 65 AI Act** definiert als „ein Risiko, das für die Fähigkeiten mit hoher Wirkkraft von KI-Modellen mit allgemeinem Verwendungszweck spezifisch ist und aufgrund deren Reichweite oder aufgrund tatsächlicher oder vernünftigerweise vorhersehbarer negativer Folgen für die öffentliche Gesundheit, die Sicherheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft insgesamt erhebliche Auswirkungen auf den Unionsmarkt hat, die sich in großem Umfang über die gesamte Wertschöpfungskette hinweg verbreiten können".

Ein KI-Modell mit allgemeinem Verwendungszweck wird nach Art. 51 Abs. 1 AI Act als KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko eingestuft, wenn eine der folgenden Bedingungen erfüllt ist:

- Es verfügt über Fähigkeiten mit hohem Wirkungsgrad, die mithilfe geeigneter technischer Instrumente und Methoden, einschließlich Indikatoren und Benchmarks, bewertet werden;

- einem unter Berücksichtigung der in Anhang XIII festgelegten Kriterien von der Kommission von Amts wegen oder aufgrund einer qualifizierten Warnung des wissenschaftlichen Gremiums getroffenen Entscheidung zufolge verfügt es über Fähigkeiten oder eine Wirkung, die denen gemäß Buchstabe a entsprechen.

Die **„Fähigkeiten mit hoher Wirkkraft"** sind durch **Art. 3 Nr. 64 AI Act** definiert als „Fähigkeiten, die den bei den fortschrittlichsten KI-Modellen mit allgemeinem Verwendungszweck festgestellten Fähigkeiten entsprechen oder diese übersteigen".

Dass ein KI-Modell mit allgemeinem Verwendungszweck über Fähigkeiten mit hohem Wirkungsgrad verfügt, wird angenommen, wenn die kumulierte Menge der für sein Training verwendeten Berechnungen, gemessen in Gleitkommaoperationen, mehr als 10Hoch25 beträgt (Art. 51 Abs. 2 AI Act).

9. Sanktionen (Art. 99 AI Act)

Die Sanktionen für Verstöße gegen den AI Act regelt sein Art. 99 wie folgt:		
Verstoß	**Regelung**	**Sanktion in Euro**
		Die Sanktionen in Art. 99 AI Act sind so gestaltet, dass eine Geldbuße bis zu einer bestimmten Summe oder einem bestimmten Prozentsatz des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden kann, je nachdem, welcher Betrag höher ist.
Missachtung des Verbots der in Art. 5 AI Act genannten KI-Praktiken	Art. 91 Abs. 3 AI Act	35 Mio./7 %

➤ Pflichten der Anbieter gemäß Artikel 16; ➤ Pflichten der Bevollmächtigten gemäß Artikel 22; ➤ Pflichten der Einführer gemäß Artikel 23; ➤ Pflichten der Händler gemäß Artikel 24; ➤ Pflichten der Betreiber gemäß Artikel 26; ➤ für notifizierte Stellen geltende Anforderungen und Pflichten gemäß Artikel 31, Artikel 33 Absätze 1, 3 und 4 bzw. Artikel 34; ➤ Transparenzpflichten für Anbieter und Betreiber gemäß Artikel 50.	Art. 99 Abs. 4 AI Act	15 Mio./3 %
falsche, unvollständige oder irreführende Informationen gegenüber notifizierten Stellen oder zuständigen nationalen Behörden auf deren Auskunftsersuchen	Art. 99 Abs. 5 AI Act	7,5 Mio./1 %
Sonderregelung für KMU und Start-ups: Im Fall von KMU, einschließlich Start-up-Unternehmen, gilt für jede in diesem Artikel genannte Geldbuße der jeweils niedrigere Betrag aus den in den Absätzen 3, 4 und 5 genannten Prozentsätzen oder Summen (Art. 99 Abs. 6 AI Act).		

Die Sanktionen des Art. 99 AI Act gelten jedoch nicht automatisch, sondern müssen durch ein nationales Gesetz umgesetzt („zum Leben erweckt") werden („*Entsprechend den Vorgaben dieser Verordnung erlassen die Mitgliedstaaten Vorschriften für Sanktionen und andere Durchsetzungsmaßnahmen, zu denen auch Verwarnungen und nichtmonetäre Maßnahmen gehören können, […]*", Art. 99 Abs. 1 AI Act). Insofern unterscheidet sich der AI Act von der Sanktionsregelung in Art. 83 DS-GVO, die keine Umsetzung durch ein nationales Gesetz erfordert.

Art. 99 Abs. 7 AI Act legt die Kriterien zur Entscheidung über das Ob und die Höhe einer Geldbuße fest.

Art. 100 AI Act regelt die Verhängung von Geldbußen gegen Organe, Einrichtungen und sonstige Stellen der Union. Zuständig hierfür ist der europäische Datenschutzbeauftragte.

10. KI-Beauftragter

Der AI Act regelt – anders als die DS-GVO in Artt. 37 bis 39 DS-GVO für den Datenschutzbeauftragten – nicht den einen KI-Beauftragten explizit. Der AI Act regelt auch keine dem Datenschutzbeauftragten vergleichbaren Qualifikationen eines KI-Beauftragten.

Wird allgemein ein KI-Beauftragter – der als **Allgemeiner KI-Beauftragter** skizziert werden kann – institutionalisiert, muss unternehmensintern aus der ihm zugewiesenen Aufgabe die Befähigung definiert werden. Die Erforderlichkeit eines solchen Beauftragten als gesonderte Institution im Unternehmen darf bezweifelt werden.

Im **Kontext von Hochrisiko-KI-Systemen** lassen sich aus der Risikomanagementpflicht (Art. 26 Abs. 1 AI Act) und der Pflicht zur menschlichen Aufsicht (Art. 26 Abs. 2 AI Act) eine Aufgabe und die Befähigung ableiten. Art. 26 Abs. 2 AI Act formuliert, dass er über die „erforderliche Kompetenz, Ausbildung und Befugnis verfügen" muss. Hieran muss sich dann auch eine Qualifikation zum KI-Beauftragten ableiten, der mit Blick auf seine besonderen Fähigkeiten als **Hochrisiko-KI-Beauftragter** skizziert werden kann.

Soweit **Anbieter von KI-Modellen mit allgemeinem Verwendungszweck** im Sinne des Kapitels V des AI Act betroffen sind, ist ebenfalls ein KI-Beauftragter nicht geregelt und es bedürfte gerade speziell ausgeprägter Befähigungen mit Blick auf die in Kapitel V des AI Act geregelten Inhalte.

Der Unterschied liegt darin, dass je nach Kontext der KI-Beauftragte über unterschiedliche und unterschiedlich ausgeprägte Kompetenzen verfügen muss. Ein Hochrisiko-KI-Beauftragter muss mit den Artt. 8 bis 27 AI Act vertraut sein, während ein allgemeiner KI-Beauftragter möglicherweise nur mit Art. 50 AI Act vertraut sein muss.

Gerade außerhalb des Kontexts von Hochrisiko-KI-Systemen darf daher die Erforderlichkeit eines KI-Beauftragten bezweifelt werden. Jedenfalls kann dessen Befähigung an den Aufgaben ausgerichtet sein.

In allen anderen Konstellationen kann jedenfalls nicht abstrakt aus dem AI Act abgeleitet werden, dass es eines KI-Beauftragten bedarf und über welche Befähigung er verfügen muss.

Auf keinen Fall darf der – wie auch immer geartete – KI-Beauftragte mit der Pflicht zur KI-Kompetenz nach Art. 4 AI Act verwechselt oder vermischt werden! Über die KI-Kompetenz muss jeder verfügen, der KI nutzt und nicht nur ein KI-Beauftragter. Umgekehrt bedarf nicht jeder, der im oder für das Unternehmen KI nutzt, einer Befähigung, wie sie der Rolle eines KI-Beauftragten zukommen müsste.

Was bedeutet das in zeitlicher Hinsicht? Die Regelungen für Hochrisiko-KI-Systeme gelten ab dem 02.08.2026 und 02.08.2027.

Hinweis

Unterscheiden Sie zwischen KI-Kompetenz und KI-Beauftragtem!

Unterscheiden Sie die Pflicht zur Einhaltung des AI Acts und das Erfordernis eines KI-Beauftragten. Die Pflichten nach dem AI Act müssen eingehalten werden. Hierfür ist die Unternehmensleitung wie auch bei anderen gesetzlichen Pflichten verantwortlich. Das erfordert jedoch keinen KI-Beauftragten und ein KI-Beauftragter ändert auch nichts an der Pflichtenstellung der Unternehmensleitung. Die Aufgabe und die Position eines KI-Beauftragten müssen daher durch das Unternehmen selbst bestimmt werden und die Erfüllung der Pflichten nach dem AI Act kann recht unterschiedlich erfolgen.

11. Verhältnis zur DS-GVO

Gegenstand des vorliegenden Buches ist die Darstellung der Rechtsakte der EU-Datenstrategie, aber nicht eine vollständige Beleuchtung des Themas Künstliche Intelligenz. Dementsprechend liegt der Schwerpunkt beim Thema Künstliche Intelligenz beim AI Act. Gleichwohl werden nachfolgend Kernüberlegungen aus der Sicht des Datenschutzrechts angesprochen.

Die **Rechtsvorschriften der Union zum Schutz personenbezogener Daten, der Privatsphäre und der Vertraulichkeit der Kommunikation** gelten nach Art. 2 Abs. 7 AI Act auch für die Verarbeitung personenbezogener Daten im Zusammenhang mit den im AI Act festgelegten Rechten und Pflichten. Der AI Act „berührt nicht" die DS-GVO bzw. die Verordnung 2018/1725[14] und ebenso nicht die

[14] Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG

Richtlinie 2002/58/EG[15] bzw. Richtlinie 2016/680[16], wobei die Art. 10 Abs. 5 und Art. 59 des AI Act „unbeschadet" gelten.

Der Erwägungsgrund 63 S. 3 AI Act führt ergänzend aus, dass der AI Act ***nicht so verstanden werden, dass sie eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten*** *bildet, „****es sei denn, in dieser Verordnung ist ausdrücklich etwas anderes vorgesehen****".* **Hinweis: Im Grundsatz geht damit die DS-GVO dem AI Act vor. Aber kein Grundsatz ohne Ausnahmen.**

Es gibt einige wenige Regelungen, die im Widerspruch zur DS-GVO stehen. Allerdings ist nach ErwGr. 63 S. 3 AI Act erforderlich, dass sie explizit regeln. Das sind, insbesondere:

- **Art. 10 Abs. 5 AI Act (plus ErwGr. 70 AI Act)**
- *„Soweit dies für die* ***Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen*** *im Einklang mit Absatz 2 Buchstaben f und g dieses Artikels* ***unbedingt erforderlich*** *ist, dürfen die Anbieter solcher Systeme* ***ausnahmsweise besondere Kategorien personenbezogener Daten verarbeiten, wobei*** *sie angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen treffen müssen. Zusätzlich zu den Bestimmungen der Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinie (EU) 2016/680 müssen alle folgenden Bedingungen erfüllt sein, damit eine solche Verarbeitung stattfinden kann: […]"*
- **Art. 59 AI Act-Weiterverarbeitung personenbezogener Daten zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse im KI-Reallabor**
- *„(1)* ***Rechtmäßig für andere Zwecke erhobene personenbezogene Daten dürfen*** *im KI-Reallabor ausschließlich für die Zwecke der Entwicklung, des Trainings und des Testens bestimmter KI-Systeme im Reallabor verarbeitet werden, wenn alle der folgenden Bedingungen erfüllt sind: […]"*
- **ErwGr. 140 AI Act: Verarbeitung personenbezogener Daten in KI-Reallaboren**

[15] Datenschutzrichtlinie für elektronische Kommunikation – auch bekannt als „ePrivacy-Richtlinie"

[16] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates

- *„Die vorliegende Verordnung sollte im Einklang mit Artikel 6 Absatz 4 und Artikel 9 Absatz 2 Buchstabe g der Verordnung (EU) 2016/679 und den Artikeln 5, 6 und 10 der Verordnung (EU) 2018/1725 sowie unbeschadet des Artikels 4 Absatz 2 und des Artikels 10 der Richtlinie (EU) 2016/680* ***die Rechtsgrundlage für die Verwendung – ausschließlich unter bestimmten Bedingungen – personenbezogener Daten, die für andere Zwecke erhoben wurden, zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse innerhalb des KI-Reallabors durch die Anbieter und zukünftigen Anbieter im KI-Reallabor bilden.*** *Alle anderen Pflichten von Verantwortlichen und Rechte betroffener Personen im Rahmen der Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinie (EU) 2016/680 gelten weiterhin****. Insbesondere sollte diese Verordnung keine Rechtsgrundlage im Sinne des Artikels 22 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679 und des Artikels 24 Absatz 2 Buchstabe b der Verordnung (EU) 2018/1725 bilden.*** *Anbieter und zukünftige Anbieter im KI-Reallabor sollten angemessene Schutzvorkehrungen treffen und mit den zuständigen Behörden zusammenarbeiten, unter anderem indem sie deren Anleitung folgen und zügig und nach Treu und Glauben handeln, um etwaige erhebliche Risiken für die Sicherheit, die Gesundheit und die Grundrechte, die bei der Entwicklung, bei der Erprobung und bei Versuchen in diesem Reallabor auftreten können, zu mindern.“*

Als Ergänzungen zum Datenschutzrecht lassen sich folgende Regelungen verstehen:

- **Art. 26 Abs. 11 AI Act**

- *„(11) Unbeschadet des Artikels 50 der vorliegenden Verordnung informieren die Betreiber der in Anhang III aufgeführten Hochrisiko-KI-Systeme, die natürliche Personen betreffende Entscheidungen treffen oder bei solchen Entscheidungen Unterstützung leisten,* ***die natürlichen Personen darüber, dass sie der Verwendung des Hochrisiko-KI-Systems unterliegen.*** *Für Hochrisiko-KI-Systeme, die zu Strafverfolgungszwecken verwendet werden, gilt Artikel 13 der Richtlinie (EU) 2016/680.“*

- **Art. 27 AI Act Grundrechte-Folgenabschätzung für Hochrisiko-KI-Systeme**

- *„(4) Wird eine der in diesem Artikel festgelegten Pflichten bereits infolge einer gemäß Artikel 35 der Verordnung (EU) 2016/679 oder Artikel 27 der Richtlinie (EU) 2016/680 durchgeführten Datenschutz-Folgenabschätzung erfüllt,* ***so ergänzt die Grundrechte-Folgenabschätzung gemäß Absatz 1 des vorliegenden Artikels diese Datenschutz-Folgenabschätzung.****“*

- **Transparenzpflichten nach Art. 50 AI Act – insbesondere Art. 50 Abs. 1, 3 AI Act**
- *„(1) Die Anbieter stellen sicher, dass KI-Systeme, die für die direkte Interaktion mit natürlichen Personen bestimmt sind,* ***so konzipiert und entwickelt werden, dass die betreffenden natürlichen Personen informiert werden, dass sie mit einem KI-System interagieren****, es sei denn, […]"*
- *„(3) Die Betreiber eines Emotionserkennungssystems oder eines Systems zur biometrischen Kategorisierung* ***informieren die davon betroffenen natürlichen Personen über den Betrieb des Systems und verarbeiten personenbezogene Daten gemäß den Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinie (EU) 2016/680****. […]"*
- **Löschpflichten in Art. 26 Abs. 10 UAbs. 1 und Art. 60 Abs. 4, Abs. 5 S. 1 AI Act**

Wie sich das in der Praxis auswirkt, ist noch nicht abschließend geklärt. Die Diskussion zu dem noch jungen AI Act wird zu verfolgen sein. In diesem Kontext ist auch zu beachten, dass die meisten Regelungen erst ab dem 02.08.2026 anzuwenden sind, sodass Zeit zur Klärung besteht.

Mit anderen Worten: Die DS-GVO ist vollständig zu beachten und hat Vorrang.

Entsprechend der Zielsetzung des Buches, einen Überblick über die neuen Rechtsakte zu geben, wird das Datenschutzrecht nicht vertieft. Hinzu kommt, dass aktuell die relevanten Aspekte (insbesondere Personenbezug, Rollenverteilung, Rechtsgrundlagen, Erfüllung von Transparenzpflichten und Betroffenenrechten) generell und insbesondere in Bezug auf die Nutzung von KI kontrovers diskutiert werden.

- Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 6. Mai 2024, Künstliche Intelligenz und Datenschutz, Version 1.0 (Link mit Stand vom 18.02.2025: https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf)
- Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, „Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von künstlicher Intelligenz", Version 2.0, 17.10.2024 (Link mit Stand vom 18.02.2025: https://www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki/)
- Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Checkliste zum Einsatz LLM-basierter Chatbots, 13.11.2023 (Link mit Stand

vom 18.02.2025: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/20231113_Checkliste_LLM_Chatbots_DE.pdf)

- Bayerisches Landesamt für Datenschutzaufsicht, Datenschutzkonforme Künstliche Intelligenz–Checkliste mit Prüfkriterien nach DS-GVO, (Link mit Stand vom 18.02.2025: https://www.lda.bayern.de/media/ki_checkliste.pdf)
- Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Diskussionspapier: Large Language Models und personenbezogene Daten, 18.07.2024 (Link mit Stand vom 18.02.2025: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Diskussionspapier_HmbBfDI_KI_Modelle.pdf)
- Pressemitteilung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 2. September 2024, Strategieklausur der Datenschutzkonferenz in Speyer: Nutzung von KI zentrales Thema, (Link mit Stand vom 18.02.2025: https://datenschutzkonferenz-online.de/media/pm/2024-09-02_Klausurtagung_KI.pdf)
- Europäischer Datenschutzausschuss, „Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models Adopted on 17 December 2024“ (Link mit Stand vom 18.02.2025: https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.p

ABBILDUNGS- UND ARBEITSHILFENVERZEICHNIS

Regulierungen Zeitstrahl 12

Übersicht Rechtsakte 13

BSIG Prüfschema 26

AI-Act Risikotaxonomie 123

Impressum

PrivacyXperts – ein Unternehmensbereich des VNR Verlags für die Deutsche Wirtschaft AG,
Theodor-Heuss-Str. 2–4, 53095 Bonn
Handelsregister: HRB 8165
Registergericht: Amtsgericht Bonn vertreten durch den Vorstand: Richard Rentrop
Umsatzsteuer-Identifikationsnummer gemäß §27a Umsatzsteuergesetz: DE 812639372
Telefon: 02 28 / 9 55 01 60
Fax: 02 28 / 3 69 64 80 (bei Rückfragen bitte Kundennummer angeben)
Vorstand: Richard Rentrop, Bonn
Internet: www.privacyxperts.de
E-Mail: kundendienst@privacyxperts.de
Herausgeber und redaktionell Verantwortlicher: Michael Jodda (Adresse siehe Verlag)
Autor: Jens Eckhardt, Düsseldorf
Produktmanagement: Milena Eilers, Bonn
Satz & Layout: Bettina Pour-Imani, BB-Design, Birken-Honigsessen
Druck: DCM Druck Center Meckenheim GmbH, Werner-von-Siemens-Str. 13,
53340 Meckenheim
Titelbild: VIK – Adobe.Stock.com

Alle Angaben wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen.Eine Gewähr kann deshalb nicht übernommen werden.

© 2025 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Berlin, Bukarest, Jacksonville, Manchester, Passau, Warschau

PRIVACYXPERTS



PX-EMF-EU-25/17

www.privacyxperts.de