IP / IT / Datenrecht

Digital, Data & Cyber

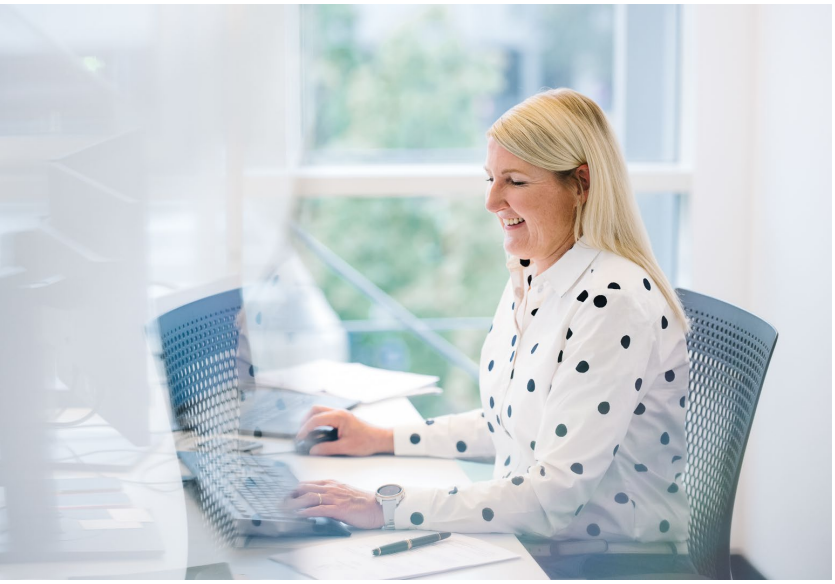
Überblick der aktuellen Digital- & Cyber-gesetzgebung (Artificial Intelligence Act, KI-Haftungs-Richtlinie, NIS2-Richtlinie, Cyber Resilience Act)

Es tut sich etwas im Bereich der **Digital- & Cybergesetzgebung** – mit weitreichender Relevanz für viele Unternehmen. Neue gesetzliche Vorschriften, beispielsweise zur Regulierung digitaler Dienste, zur Bereitstellung und Nutzung von Daten oder zur Verwendung künstlicher Intelligenz, befinden sich aktuell im Gesetzgebungsverfahren oder sind bereits verabschiedet bzw. in Kraft getreten.

Die relevanten gesetzlichen Vorschriften haben insgesamt einen **sehr weiten Anwendungsbereich**, sodass es kaum ein Unternehmen geben dürfte, das von keinem der neuen Gesetzgebungsvorhaben betroffen sein wird. Aus diesem Grund ist es für Unternehmen heute von wesentlicher Relevanz, einen Überblick über die für sie möglicherweise geltenden Rechtsvorschriften zu behalten.

Um Ihnen diesen **Überblick** zu erleichtern, stellen wir Ihnen nachfolgend die **wichtigsten Vorhaben im Bereich der Digital- & Cybergesetzgebung** dar.

OrthKluth



Dabei legen wir den Fokus auf die folgenden Aspekte:

- Was regelt das Gesetz im Wesentlichen?
- Wer wird durch das Gesetz verpflichtet?
- Wie ist der aktuelle Stand des Gesetzgebungsverfahrens?

Artificial Intelligence Act & KI-Haftungs-Richtlinie

Der **EU Artificial Intelligence Act** (**AI Act** – zu Deutsch: Gesetz über künstliche Intelligenz) und die EU-Richtlinie zur Anpassung von Vorschriften über außervertragliche zivilrechtliche Haftung an künstlicher Intelligenz (**KI-Haftungs-RL**) sind zwei EU-Gesetzgebungsvorhaben, die aktuell auf EU-Ebene verhandelt werden. Beide Rechtsvorschriften sind bislang nicht verabschiedet und daher noch nicht verbindlich.

Als EU-Verordnung wird der AI Act zukünftig unmittelbare Wirkung in allen EU-Mitgliedstaaten erlangen; die KI-Haftungs-RL wird dementgegen noch in nationales Recht umgesetzt werden müssen.

Zentrales Ziel beider Gesetze ist die **Regulierung des Einsatzes künstlicher Intelligenz**, insbesondere im Hinblick auf deren Sicherheit und die Zurechenbarkeit mittels KI getroffener Entscheidungen.

Zur Erreichung dieses Ziels statuiert der AI Act insbesondere **Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen** in der EU, **Verbote bestimmter Praktiken** im Bereich der künstlichen Intelligenz, besondere Anforderungen an Hochrisiko-KI-Systeme und **Transparenzvorschriften** für bestimmte KI-Systeme.

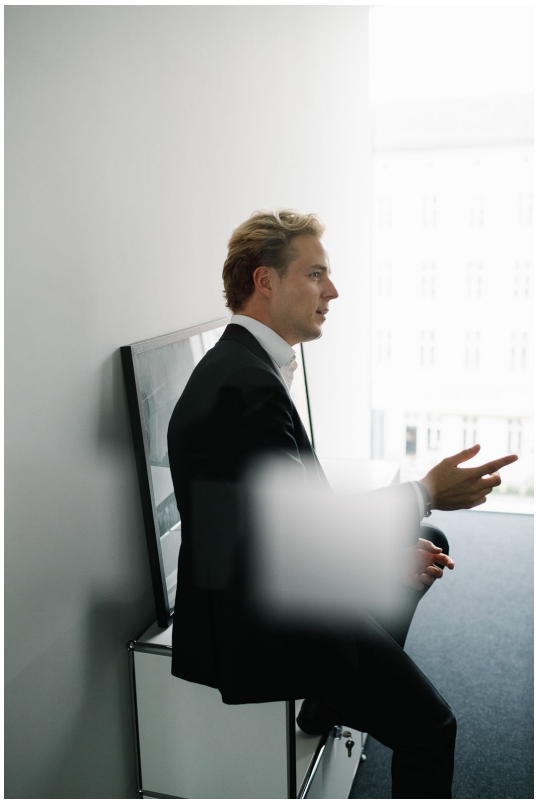
Sowohl der AI Act als auch die KI-Haftungs-RL **verpflichten Anbieter**, die KI-Systeme in der EU in Verkehr bringen oder in Betrieb nehmen (unabhängig davon, ob diese Anbieter in der EU oder in einem Drittland niedergelassen sind) **sowie die Nutzer von KI-Systemen**.

Der AI Act nimmt daneben auch Anbieter sowie Nutzer von KI-Systemen, die in einem Drittland niedergelassen oder ansässig sind, in die Pflicht, wenn die von einem KI-System hervorgebrachten Ergebnisse in der EU verwendet werden.

Der AI Act verpflichtet Anbieter von KI-Systemen u.a. zur **Gewährleistung einer Transparenz von KI-Systemen**, die für die Interaktion mit natürlichen Personen bestimmt sind; diese müssen so konzipiert und entwickelt werden, dass natürlichen Personen mitgeteilt wird, dass sie es mit einem KI-System zu tun haben. Nutzer von KI-Systemen, die **sog. Deepfakes** ermöglichen, müssen offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden.

Besonders weitgehende Pflichten statuiert der AI Act in Bezug auf **sog. Hochrisiko-KI-Systeme**, die unter bestimmte Harmonisierungsrechtsvorschriften der EU fallen (z.B. Richtlinie über die Sicherheit von Spielzeug, Medizinprodukteverordnung) oder **in bestimmten Bereichen bzw. zu bestimmten Verwendungszwecken eingesetzt werden** sollen (z.B. zur biometrischen Identifizierung natürlicher Personen oder im Bereich des Personalmanagements).

Die KI-Haftungs-RL enthält Vorschriften bezüglich der **zivilrechtlichen Haftung für das Verhalten von KI-Systemen**. Die besonderen Merkmale von KI-Systemen, insbesondere deren Komplexität und Undurchsichtigkeit (der sog. „Blackbox"-Effekt), können die Ermittlung der haftbaren Person und die Erfüllung der Voraussetzungen einer erfolgreichen Haftungsklage für betroffene Personen erheblich erschweren oder gar unmöglich machen.



Diese Probleme versucht die KI-Haftungs-RL zu beseitigen, indem sie insbesondere Vorschriften statuiert über

- die **Offenlegung von Beweismitteln** betreffend Hochrisiko-KI-Systeme mit dem Ziel, es einem Kläger zu ermöglichen, einen außervertraglichen verschuldensabhängigen zivilrechtlichen Schadensersatzanspruch zu begründen, und
- die **Beweislast bei der Geltendmachung außervertraglicher verschuldensabhängiger zivilrechtlicher Ansprüche** vor nationalen Gerichten in Bezug auf Schäden, die durch ein KI-System verursacht wurden.

Im Kern statuiert die KI-Haftungs-RL eine **Art „Gefährdungshaftung"** für Anbieter von KI-Systemen, die mit der Haftung von Haltern eines Kraftfahrzeugs in Teilen vergleichbar ist. Aus den Vorschriften der KI-Haftungs-RL resultiert unter bestimmten Voraussetzungen eine widerlegbare Vermutung eines ursächlichen Zusammenhangs zwischen dem Verschulden eines beklagten KI-Anbieters und dem vom KI-System hervorgebrachten Ergebnis.

Dies hat zur **Folge, dass es ggfs. den Anbietern bzw. Betreibern von KI-Systemen obliegt, die gesetzliche Vermutung zu widerlegen**. Sie müssen ggfs. darlegen und beweisen, dass ein eingetretener Schaden nicht kausal durch ihr KI-System verursacht wurde. Dies wird den betroffenen Stellen regelmäßig nur möglich sein, wenn sie geeignete Vorsorgemaßnahmen ergreifen.

Die Nichteinhaltung bestimmter Vorschriften des AI Acts soll mit Geldbußen in Höhe von 30 Mio. EUR bzw. 6 Prozent des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres sanktioniert werden können.

IT-Sicherheit für KRITIS (NIS2-Richtlinie)

Am 16. Januar 2023 ist die sog. NIS2-Richtlinie in Kraft getreten.[1] Die EU-Mitgliedstaaten müssen die **NIS2-Richtlinie bis zum 17. Oktober 2024 in nationales Recht umsetzen**.

Die NIS2-Richtlinie reformiert insbesondere die bisher gültigen Vorschriften zum **Schutz der Cybersicherheit sog. Kritischer Infrastrukturen (KRITIS)** sowie die Pflichten diesbezüglicher Betreiber.

Zentrales Ziel der NIS2-Richtlinie ist die Steigerung des allgemeinen Cybersicherheitsniveaus in der EU. Damit adressiert die NIS2-Richtlinie eines der aktuell wesentlichsten Bedrohungsszenarien für Unternehmen aus allen Bereichen.

Zur Erreichung dieses Ziels wird insbesondere der **Umfang der verpflichteten Stellen auf neue Sektoren und Einrichtungen erweitert**; insoweit besteht eine Parallelität zur EU-Richtlinie 2022/2557 über die Resilienz kritischer Einrichtungen. Zu den neu verpflichteten Sektoren gehören u.a. folgende Einrichtungen und zugehörige Anlagen:

- Fernwärme/-kälte,
- Wasserstoff,
- Abwasser,
- Cloud-Computing- und Rechenzentrumsdienste,
- öffentliche elektronische Kommunikationsnetze (TK-Netze),
- öffentlich zugängliche elektronische Kommunikationsdienste (TK-Dienste),
- Weltraum,
- Öffentliche Verwaltung.

Verpflichtete Stellen müssen insbesondere **Risikomanagementmaßnahmen im Bereich der Cybersicherheit** ergreifen, um Cyberangriffe frühzeitig erkennen und abwehren zu können bzw. die Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Dabei sieht die NIS2-Richtlinie ausdrücklich **Überwachungspflichten der Leitungsorgane** vor mit der Folge, dass Leitungsorgane u.U. für Verstöße verantwortlich gemacht werden können.

[1] 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

Zur Verbesserung der allgemeinen Cybersicherheit soll zukünftig sichergestellt werden, dass KRITIS-Betreiber und ggfs. andere Stellen relevante **Cybersicherheitsinformationen auf freiwilliger Basis untereinander austauschen** können, um Sicherheitsvorfälle zu verhindern, aufzudecken oder darauf reagieren zu können.

Im Falle von Verstößen sieht die NIS2-Richtlinie vor, dass Verstöße mit **Geldbußen in Höhe von bis zu 10 Mio. EUR bzw. 2 Prozent** des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes geahndet werden können.

Cyber Resilience Act

Mit dem **Cyber Resilience Act (CRA)** gibt es ein weiteres Gesetzgebungsvorhaben auf EU-Ebene mit dem **Ziel der Verbesserung der Cybersecurity**. Damit ergänzt der CRA den bereits geltenden EU-Cybersecurity Act[2]. Der CRA wird aktuell politisch diskutiert, ist mithin noch nicht in Kraft getreten.

Im Fokus des CRA steht die **Verbesserung der Cybersicherheit sog. Produkte mit digitalen Elementen**. Diese Begrifflichkeit bezieht sich auf Software- oder Hardwareprodukte, mittels derer eine Remote-Verbindung hergestellt werden kann, d.h. insbesondere sog. vernetzte Geräte.

Zum einen soll der CRA eine Verbesserung der Cybersicherheit solcher Produkte erreichen; zu diesem Zweck sollen Produkte **bestimmte Cybersicherheit-Merkmale** erfüllen müssen, um in der EU in Verkehr gebracht werden zu dürfen. Zum anderen sollen Nutzer **bessere Informationen** erhalten, um Produkte mit angemessenen Cybersicherheitsmerkmalen auswählen und sicher verwenden zu können.

Zu den verpflichteten Stellen des CRA gehören neben den **Herstellern** von Produkten mit digitalen Elementen insbesondere **Händler und Importeure**, die entsprechende Produkte in der EU in Verkehr bringen oder verbreiten.

[2] 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

Ansprechpartner

Dr. Ulla Kelp, LL.M.
Rechtsanwältin, Partner

T +49 211 600 35-176
ulla.kelp@orthkluth.com

Dr. Philipp Mels
Rechtsanwalt, Partner

T +49 211 600 35-180
philipp.mels@orthkluth.com

Elisaveta Breckheimer
Rechtsanwältin, Salary Partner

T +49 211 600 35-190
elisaveta.breckheimer@orthkluth.com

Dr. Anja Doepner-Thiele. LL.M.
Rechtsanwältin, Salary Partner

T +49 211 600 35-168
anja.doepner-thiele@orthkluth.com

Dr. Michael Grobe-Einsler
Rechtsanwalt, Salary Partner

T +49 211 600 35-450
michael.grobe-einsler@orthkluth.com

Maren Müller-Mergenthaler, LL.M.
Rechtsanwältin, Salary Partner

T +49 211 600 35-445
maren.mueller-mergenthaler@orthkluth.com

Laura Delpy
Rechtsanwältin, Senior Associate

T +49 211 600 35-310
laura.delpy@orthkluth.com

Felix Meurer
Rechtsanwalt, Associate

T +49 30 50 93 20-117
felix.meurer@orthkluth.com

Philippe Julius Träm
Rechtsanwalt, Associate

T +49 30 50 93 20-134
philippe.traem@orthkluth.com

Markus Kreuzkamp
Rechtsanwalt, Counsel

T +49 211 600 35-0
markus.kreuzkamp@orthkluth.com

Prof. Dr. Michael Bohne
Of Counsel

T +49 211 600 35-174
michael.bohne@orthkluth.com

Prof. Dr. Kristoff Ritlewski, LL.M.
Of Counsel

T +49 30 50 93 20-0
kristoff.ritlewski@orthkluth.com

One Team.
One Goal.