

# Cybersecurity – Hintergrund der vielen neuen Gesetzgebungen



| Gesetzgebung   | Inhalte  |  |
|--|--|--|
| <p><u>Richtlinie über die Haftung für fehlerhafte Produkte (EU) 2024/2853</u><br/> <b>Produktebene</b></p>   | <p>Es kann auch festgestellt werden, dass ein Produkt aufgrund seiner Sicherheitslücken im Bereich der <b>Cybersicherheit</b> fehlerhaft ist, etwa wenn das Produkt die sicherheitsrelevanten Cybersicherheitsanforderungen nicht erfüllt.“<br/> (Erwägungsgrund 32)</p>   | <p>[...] unter „Produkt“ sind auch Elektrizität, digitale Konstruktionsunterlagen, Rohstoffe und <b>Software</b> zu verstehen<br/> (Artikel 4, Begriffsbestimmungen)</p>   |
| <p><u>Verordnung über Künstliche Intelligenz (COM/2021/206 final)</u><br/> <b>Produktebene + Software als Produkt</b></p>                              | <p>Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass sie im Hinblick auf ihre Zweckbestimmung ein angemessenes Maß an Genauigkeit, Robustheit und <b>Cybersicherheit</b> erreichen und in dieser Hinsicht während ihres gesamten Lebenszyklus beständig funktionieren.<br/> (Artikel 15, Genauigkeit, Robustheit und <b>Cybersicherheit</b>)</p> |  |
| <p><u>Agentur der Europäischen Union für Cybersicherheit zur Zertifizierung der Cybersicherheit (EU) 2019/881</u><br/> <b>Mitgliedstaatenebene</b></p> | <p>„<b>Cybersicherheit</b>“ bezeichnet alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von <b>Cyberbedrohungen</b> betroffene Personen zu schützen;</p>  | <p>„<b>Cyberbedrohung</b>“ bezeichnet 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;</p> |
| <p><u>Cybersicherheitsanforderungen für Produkte (EU)2024/2847</u><br/> <b>Produktebene + Marktüberwachungsebene</b></p>                               | <p>grundlegende <b>Cybersicherheitsanforderungen</b> an die von den Herstellern festgelegten Verfahren zur Behandlung von Schwachstellen, um die <b>Cybersicherheit von Produkten mit digitalen Elementen</b> während der erwarteten Nutzungsdauer der Produkte zu gewährleisten, sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Verfahren;</p>     | <p>Vorschriften für die Marktüberwachung, einschließlich Überwachung, und die Durchsetzung der in diesem Artikel genannten Vorschriften und Anforderungen.<br/> (Artikel 1, Gegenstand)</p>  |

# Cybersecurity – Hintergrund der vielen neuen Gesetzgebungen



| Gesetzgebung   | Inhalte   |
|--|---|
| <u>Datenzugang- und Datennutzungsverordnung (EU) 2023/2854</u><br>Mitgliedsstaatenebene  | „ <b>öffentlicher Notstand</b> “ eine zeitlich begrenzte Ausnahmesituation – wie etwa Notfälle im Bereich der öffentlichen Gesundheit, Notfälle infolge von Naturkatastrophen sowie von Menschen verursachte Katastrophen größeren Ausmaßes, einschließlich schwerer <b>Cybersicherheitsvorfälle</b> –, die sich negativ auf die Bevölkerung der Union oder eines Mitgliedstaats bzw. eines Teils davon auswirkt, das Risiko schwerwiegender und dauerhafter Folgen für die Lebensbedingungen, die wirtschaftliche Stabilität oder die finanzielle Stabilität oder die Gefahr einer erheblichen und unmittelbaren Beeinträchtigung wirtschaftlicher Vermögenswerte in der Union oder in dem betroffenen Mitgliedstaat birgt und die nach den einschlägigen Verfahren des Unionsrechts oder des nationalen Rechts festgestellt und amtlich ausgerufen wurde; (Artikel 2, Begriffsbestimmungen) |
| <u>Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2, (EU) 2022/2555)</u><br>Mitgliedsstaaten-, Behörden-, Hersteller- / Produktebene | In dieser Richtlinie werden Maßnahmen festgelegt, mit denen in der gesamten Union ein hohes gemeinsames <b>Cybersicherheitsniveau</b> sichergestellt werden soll, um so das Funktionieren des Binnenmarkts zu verbessern.   |
| <u>Funkanlagenrichtlinie 2014/53/EU</u> → Delegierte Verordnung<br>(EU) 2023/2444 (Neue Normen)<br>Produktebene  | „[...] <b>Cybersicherheit</b> , nämlich den Schutz von Netzwerken, personenbezogenen Daten und der Privatsphäre sowie den Schutz vor Betrug.“<br><br>Anforderungen an Funkanlagen, die über das <b>Internet kommunizieren</b> können (Art. 1, Abs. 1), <b>Personenbezogene Daten</b> verarbeiten können (Art. 1, Abs. 2) monetäre Werte übertragen können (Art. 1, Abs. 3) neu erarbeitete <b>Normreihe EN 18031-1 / -2 / -3</b> : einheitliche Prüfverfahren für Konformität mit <b>Cybersicherheitsanforderungen</b> der Funkanlagenrichtlinie  |
| <u>Durchführungsverordnung (EU) 2024/482 hinsichtlich der Annahme des auf den Gemeinsamen Kriterien beruhenden europäischen Systems für die Cybersicherheitszertifizierung (EUCC)</u><br>Produkt und Behördenebene   | Festlegung eines auf den Gemeinsamen Kriterien beruhenden europäischen Systems für die <b>Cybersicherheitszertifizierung (EUCC)</b> für alle Produkte der Informations- und Kommunikationstechnik (IKT) (Art. 1)  |

**Bitte beachten Sie:** Die trade-e-bility GmbH erbringt keine Rechtsdienstleistungen gemäß § 2 Abs. 1 des Rechtsdienstleistungsgesetzes (RDG) erbringt, das heißt keine Tätigkeiten in konkreten fremden Angelegenheiten mit rechtlicher Prüfung des Einzelfalls vornimmt. Die Anwendung und Auslegung von Gesetzestexten in Bezug auf Ihre Produkte oder Fragen liegt allein in Ihrer Verantwortung. Selbstverständlich werden Ihre Daten vertraulich behandelt. Eine handelsrechtliche Bewertung erfolgt nicht. Hier finden Sie unsere [AGBs](#).