

Whitepaper

Neue Pflichten für Tech- & Cloud- Anbieter

Ein praxisnaher Überblick über die
Umsetzung der EU-Digitalstrategie im
Unternehmensalltag



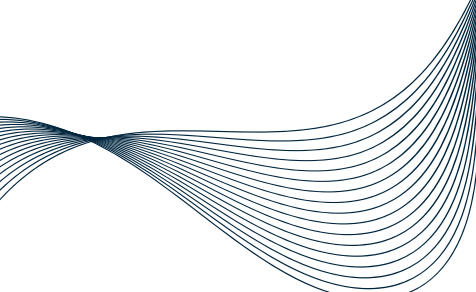
Vorwort

Europa zieht die Regulierungsschrauben an – und das nicht irgendwo, sondern im Herzen der digitalen Wertschöpfung. Daten, Künstliche Intelligenz, Cybersicherheit und Plattformregeln sind längst nicht mehr nur Themen für große Tech-Konzerne. Die neuen Regelungen betreffen inzwischen nahezu jedes Unternehmen, das digitale Technologien einsetzt, vernetzte oder intelligente Produkte entwickelt (z.B. IoT-Geräte), digitale Dienste bereitstellt oder in digitalen Wertschöpfungsketten tätig ist.

Mit einem dichten Netz aus neuen Vorgaben – von der KI-Verordnung über den Cyber Resilience Act bis hin zu NIS-2 und dem Data Act – definiert die EU die Spielregeln für die digitale Wirtschaft neu. Für Unternehmen, die Tech-Services anbieten, Software entwickeln oder vernetzte Produkte herstellen, ist die Botschaft klar: **Wer digitale Geschäfte macht, muss mehr Verantwortung übernehmen.**

Dabei ist die schiere Menge an neuen Regelungen und Vorgaben beachtlich und stellt Unternehmen vor neue Herausforderungen. Dies beginnt bei der Unternehmensorganisation, wo Cybersicherheitsvorgaben wie NIS-2 oder der Digital Operational Resilience Act (DORA) auf Unternehmensebene umgesetzt werden müssen und geht von dort in **nahezu jeden Unternehmensbereich**. Die Regelungen greifen ineinander, verschärfen bestehende Haftungsregeln, schaffen neue Transparenzanforderungen und verlangen, dass Sicherheit, Datenstrategie und Rechtskonformität von Anfang an mitgedacht werden. „Compliant“ zu sein wird damit zunehmend komplexer.

Das hat auch die Europäische Union (EU) selbst erkannt und am 19. November 2025 zwei Verordnungsvorschläge vorgestellt (nachfolgend **„Digital Omnibus“**), welche die erst vor kurzem eingeführten Regeln für Künstliche Intelligenz, Cybersicherheit und den Umgang mit Daten wieder etwas abschwächen und besser miteinander harmonisieren sollen. Bislang handelt es sich beim Digitalen Omnibus jedoch nur um erste Vorschläge – bis es endgültige Änderungen gibt, wird es noch dauern.



Dieses Whitepaper richtet sich an Unternehmen, die als Anbieter von Leistungen auf dem Markt auftreten, sprich digitale Produkte entwickeln und anbieten oder digitale Dienstleistungen erbringen. Das Whitepaper soll Ihnen dabei helfen, einen Überblick über die neue Regelungslandschaft zu gewinnen. Dabei ist es nicht als juristische Abhandlung gedacht, sondern als **praktischer Wegweiser**: Es hilft Ihnen, die Vielzahl neuer EU-Vorgaben zu erfassen, Ihre Rollen und Pflichten richtig einzuordnen und daraus strategische Entscheidungen für Ihr Unternehmen abzuleiten.

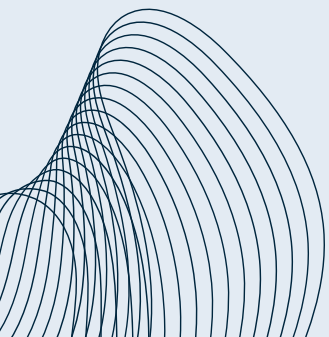
Dabei haben wir die regulatorischen Anforderungen dort verortet, wo sie hingehören: in Ihre Unternehmensabläufe. Dementsprechend folgt der **Aufbau des Whitepapers nicht der Logik des Gesetzgebers, sondern der Logik der typischen Geschäftsprozesse in einem Unternehmen** („Workflow-Compliance“).

Denn wer die neuen Regeln rechtzeitig versteht, kann nicht nur Risiken reduzieren, sondern sich auch Wettbewerbsvorteile durch die richtigen Weichenstellungen sichern.

Hamburg, Februar 2026

Inhalt

Phase 1: Entwicklung & Design	5
1. Cyber Resilience Act: Sicherheit ab der Entwicklung	5
2. High-Risk oder harmlos? Der abgestufte Pflichtenkatalog der KI-Verordnung	6
3. Aufbruch von Datenmonopolen: Der Data Act	8
4. Der Data Governance Act: Fundament einer europäischen Datenwirtschaft	10
Phase 2: Vertrieb & Vertragsgestaltung	11
Data Act: Neue Informationspflichten, Datenlizenzen und Cloud-Switching- Regelungen	11
Phase 3: Laufender Betrieb	13
1. KI-Verordnung: Pflichten nach der Inbetriebnahme	13
2. Digital Services Act: Schutz für Nutzer und Chancen für Unternehmen	14
3. Cyber Resilience Act: Cybersicherheit über den ganzen Produktlebenszyklus	15
Phase 4: Haftung & Exit	16
1. Cyber Resilience Act: Neue Haftungsregeln bei Produkten mit digitalen Elementen	16
2. Produkthaftungsrichtlinie – Haftung entlang der gesamten Lieferkette	17
3. Data Act: Das Ende des Vendor Lock-in – Datenfreiheit statt künstlicher Hürden	18





Ansatzpunkte der Regulierung im Überblick

Fast jeder Unternehmensbereich ist betroffen



Phase 1: Entwicklung & Design

Viele der neuen EU-Vorgaben sind produktbezogen und betreffen direkt das Produkt selbst, und zwar über den gesamten Lebenszyklus hinweg. Das bedeutet: Wer digitale Produkte oder Services anbietet, muss künftig Datenstrategien, Sicherheitsanforderungen, Transparenzpflichten und Haftungsthemen von Anfang an mitdenken. Auch verschärft die EU mit dem Cyber Resilience Act (CRA) die sicherheitsrechtlichen Anforderungen an digitale Produkte.

1. Cyber Resilience Act – Sicherheit ab der Entwicklung

Cybersicherheit muss von Anfang ein zentraler Bestandteil der Produktentwicklung sein. Die neuen Regelungen des CRA, von denen die Wichtigsten ab Dezember 2027 greifen, betreffen insbesondere nahezu alle Hersteller vernetzter Geräte und schaffen verbindliche Sicherheitsstandards über den gesamten Produktlebenszyklus hinweg. Daneben fallen auch Hersteller von Software- und Cloud-Lösungen (z.B. Steuerungssoftware für IoT-Geräte, mobile Apps, Passwortmanager; Firewalls, Intrusion-Detection-Systeme, Intrusion-Prevention-Systeme etc.) unter das Pflichtenprogramm des CRA.

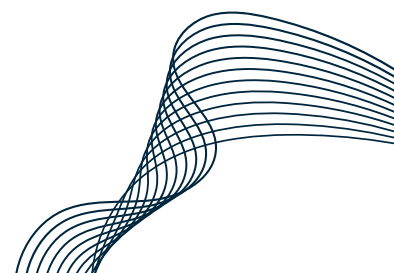
Bereits in der Entwicklungsphase sollten Unternehmen den jeweils relevanten Sicherheitsstandard für ihr Produkt identifizieren. Erst wenn klar ist, welche Anforderungen einzuhalten sind, können Sicherheitsprozesse strukturiert verankert werden. Ein zentrales Instrument dafür ist die Software Bill of Materials (SBOM) – eine vollständige Auflistung aller verwendeten Softwarekomponenten, einschließlich Open-Source-Bausteinen. Nur wer alle eingesetzten Komponenten kennt, kann Sicherheitslücken erkennen, bewerten und schließen.

Ergänzend verlangt der CRA künftig eine Konformitätserklärung mit CE-Kennzeichnung. Dabei gilt: Je sicherheitskritischer das Produkt, desto strenger sind die Anforderungen der Konformitätsbewertung. Hersteller weisen damit nach, dass ihr Produkt auch die Sicherheitsanforderungen des CRA erfüllt.



To-Do für Unternehmen:

Zentrales To Do ist die Prüfung der für das Produkt relevanten Sicherheitsstandards und -vorgaben. Eine frühzeitige Umsetzung gewährleistet, kostspielige Nacharbeiten oder Entwicklungssackgassen zu vermeiden und Haftungsrisiken zu minimieren.



2. High-Risk oder harmlos? Der abgestufte Pflichtenkatalog der KI-Verordnung

Mit der neuen KI-Verordnung hat die EU einen umfassenden Rechtsrahmen für die Entwicklung und den Einsatz künstlicher Intelligenz geschaffen. Ziel ist es, Innovationen zu ermöglichen, aber unter klaren Regeln und abgestuften Pflichten.

Für Entwickler von KI-Lösungen bzw. Produkten mit KI-Integration bedeutet das: Compliance beginnt nicht erst beim Verkauf, sondern bereits in der Design-/Entwicklungsphase. Wer KI-Systeme entwickelt und in den Verkehr bringt, trägt die Hauptverantwortung für die Marktfähigkeit des Produkts.

Konzeption & Rollenklärung: Definition von Identität und Einsatzzweck

Noch vor dem Training des Modells steht die entscheidende Weichenstellung: Die Definition des Einsatzzwecks. Anders als bei klassischer Software bestimmt in der KI-Verordnung der vom Anbieter definierte Zweck die Regulierungstiefe. Es ist zu klären, ob ein KI-System für einen spezifischen Zweck (z. B. Kreditwürdigkeitsprüfung) oder eine KI mit allgemeinem Verwendungszweck (General Purpose AI) entwickelt wird. Ebenso relevant ist die Frage, ob eine Eigenentwicklung vorliegt oder Modelle/Systeme Dritter integriert werden.

Weichenstellung durch Risikoklassen: Von Verbot bis Transparenzpflicht

Die KI-Verordnung arbeitet mit einem risikobasierten Ansatz. Für die Entwicklungsphase bedeutet dies, dass die KI basierend auf dem Einsatzzweck in eine der Risikoklassen der KI-Verordnung eingeordnet werden muss. Dieser Schritt ist von ganz entscheidender Bedeutung, denn: Je nach Risikoklasse unterliegt die KI unterschiedliche Pflichten. Dabei gilt, dass die Anforderungen umso strenger sind, je höher das Risiko ist:

Einige KI-Anwendungen sind vollständig verboten, andere (Hochrisiko-KI) dürfen nur unter strengen Voraussetzungen eingesetzt werden. Die KI-Verordnung stellt bei solchen KI-Lösungen erhebliche Anforderungen an die Datenqualität (Trainings-, Validierungs- und Testdaten), die Dokumentation und das Risikomanagement.

Wieder andere KI-Lösungen können weitgehend frei genutzt werden, müssen aber ggf. bestimmte Transparenzpflichten erfüllen (z.B. Chatbots oder Deepfakes).



Phase 1: Entwicklung & Design

KI und Datenschutz: Geht KI datenschutzkonform?

Losgelöst davon, inwieweit die KI-VO Anwendung findet, stellen sich Unternehmen und Organisationen immer wieder die Frage, ob personenbezogene Daten für Test- bzw. Trainingszwecke überhaupt genutzt werden dürfen. Auch die EU hat dieses Thema erkannt und im Digitalen Omnibus einen Vorschlag aufgenommen, der klarstellt, dass die Verarbeitung personenbezogener Daten für die Zwecke der Entwicklung und des Betriebs von KI-Systemen bzw. Modellen unter Einhaltung bestimmter Voraussetzungen auf die Rechtsgrundlage des „berechtigten Interesses“ gestützt werden kann.

Zudem sieht der Vorschlag vor, dass künftig sensible Daten unter Einhaltung strenger Voraussetzungen zur Erkennung und Korrektur von Bias nicht nur in Hochrisiko-Systemen, sondern auch in anderen KI-Systemen und -Modellen verarbeitet werden dürfen.

Künftige Compliance-Erleichterungen durch den Digitalen Omnibus?

Daneben könnte der Digitale Omnibus weitere Vereinfachungen mit sich bringen. Im Vorschlag ist beispielsweise vorgesehen, dass KI-Systeme, die als Nicht-Hochrisiko eingestuft wurden, künftig nicht mehr in die EU-Datenbank eingetragen werden müssen.

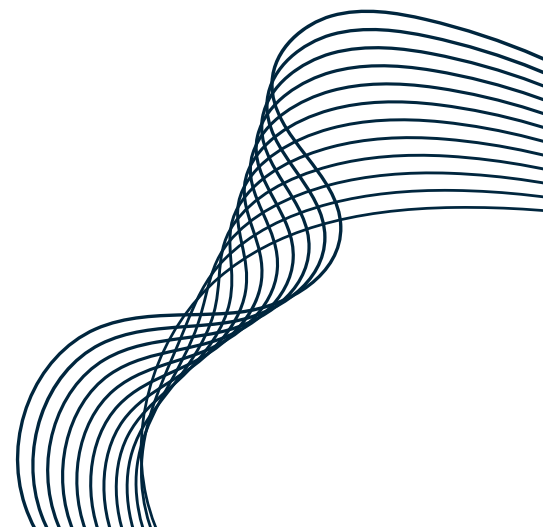
Gleichzeitig sieht der Vorschlag Entlastungen für kleinere Unternehmen vor, wie etwa vereinfachte technische Dokumentationen und reduzierte Bußgelder. Es bleibt abzuwarten, ob sich der Vorschlag durchsetzen wird, sodass Unternehmen die Entwicklungen weiterhin verfolgen sollten.



To-Do für Unternehmen:

Die KI-Verordnung sollte unbedingt in der Design- und Entwicklungsphase einer KI bereits berücksichtigt werden. Viele der Pflichten lassen sich im Nachhinein kaum erfüllen. Bestimmen Sie direkt zu Beginn den Zweck der KI. Prüfen Sie anschließend, in welche Risikoklasse die KI fällt.

Nur so lässt sich feststellen, welche rechtlichen Anforderungen gelten und ob der Einsatz beim Kunden überhaupt zulässig ist. So lassen sich Nutzungsverbote oder Verzögerungen in der Produktentwicklung vermeiden. Stellen Sie sicher, dass die Trainingsdaten den Anforderungen der KI-Verordnung (Relevanz, Fehlerfreiheit, Vollständigkeit) und des Datenschutzes genügen.



3. Aufbruch von Datenmonopolen: Der Data Act

Neues Herzstück der europäischen Datenstrategie ist der Data Act (DA) - und er bringt Bewegung in die Art und Weise, wie Unternehmen mit Daten umgehen. Seit dem 12. September 2025 gilt der DA in allen EU-Mitgliedstaaten und verpflichtet Hersteller und Anbieter vernetzter Produkte oder verbundener Dienste – etwa Smart-Home-Geräte, Maschinen oder Fahrzeuge – dazu, die bei der Nutzung entstehenden Daten den Nutzern zugänglich zu machen.

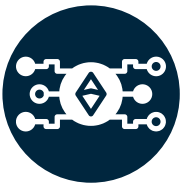
Besonders spannend: Der DA umfasst sowohl personenbezogene als auch nicht-personenbezogene Daten und reicht damit deutlich weiter als die DSGVO.

Für Unternehmen bedeutet das mehr Transparenz, neue Pflichten, aber auch echte Chancen, denn der Data Act soll den fairen Zugang zu Daten fördern, Datenmonopole aufbrechen und Innovationen erleichtern. So können beispielsweise Geschäftspartner einfacher Daten austauschen oder Kunden problemlos den Cloud-Anbieter wechseln.



Wer muss Daten teilen?

Sobald ein Produkt mit digitalen Funktionen vernetzt ist, greifen die Vorgaben des Data Acts. Beispiele reichen von Industrieanlagen und Fahrzeugen bis hin zu Haushaltsgeräten oder smarten Wearables. Auch Unternehmen, die physische Produkte mit digitalen Funktionen anbieten, sind betroffen, sobald diese Produkte vernetzt sind.



Aber wann gilt mein Produkt als vernetzt?

Vernetzte Produkte (IoT-Produkte) sind physische Produkte, die in der Regel mit Sensoren ausgestattet sind und während ihrer Nutzung Daten erfassen – etwa über ihren Zustand, ihr Verhalten oder ihre Umgebung – und diese Informationen über eine digitale Schnittstelle übermitteln können. Entscheidend ist dabei nicht nur die Datenerfassung, sondern auch die digitale Nutzbarkeit der Daten, etwa über WLAN, Bluetooth, Mobilfunk oder andere Übertragungswege.

Ergänzt werden vernetzte Produkte häufig durch verbundene Dienste. Das sind digitale Anwendungen, die mit dem Produkt interagieren, wie beispielsweise eine App, mit der sich Funktionen steuern lassen, oder ein Cloud-Dienst, der Maschinendaten auswertet.

Der DA greift also, wenn ein Produkt nicht nur „smart“ ist, sondern auch Daten sendet, empfängt oder mit digitalen Diensten gekoppelt ist.



To-Do für Unternehmen:

Identifizieren Sie Ihre vernetzten Produkte, die unter den Data Act fallen, um klären zu können, inwieweit die Produkte an die Vorgaben aus dem Data Act ausgerichtet werden müssen.



Data Access by Design

Vernetzte Produkte erzeugen laufend Daten. Bisher war oft unklar, wer eigentlich über diese Daten verfügen darf. Der Data Act schafft hier nun Klarheit: Nicht nur der Hersteller, sondern auch Nutzer haben ein Recht auf Zugang zu den durch die Nutzung entstehenden Daten. Der Zugang muss einfach, verständlich und ohne künstliche Hürden erfolgen. Nutzer dürfen die Daten zudem an Dritte weitergeben oder selbst weiterverwenden. Hersteller müssen entsprechende technische Möglichkeiten schaffen. Überhöhte Gebühren oder technische Sperren sind nicht zulässig.

Mit dem Data Act wird die Zugänglichkeit von Daten deshalb zu einer Anforderung an das Produktdesign. Das Prinzip „Data Access by Design“ verlangt, dass vernetzte Produkte technisch so konstruiert werden, dass Nutzer direkt – also ohne Umweg über den Hersteller – auf die generierten Daten zugreifen können. Für die Entwicklung bedeutet dies, dass Schnittstellen für den Echtzeit-Zugriff (On-Device oder via API) sowie standardisierte, maschinenlesbare Datenformate bereits im Entwicklungsstadium vorgesehen werden müssen. Da diese Pflicht zum direkten Zugang für alle ab dem 12. September 2026 neu eingeführten Produkte greift, sind entsprechende Hardware- und Software-Spezifikationen frühzeitig festzulegen, um spätere Hürden beim Markteintritt zu vermeiden.



Weniger ist manchmal mehr: Steuerung der Compliance-Last durch Datenverzicht

Vor dem Hintergrund dieser – weit in die Produktgestaltung hineingehenden – Pflichten sollte im Entwicklungsprozess auch darüber nachgedacht werden, welche Daten überhaupt von dem Gerät erzeugt bzw. erhoben werden. Schließlich bietet die Design-/Entwicklungsphase insoweit eine oft übersehene Möglichkeit zur Steuerung der Compliance-Last: den bewussten Verzicht auf die Datenerhebung. Der Data Act verpflichtet Hersteller nämlich nicht dazu, so viele Daten wie möglich zu sammeln; er regelt lediglich den Zugang zu jenen Daten, die tatsächlich generiert werden. Entscheidet sich das Entwicklungsteam dazu, bestimmte Daten gar nicht erst zu erfassen oder Prozessdaten nicht dauerhaft zu speichern, entfällt für diese Daten die Bereitstellungspflicht.



To-Do für Unternehmen:

Stellen Sie Data-Act-konforme Datenzugangsmöglichkeiten bereit. Prüfen Sie vor dem Hintergrund der Bereitstellungspflichten aus dem Data Act, welche Daten von Ihrem Produkt tatsächlich erzeugt werden müssen. Prüfen Sie, inwieweit Sie den Datenzugang verweigern dürfen und welche Gestaltungsmöglichkeiten es gibt.

4. Der Data Governance Act: Fundament einer europäischen Datenwirtschaft

Europa schafft einen Binnenmarkt für Daten

Mit dem Hauptziel vor Augen, Innovation und Wettbewerbsfähigkeit zu fördern, bildet der Data Governance Act (**DGA**) eine zentrale Säule der europäischen Datenstrategie. Ziel ist es, die Wertschöpfung aus Daten zu fördern, indem klare rechtliche Rahmenbedingungen für Datennutzung und -austausch geschaffen werden. Der DGA richtet sich primär an öffentliche Stellen, Datenvermittlungsdienste und datenaltruistische Organisationen. In strategisch wichtigen Bereichen wie Gesundheit, Umwelt, Energie, Mobilität etc. soll ein gemeinsamer europäischer Datenraum geschaffen und sektorübergreifender, freiwilliger Datenaustausch ermöglicht werden. Der DGA unterstützt dieses Vorhaben durch das Vorantreiben vertrauenswürdiger Datenaustauschsysteme.

Neue Chancen als Datenintermediär – der frühe Vogel fängt die Daten

Der Markt für Datenvermittlungsdienste, auch bekannt als Datenintermediäre, steckt noch in den Kinderschuhen – hier gibt es bisher nur wenige registrierte Anbieter. Unternehmen, die diese Rolle übernehmen wollen, müssen sich aktuell vor Aufnahme der Tätigkeit bei der zuständigen Behörde anmelden – in Deutschland ist das die Bundesnetzagentur.

Die Prüfung ist zunächst eher formal: Stimmt alles mit der Anmeldung, darf der Anbieter das Label „in der Union anerkannter Anbieter von Datenvermittlungsdiensten“ sowie das offizielle Logo der EU-Kommission führen. Die Kommission selbst führt zudem ein zentrales Register aller anerkannten Datenintermediäre.

Vor dem Hintergrund des Vorschlags des Digitalen Omnibus steht derzeit im Raum, ob die verpflichtende Registrierung und das EU-Label für Datenintermediäre künftig entfallen. Die Markteintrittshürden würden dadurch deutlich sinken, sodass entsprechende Geschäftsmodelle schneller und mit weniger bürokratischem Aufwand verfolgt werden könnten. Es bleibt abzuwarten, ob die Vorschläge des Digitalen Omnibus tatsächlich umgesetzt werden.

Der aktuelle Vorschlag des Digitalen Omnibus sieht zudem vor, dass der DGA sowie andere Rechtsakte, die nicht-personenbezogene Daten betreffen, künftig in den Data Act integriert werden sollen, um ein einheitliches Regelwerk zu schaffen. Dies dürfte die Auffindbarkeit relevanter Regelungen künftig erleichtern.



To-Do für Unternehmen:

Wenn Ihr Unternehmen als Datenintermediär tätig werden möchte, muss gegenwärtig eine Anmeldung bei der Bundesnetzagentur erfolgen. Um sich erfolgreich anzumelden, müssen die EU-Anforderungen für die Zulassung sichergestellt werden. Plattformen und Prozesse müssen den sicheren und regelkonformen Datenaustausch ermöglichen. Es ist allerdings empfehlenswert die Entwicklungen rund um die Vorschläge des Digitalen Omnibus zu verfolgen, da die Markteintrittshürden deutlich sinken könnten.



Phase 2: Vertrieb & Vertragsgestaltung

Data Act: Neue Informationspflichten, Datenlizenzen und Cloud-Switching-Regelungen

Mit dem Data Act ändern sich die Spielregeln für den Vertrieb vernetzter Produkte grundlegend. Die gängige Praxis, Datenrechte pauschal über das Kleingedruckte zu vereinnahmen, wird durch strikte vorvertragliche Transparenzpflichten und eine Pflicht zur Regelung von Datenlizenzen abgelöst. Zudem enthält der Data Act Vorgaben zu Exit-Regelungen bei Clouddiensten.

Die neue Transparenzpflicht vor Vertragsschluss

Noch bevor ein Kunde (ob B2B oder B2C) einen Vertrag für ein vernetztes Produkt unterzeichnet, muss der Anbieter konkret darüber informieren, welche Datenarten generiert werden, in welchem Format und Umfang diese anfallen und wie der Nutzer darauf zugreifen kann. Fehlen diese Angaben oder sind sie unpräzise („wir erheben alle relevanten Daten“), drohen nicht nur Bußgelder, sondern auch vertragsrechtliche Risiken und Wettbewerbsverstöße. Der Vertrieb muss folglich mit präzisen Datenblättern ausgestattet werden, die Teil der Vertragsunterlagen werden.

Datenhoheit und Lizenzierung

Wie bereits angedeutet, führt der Data Act zu einem Paradigmenwechsel: Der Hersteller gilt nicht automatisch als Eigentümer der Maschinendaten. Vielmehr stellt der Data Act klar: Der Hersteller (Dateninhaber) darf nicht-personenbezogene Daten primär nur nutzen, um den vertraglich vereinbarten Dienst zu erbringen. Möchte der Hersteller diese Daten für eigene Zwecke nutzen – etwa zur Produktverbesserung, für Analysen oder den Verkauf neuer Services – benötigt er eine explizite vertragliche Erlaubnis des Nutzers (eine Datenlizenz). Die Vertragsgestaltung erfordert in diesen Fällen dann die Aufnahme eines Lizenzvertrags, in dem sich der Hersteller Nutzungsrechte vom Kunden einräumen lassen muss. Dabei macht der Data Act strenge Vorgaben dazu, welche Regelungen in diesem Zusammenhang missbräuchlich sind und nicht verwendet werden dürfen.

Gefährlich transparent: Schutz von Betriebsgeheimnissen

Daten von Maschinen, Fahrzeugen oder vernetzten Systemen enthalten oft mehr als nur technische Fakten. Häufig stecken darin wertvolle Geschäftsgeheimnisse, etwa Leistungskennzahlen, Performance-Daten oder Informationen, die Rückschlüsse auf den betriebsinternen Ablauf erlauben. Der Data Act erkennt dieses Risiko und sieht Schutzmechanismen vor.

Unternehmen sind nicht verpflichtet, Daten herauszugeben, wenn dadurch Geschäftsgeheimnisse gefährdet würden. Der Zugriff kann in solchen Fällen verweigert oder eingeschränkt werden. Um das sicherzustellen, braucht es klare Schutzmaßnahmen wie Berechtigungskonzepte, verschlüsselte Zugänge oder Vertraulichkeitsvereinbarungen. Wer Daten freigibt, sollte genau wissen, welche Informationen besonders schutzwürdig sind und wie sie geschützt werden.



To-Do für Unternehmen:

- **Identifikation von schutzbedürftigen Daten:** Sensible Daten identifizieren & definieren. Prüfen, ob Herausgabe eingeschränkt werden kann. Schutzmaßnahmen etablieren.
- **Update der Vertragsunterlagen:** Standardisierte Datenblätter zur Erfüllung der Transparenzpflichten für jedes vernetzte Produkt erstellen.
- **Anpassung der AGB:** Revision der Datennutzungsklauseln. Pauschale Rechteeinräumungen sind durch spezifische Lizenzvereinbarungen zu ersetzen.

Neues Vertragsrecht für Cloud Service Provider

Ausdrücklich vom Data Act erfasst werden außerdem auch Anbieter von Cloud-Services (z.B. SaaS, PaaS, IaaS etc.). Dies hat echte Auswirkungen auf den europäischen Datenmarkt. Ziel der EU ist es, den Wechsel zwischen Anbietern von Cloud-Services zu erleichtern, neue Anbieter besser in den Markt zu bringen und nach und nach Wechselentgelte wie bspw. Datenübertragungskosten abzuschaffen.

Dies bedeutet in der Praxis mehr als nur neue Vorschriften:

- neue **Datenzugangsrechte**
- eigenständige **Vertragsregeln für den Exit** des Kunden sowie
- erweiterte **Informations- und Dokumentationspflichten** müssen umgesetzt werden.

Spannend ist, dass der aktuelle Vorschlag für den **Digitalen Omnibus** einige Ausnahmen vorsieht und Anbieter dadurch entlasten könnte:

So sollen die Wechselpflichten für KMU und Kleinunternehmen nur gelten, soweit diese in ihrer Rolle als Anbieter technisch umsetzen können und ihnen dies auch wirtschaftlich zumutbar ist. Individuell entwickelte Cloud-Services, die ausschließlich für einen Kunden bereitgestellt werden, sollen nicht den Wechselpflichten unterliegen. Zudem soll klargestellt werden, dass Anbieter keine neuen proprietären Schnittstellen entwickeln müssen, sodass Aufwand und Kosten für die Einhaltung des Data Act reduziert werden könnten.



To-Do für Unternehmen:

Anbieter von Cloud-Services sollten prüfen, welche Auswirkungen der Data Act auf sie hat. Ist der Data Act anwendbar, sollten Anbieter insbesondere entsprechende Prozesse zur Umsetzung des Exit-Managements und der Informations- und Dokumentationspflichten vorsehen. Daneben sollten entsprechende Vertragsunterlagen (insb. Kundenverträge) dahingehend geprüft werden, ob diese mit dem Data Act vereinbar sind und im Bedarfsfall angepasst werden.

Phase 3: Laufender Betrieb

Digitale Produkte erfordern auch nach dem Verkauf eine aktive Betreuung. Hersteller tragen die Verantwortung, ihre Systeme **über den gesamten Lebenszyklus** hinweg sicher zu halten. Das bedeutet: Sicherheitsupdates bereitstellen, Supportzeiträume klar kommunizieren und Update-Prozesse rechtlich absichern.

1. KI-Verordnung: Pflichten nach der Inbetriebnahme

Integration von fremden KI-Lösungen in eigene Produkte

Wer KI-Systeme in seinen Produkten oder Services einsetzt, kann die Verantwortung nicht einfach an den ursprünglichen Entwickler der KI-Lösung weiterreichen. Anbieter solcher integrierter KI-Lösungen tragen nach der KI-Verordnung die volle Verantwortung dafür, wie die integrierten KI-Systeme handeln, lernen und mit Kunden interagieren.

Ein Beispiel: Wenn ein Online-Händler einen Chatbot integriert, um Kundenanfragen zu beantworten, ist nicht der Entwickler der Betreiber, sondern der Händler selbst. Die KI ist das Werkzeug, aber die Verantwortung bleibt beim Menschen (oder genauer gesagt: beim Unternehmen).



To-Do für Unternehmen:

Wer KI in seinem Betrieb integriert, sollte nicht nur über Datensätze und Modelle nachdenken, sondern auch über Haftung, Transparenz und Governance. Auch fremdeingekaufte Systeme müssen nach der KI-Verordnung klassifiziert werden. Viele Anwendungen lassen sich nicht auf den ersten Blick eindeutig einer Risikostufe zuordnen. Unternehmen sind müssen sicherstellen, dass auch eingekaufte KI-Systeme rechtmäßig genutzt werden.

Beobachten, Melden, Verantwortung übernehmen – zusätzliche Pflichten von Anbietern von Hochrisiko-KI

Wer Hochrisiko-KI-Systeme anbietet, bei dem ist künftig nicht nur technologische, sondern auch rechtliche Intelligenz gefragt. Die KI-Verordnung verlangt, dass Anbieter ihre Systeme über die gesamte Lebensdauer im Blick behalten, indem sie Leistungsdaten sammeln, Auswertungen durchführen und alles sauber in der technischen Dokumentation festhalten.

Kommt es doch einmal zu einem Problem, greift die Meldepflicht für „schwerwiegende Vorfälle“. Ob Fehlentscheidungen, Sicherheitslücken oder unerwartete Risiken – je nach Schweregrad müssen diese innerhalb von 2, 10 oder 15 Tagen gemeldet werden.

2. Digital Services Act: Schutz für Nutzer und Chancen für Unternehmen

Der Digital Services Act (**DSA**) zielt darauf ab, Nutzer sowie ihre Grundrechte im Internet zu schützen. Dabei ist der DSA sowohl für den B2B- als auch für den B2C-Bereich relevant. Im Fokus stehen insbesondere die Bekämpfung illegaler Inhalte, schädlicher Online-Aktivitäten und der Verbreitung von Desinformation.

Gleichzeitig schafft der DSA Chancen für Unternehmen: Er fördert Innovation, Wachstum und Wettbewerbsfähigkeit und erleichtert die Expansion kleinerer Plattformen, von KMU und Start-ups. So entsteht ein ausgewogenes Gleichgewicht zwischen Schutz der Nutzer und offenen Märkten für digitale Geschäftsmodelle.

Noch Hostingdienst oder schon Online-Plattform?

„Endlich greift die EU gegen die großen Plattformen durch!“ – Der DSA wird in der öffentlichen Diskussion häufig als Gesetz für Tech-Giganten dargestellt. Doch das greift zu kurz. Zwar gelten für sehr große Online-Plattformen besonders strenge Vorgaben, doch der DSA betrifft nicht nur die „Großen“, sondern grundsätzlich alle Vermittlungsdienste, die Nutzern den Zugang zu Inhalten ermöglichen oder selbst Inhalte speichern. Und das unabhängig von Größe, Reichweite oder Nutzerzahl.

Leicht übersieht man also die eigenen Compliance-Verpflichtungen. Inmitten der verschiedenen Kategorien wie Hosting-Dienst, Online-Plattform oder Caching-Service sind Unternehmen gut beraten, frühzeitig zu prüfen, welche Rolle sie einnehmen und welche konkreten Verpflichtungen sich daraus ergeben.



To-Do für Unternehmen:

Prüfen Sie, ob und in welche Kategorie Ihr Dienst unter den DSA fällt (z.B. Hosting, Online-Plattform) und beachten Sie die daraus folgenden Verpflichtungen.

Was offline illegal ist, bleibt auch online illegal

Ausgehend von diesem Grundsatz verpflichtet der DSA Plattformen, illegale Inhalte aktiv zu entfernen und das Risiko zu minimieren, dass solche Inhalte überhaupt auf die Plattform gelangen. Um illegale Inhalte schnell und effizient zu entfernen, müssen Online-Plattformen und andere Vermittlungsdienste Melde- und Abhilfeverfahren vorhalten, die bestimmte Anforderungen erfüllen.

Der DSA selbst legt jedoch nicht fest, was genau illegal ist. Stattdessen schafft er einen EU-weiten Rahmen für die Aufdeckung, Kennzeichnung und Entfernung illegaler Inhalte sowie für Risikobewertungspflichten von Plattformen. Die konkrete Definition illegaler Inhalte erfolgt in anderen EU- oder nationalen Gesetzen.

✓ To-Do für Unternehmen:

Schaffen Sie entsprechende Meldewege und Abhilfeverfahren für rechtswidrige Inhalte, wenn Sie dazu nach dem DSA verpflichtet sind. Werden Sie sich darüber klar, wann nutzergenerierten Inhalte zu entfernen sind und schaffen Sie klare Prozesse, um illegale Inhalte konsequent von Ihren Diensten auszuschließen. Andernfalls drohen Haftungsrisiken.

3. Cyber Resilience Act: Cybersicherheit über den ganzen Produktlebenszyklus

Verantwortung endet nicht mit Verkauf

Cybersicherheit ist keine einmalige Maßnahme, sondern eine dauerhafte Verpflichtung. Hersteller müssen ihre Produkte auch nach dem Inverkehrbringen regelmäßig mit kostenlosen Sicherheitsupdates versorgen und klar kommunizieren, wie lange ein Produkt aktiv unterstützt wird. Gerade für mittelständische Unternehmen, die Maschinen und Systeme mit langen Produktlebenszyklen herstellen, stellen die neuen Vorgaben des CRA eine besondere Herausforderung dar.

Der Support-Zeitraum ist dabei kein starrer Wert, sondern orientiert sich an mehreren Faktoren:

- den **Erwartungen** der Nutzer,
- der **Art des Produkts** mit digitalen Elementen,
- sowie an **rechtlichen** Vorgaben, die die **Lebensdauer des Produkts beeinflussen**.

Grundsätzlich gilt ein Mindest-Support-Zeitraum von fünf Jahren. Eine Ausnahme bilden Produkte, deren tatsächliche Lebensdauer kürzer ist, beispielsweise temporär genutzte Apps.

Diese Pflicht dient nicht nur dem Schutz vor veralteten, unsicheren Systemen. Sie erhöht die Transparenz gegenüber Kunden und Partnern und schafft Rechtssicherheit, indem Verantwortlichkeiten klar geregelt werden. Wer hier frühzeitig Prozesse etabliert, kann Risiken langfristig reduzieren.

✓ To-Do für Unternehmen:

Auch nach dem Verkauf bleibt der Hersteller verantwortlich. Planen Sie Update-Prozesse und Supportzeiten vertraglich ein. Informieren Sie Kunden klar über Supportdauer und Sicherheitsmaßnahmen. Schaffen Sie interne Strukturen für regelmäßige Sicherheitsaktualisierungen.



Phase 4: Haftung & Exit

Über manche Themen macht man sich nur ungern Gedanken. Dazu gehört die Haftung genauso wie das, was am möglichen Ende eines Vertragsverhältnisses zu tun ist. Aber auch diese Themen sollten von Anfang an mitgedacht werden, um Nachteile zu vermeiden und Risiken zu reduzieren.

1. Cyber Resilience Act: Neue Haftungsregeln bei Produkten mit digitalen Elementen

Updates verlängern Ihre Verantwortung

Updates sind längst Teil des Geschäftsmodells vieler Unternehmen. Sie verbessern Funktionen, schließen Sicherheitslücken oder erweitern den Leistungsumfang.

Wer jedoch auch nach der Inbetriebnahme Kontrolle über das Produkt behält – etwa durch Fernzugriff, Software-Updates oder smarte Funktionen – trägt weiterhin Verantwortung. Kommt es durch ein fehlerhaftes Update oder mangelnde Cybersicherheit zu einem Schaden, bleibt das Unternehmen haftbar.

✓ To-Do für Unternehmen:

Hersteller sind daher gut beraten, ihre Update-Prozesse rechtlich und technisch sorgfältig abzusichern und lückenlos zu dokumentieren.

Fehler über Fehler – wenn Produkte selbst lernen

Der Begriff der Fehlerhaftigkeit wird erweitert. Auch KI-Systeme und Produkte, die nach dem Verkauf selbstständig lernen oder neue Funktionen entwickeln, können später als fehlerhaft gelten.

Zeigt ein Produkt durch ein Update, eine erlernte Funktion oder geänderte Einsatzbedingungen ein unerwartet gefährliches Verhalten, haftet der Hersteller. Maßgeblich ist der Zeitpunkt, zu dem das Produkt die Kontrolle des Herstellers verlässt.

✓ To-Do für Unternehmen:

Unternehmen müssen künftig nachvollziehbar dokumentieren, wie das Produkt zu diesem Zeitpunkt abgesichert war.

Neue Beweisregeln erhöhen die Anforderungen für Hersteller

Die Beweisführung in Produkthaftungsfällen wird für Geschädigte erleichtert. Künftig müssen sie lediglich plausible Tatsachen und Beweismittel vorlegen, die einen Schadensersatzanspruch stützen.

Für Unternehmen bringt das erweiterte Offenlegungspflichten mit sich, die dem deutschen Zivilprozessrecht bislang fremd waren. Auch wenn Vorschriften zum Schutz von Geschäftsgeheimnissen gelten, bestehen Bedenken, dass sensible Informationen wie Quellcodes oder KI-Algorithmen nicht ausreichend geschützt sind.

Die Hürden zur Offenlegung sind niedrig. Das kann insbesondere für technologiegetriebene KMU eine erhebliche Belastung darstellen.



To-Do für Unternehmen:

Unternehmen sollten frühzeitig prüfen, welche Daten besonders schutzwürdig sind, und entsprechende Sicherungsstrategien entwickeln.

2. Produkthaftungsrichtlinie – Haftung entlang der gesamten Lieferkette

40 Jahre später: Die EU macht Produkthaftung digital

Nach rund 40 Jahren hat die EU die Produkthaftungsregeln grundlegend modernisiert. Die bisherigen Vorschriften stammen aus einer Zeit, in der Digitalisierung, KI und vernetzte Systeme noch keine Rolle spielten. Heute prägen sie den Markt.

Neben klassischen physischen Produkten wie Maschinen oder Geräten fallen nun auch Software und KI-basierte Systeme ausdrücklich unter die Produkthaftung. Unternehmen haften künftig nicht nur für Produktionsfehler, sondern auch für unzureichende Sicherheitsupdates, mangelnden Cyberschutz und digitale Fehlfunktionen.

Neu ist außerdem, dass auch Schäden durch Datenverlust oder Datenverfälschung erfasst werden. Damit stellt die EU klar: Haftung endet nicht beim Produktgehäuse, sondern umfasst den gesamten digitalen Lebenszyklus.

Haftungskette statt Lieferkette – wer zahlt am Ende?

Die Produkthaftung wird auf mehrere Akteure verteilt. Ziel ist es, der geschädigten Personen einen Anspruch gegen mindestens einen in der EU ansässigen Akteur zu sichern.

Neben Herstellern können auch Akteure, die wesentliche Veränderungen an den Produkten vornehmen in die Verantwortung genommen werden, genauso wie Zulieferer, Importeure, Fulfillment-Dienstleister und Online-Plattformen.



To-Do für Unternehmen:

Für Unternehmen bedeutet das: Es reicht nicht mehr, den Hersteller zu kennen oder zu kontrollieren. Unternehmen sind beraten, Haftungsrisiken entlang der gesamten Lieferkette zu identifizieren, sich vertraglich abzusichern und laufend zu überprüfen.

3. Data Act: Das Ende des Vendor Lock-in – Datenfreiheit statt künstlicher Hürden

Ob Musik-Playlist, Fitnessdaten oder Maschinenauswertungen – was wir heute digital erzeugen, soll nicht an einen Anbieter gebunden sein. Nutzer sollen ihre Daten künftig einfach exportieren und weiterverwenden können, unabhängig vom Anbieter.

Für Unternehmen bedeutet das: Technische oder vertragliche Hürden, die den Datenexport behindern, sind unzulässig. Das gilt insbesondere beim Wechsel des Cloud-Anbieters, bei neuen Partnern oder bei der Integration anderer Systeme.

Was einfach klingt, wirft in der Praxis viele Fragen auf:



Welche Daten sind exportfähig?



In welchem Format müssen sie bereitgestellt werden?



Und wie stellen Sie sicher, dass alle Datenschutz- und Sicherheitsvorgaben eingehalten werden?



To-Do für Unternehmen:

Anbieter sollten ihre eigenen Systeme frühzeitig prüfen. Prüfen Sie, welche Daten exportfähig sind und schaffen Sie technische Exportfunktionen, wo notwendig. Stellen Sie sicher, dass Datenschutz- und Sicherheitsvorgaben eingehalten werden.

Es lohnt sich, genauer hinzuschauen, ob die eigenen Systeme und Prozesse für den Datenexport schon bereit sind oder ob es noch Nachholbedarf gibt.

Kontakt



Dr. André Schmidt
Partner

Fachanwalt für IT-Recht

✉ schmidt@lutzabel.com

☎ +49 40 3006996-7765

[LinkedIn](#)



Angelika Szalek
Senior Associate

IAPP CIPP/E (Certified
Information Privacy
Professional / Europe)

✉ szalek@lutzabel.com

☎ +49 40 3006996-7807

[LinkedIn](#)



Niklas Vogt
Senior Associate

Fachanwalt für IT-Recht

✉ vogt@lutzabel.com

☎ +49 40 3006996-7876

[LinkedIn](#)



Dr. Philipp Knitter
Associate

✉ knitter@lutzabel.com

☎ +49 40 3006996-7903

[LinkedIn](#)