PAiCE

DIE AKTUELLE IT-SICHERHEITS-GESETZGEBUNG UND DIE URHEBERRECHTSREFORM

ERSTE EINSCHÄTZUNGEN FÜR DIE BETREIBER VON INDUSTRIEPLATTFORMEN

Impressum

Herausgeber
Begleitforschung PAiCE
iit – Institut für Innovation und Technik in der
VDI / VDE Innovation + Technik GmbH
Peter Gabriel
Steinplatz 1
10623 Berlin
gabriel@iit-berlin.de
www.paice.de

Autoren
Karsten U. Bartels LL.M., HK2 Rechtsanwälte
Sebastian Straub LL.M, VDI/VDE-IT

Gestaltung
Loesch*Hund*Liepold
Kommunikation GmbH
Hauptstraße 28 | 10827 Berlin
paice@lhlk.de

Stand
Januar 2020

Bildnachweis
BillionPhotos.com – stock.adobe.com (Titel)

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Inhalt

Einleitung

Die Verbundprojekte des BMWi-Technologieprogramms PAiCE beschäftigen sich in praxisnahen Pilotprojekten mit dem Aufbau digitaler Industrieplattformen und der Kollaboration von Unternehmen über Plattformen. Sie stehen damit prototypisch für viele andere Unternehmen, die ähnliche Vorhaben verfolgen. Dabei müssen die Betreiber der Plattformen bei der Umsetzung ihrer Vorhaben immer auch die aktuellen rechtlichen Rahmenbedingungen berücksichtigen. Zuletzt gab es im Bereich des IT-Sicherheitsrechts und des Urheberrechts Anpassungen, die ggf. Auswirkungen auf Industrieplattformen haben.

Zu den gesetzgeberischen Aktivitäten im Bereich des IT-Sicherheitsrecht gehörten in der jüngeren Vergangenheit unter anderem das IT-Sicherheitsgesetz und die Datenschutz-Grundverordnung (DSGVO). Vor einigen Monaten kam auf europäischer Ebene der Cyber Security Act (CSA) hinzu, und eine signifikante Änderung des deutschen IT-Sicherheitsgesetzes (ITSig 2.0) kündigt sich bereits konkret an. Die Unternehmen müssen eine Vielzahl rechtlicher Pflichten in Bezug auf ihre IT-Sicherheit erfüllen, die jedoch in höchst unterschiedlichen gesetzlichen Regelungen verankert sind. Zusätzlich kann die gerade verabschiedete Reform des europäischen Urheberrechts Auswirkungen auf Plattformbetreiber haben.

Dieses Papier stellt ausgewählte, relevante Herausforderungen zusammen, die sich für Plattformbetreiber, zumindest potenziell, aus den gerade diskutierten oder schon verabschiedeten IT-Sicherheitsgesetzen und aus der europäischen Urheberrechtsreform ergeben. Dies erfolgt beispielhaft anhand der Projekte im Technologieprogramm PAiCE: Die Projekte im Cluster Robotik befassen sich mit offenen Baukastensystemen für Serviceroboter in Industrie und Dienstleistungsgewerbe. Im Cluster 3D arbeiten die Projekte an dezentralen Produktionsplattformen auf Basis der additiven Fertigung. Die Projekte des Clusters Engineering entwickeln und erproben Konzepte für ein kooperatives Engineering von Produkten und Industrieanlagen. Die Projekte des Clusters Logistik beschäftigen sich mit Plattformen für das Management von Logistiknetzwerken.

Die Aktualität der diskutierten Gesetze und Gesetzesvorhaben bringt es mit sich, dass abschließende Antworten oft kaum möglich sind und der beste Rat häufig ist, die Entwicklungen aktiv zu beobachten. Leser und Leserinnen, die sich außerhalb von PAiCE mit ähnlichen Plattformprojekten beschäftigen, werden sicherlich unsere Argumentation auch auf ihre Vorhaben übertragen können.

1 Cyber Security Act

Im Dezember 2018 hatten sich das Europäische Parlament, der Rat und die Europäische Kommission im Triolog-Verfahren auf den Cyber Security Act geeinigt, der zum einen erstmalig einen europaweit geltenden Zertifizierungsrahmen für die Cybersicherheit von Produkten, Verfahren und Diensten schaffen und zum anderen die ENISA (Agentur der Europäischen Union für Netz- und Informationssicherheit) mit einem ständigen und weitreichenderen Mandat ausstatten sollte. Am 12.03.2019 hat das Europaparlament den CSA nun mit großer Mehrheit verabschiedet.

Ziel ist die Anhebung und Harmonisierung des Niveaus der IT-Sicherheit in der EU. Entsprechende Mindestsicherheitsstandards sollen von der ENISA festgelegt werden. Der geplante Zertifizierungsrahmen soll verschiedene Levels der IT-Sicherheit aufweisen (Art. 52 Abs. 1 CSA). Je nach Einordnung soll der Adressat erkennen können, inwieweit der beschriebenen Sicherheit des jeweiligen Produktes bzw. der jeweiligen Dienstleistung vertraut werden kann. Die einzelnen Anforderungen an die Sicherheitslevels werden wiederum vom Risiko im Einzelfall abhängig sein.

Die kommenden Mindestsicherheitsstandards sollen unter anderem derart konzipiert sein, dass gespeicherte, übertragene oder anderweitig verarbeitete Daten vor unbeabsichtigten oder unvorhergesehenen Ereignissen, unbefugter Speicherung, Verarbeitung, Zugriff oder Offenlegung während des gesamten Lebenszyklus des Produkts, Dienstes oder Prozesses geschützt werden.

Daneben soll es europäische Sicherheitszertifikate sowie Angemessenheitsentscheidungen geben, die auch europaweite Gültigkeit erhalten sollen. Verbindliche Zertifizierungsschemata sollen in einer Liste festgeschrieben werden. Bestimmte Zertifizierungen werden von ausgewählten privaten Zertifizierungsstellen, die wiederum durch nationale Aufsichtsbehörden überwacht werden, durchgeführt werden dürfen. In Deutschland wird diese Aufgabe voraussichtlich von der Deutschen Akkreditierungsstelle (DAkkS) sowie vom Bundesamt für Sicherheit in der Informationstechnik (BSI) übernommen werden.

Darüber hinaus wird es Selbstzertifizierungsmechanismen für Hersteller von IT-Produkten geben, sofern deren Einsatz ein geringes Risiko aufweist. Ähnlich der Pflicht zu Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen aus Art. 25 DSGVO soll der CSA zu einer Beachtung der Grundsätze von security by design und privacy by design bereits bei der Entwicklung von Lösungen beitragen (s. III. sowie Erwägungsgrund 12, 13 CSA).

Der CSA formuliert bereits jetzt Pflichten für Hersteller von IT-Produkten und -Diensten; welche praktischen Folgen dies im Detail für die Nutzung von IT haben wird, ist jedoch mangels Finalisierung der Zertifizierungsprozesse noch unklar. Auch ist noch offen, in welchem Verhältnis CSA-basierte Zertifizierungen zu anderen Zertifizierungen mit Fokus auf die IT-Sicherheit oder Datenschutz stehen werden. Es ist von wesentlicher Bedeutung, wie mit der Vielzahl geplanter und sich in ihrem Anwendungsbereich überschneidender IT-Sicherheitszertifikaten der ENISA, des BSI, der European Cyber Security Organisation (ECSO) sowie der privaten oder öffentlichen Zertifizierer gemäß Art. 43 DSGVO umzugehen sein wird und inwieweit Zertifizierungen für unterschiedliche Unternehmensbereiche und Geschäftsprozesse eingesetzt werden können. Hier scheinen alle Fragen offen.

Ist das für mich als Plattformbetreiber relevant?

Der CSA schafft einen Zertifizierungsrahmen für die Sicherheit von Produkten, Verfahren und Diensten. Die Auswirkungen des CSA auf Industrieplattformen lassen sich derzeit nicht abschließend bewerten. Vor der Ausarbeitung konkreter Zertifizierungsprozesse müssen cybersicherheitsrelevante Produkte und Dienste zunächst durch die EU-Kommission definiert werden. Dies ist bislang nicht geschehen. Es ist jedoch nicht unwahrscheinlich, dass im Rahmen der bevorstehenden Ausarbeitung der Cybersicherheitsschemata Umsetzungsbedarf auf die Betreiber von Industrieplattformen zu kommen wird. Der Prozess und insbesondere die Zertifizierungsaktivitäten der ENISA sollten daher verfolgt werden.

Relevant bei Logistikplattformen mit intelligenten Ladungsträgern?	(✓)	eventuell, wenn die Plattformen von der EU-Kommission als cybersicherheitsrelevante Dienste definiert werden. Die Entwicklungen beim CSA sollten zumindest beobachtet werden
Relevant bei offenen Baukastensystemen für Serviceroboter?	(✓)	eventuell, wenn die Plattformen von der EU-Kommission als cybersicherheitsrelevante Dienste definiert werden. Die Entwicklungen beim CSA sollten zumindest beobachtet werden
Relevant bei dezentrale Produktionsplattformen auf Basis der additiven Fertigung?	(✓)	eventuell, wenn die Plattformen von der EU-Kommission als cybersicherheitsrelevante Dienste definiert werden. Die Entwicklungen beim CSA sollten zumindest beobachtet werden
Relevant bei Plattformen für das kooperative Engineering von Produkten und Industrieanlagen?	(✓)	eventuell, wenn die Plattformen von der EU-Kommission als cybersicherheitsrelevante Dienste definiert werden. Die Entwicklungen beim CSA sollten zumindest beobachtet werden

2 IT-Sicherheitsgesetz 2.0

Das IT-Sicherheitsgesetz gilt bereits seit Juli 2015 und hat als Artikeländerungsgesetz umfangreiche Anforderungen an für die Gesellschaft kritische Versorgungsbereiche (Kritische Infrastrukturen – KRITIS) formuliert. In den Jahren 2016 und 2017 wurde das Gesetz per Rechtsverordnung für die KRITIS-Sektoren konkretisiert.

Da der Gesetzgeber die entsprechenden IT-sicherheitsrechtlichen Vorgaben nach dem ersten Aufschlag weiter an die praktischen Gegebenheiten anpassen will, soll nun das sogenannte IT-Sicherheitsgesetz 2.0, welches aktuell in Form eines Referentenentwurfs vorliegt, verabschiedet werden.

Auch das neue Gesetz wird zukünftig durch Rechtsverordnungen konkretisiert werden und zu erneuten Änderungen und folglich Pflichten im Bereich der IT-Sicherheit führen. Hinzu kommt eine generelle Ausweitung des Anwendungsbereiches, da unter anderem Infrastrukturen von besonderem öffentlichem Interesse aus dem Bereich Rüstungsindustrie, Kultur und Medien sowie Unternehmen von erheblicher volkswirtschaftlicher Bedeutung wie KRITIS-Betreiber behandelt werden können. Zudem soll das BSI Anlagenbetreibern, die nicht KRITIS-Betreiber sind, bei Vorliegen einer „Cyberkritikalität" auch durch Verwaltungsakt die Pflichten zur IT-Sicherheit auferlegen dürfen (§ 8g BSIG-E).

Der Entwurf enthält diverse Befugniserweiterungen des BSI. Der derzeitige Entwurf formuliert unter anderem, ähnlich wie der CSA, Regelungen zur Kennzeichnung von IT-Sicherheitsprodukten zum Zwecke des Verbraucherschutzes, die wiederum nun auch das BSI durchführen soll. Darüber hinaus wird das BSI Mindeststandards für Kernkomponenten Kritischer Infrastrukturen (KRITIS-Kernkomponenten), also Maßnahmen, die für den Betrieb kritischer Anlagen erforderlich sind bzw. deren Störung weitreichende Folgen hätte, ausarbeiten. Hersteller von KRITIS-Kernkomponenten werden ergänzend eine BSI-Sicherheitskennzeichnung beantragen müssen, um es KRITIS-Betreiber zu ermöglichen, die jeweiligen Produkte zu verwenden. Zu beachten ist, dass nicht nur einzelne IT-Produkte erfasst werden sollen, sondern insbesondere vernetzte Systeme.

Zudem sollen künftig auch die Hersteller von IT-Produkten verpflichtet sein, erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Produkte unverzüglich dem BSI zu melden, § 8h Abs. 2 BSIG-E.

Ähnlich wie die DSGVO im Bereich des Datenschutzrechts, sieht auch die Reformierung des IT-Sicherheitsgesetzes eine drastische Erhöhung des Bußgeldrahmens vor. Auch hier sollen Geldbußen von bis zu EUR 20.000.000 oder von bis zu 4 % des gesamten weltweit erzielten Vorjahresumsatzes, je nachdem, welcher der Beträge höher ist, verhängt werden können.

Ist das für mich als Plattformbetreiber relevant?

Der aktuelle Referentenentwurf zum IT-Sicherheitsgesetz sieht eine Erweiterung des Anwendungsbereichs vor. Pflichten zur Gewährleistung von IT-Sicherheitsmindeststandards ergäben sich jetzt auch für Unternehmen von besonderem öffentlichem Interesse. Darüber hinaus würden die Befugnisse des BSI erweitert und neue Meldepflichten eingeführt. Industrieplattformen betreiben in der Regel keine kritischen Infrastrukturen, auch nicht im erweiterten Sinne, so dass sie nicht primär in den Anwendungsbereich des geplanten Gesetzes fallen. Unterhalb der KRITIS-Schwellenwerte könnten Plattformen ggf. aber dann zu technisch-organisatorischen Vorkehrungen verpflichtet werden, wenn Störungen der eingesetzten IT wegen des hohen Grades an Vernetzung zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der betroffenen Dienstleistung insgesamt führen würden (sog. „Cyberkritikalität"). Daneben können sich Meldepflichten ergeben, insbesondere wenn Plattformen IT-Produkte (Soft- oder Hardware) bereitstellen und ein Ausfall dieser IT-Produkte erhebliche Auswirkungen auf den Betrieb von Kritischen Infrastrukturen oder Unternehmen von besonderem öffentlichem Interesse hat.

Relevant bei Logistikplattformen mit intelligenten Ladungsträgern?	(✓)	Ggf. ergeben sich Pflichten bei Vorliegen von „Cyberkritikalität". Daneben können sich auch Meldepflichten ergeben, wenn IT-Produkte für KRITIS-Betreiber oder Infrastrukturen von besonderem öffentlichem Interesse (z.B. für die Automobilindustrie) bereitgestellt werden
Relevant bei offenen Baukastensystemen für Serviceroboter?	(✓)	Eher nein. Es können sich aber Meldepflichten ergeben, wenn IT-Produkte für KRITIS-Betreiber oder Infrastrukturen von besonderem öffentlichem Interesse bereitgestellt werden
Relevant bei dezentrale Produktionsplattformen auf Basis der additiven Fertigung?	(✓)	Eher nein. Es können sich aber Meldepflichten ergeben, wenn IT-Produkte für KRITIS-Betreiber oder Infrastrukturen von besonderem öffentlichem Interesse bereitgestellt werden
Relevant bei Plattformen für das kooperative Engineering von Produkten und Industrieanlagen?	(✓)	Ggf. ergeben sich Pflichten bei Vorliegen von „Cyberkritikalität". Daneben können sich auch Meldepflichten ergeben, wenn IT-Produkte für KRITIS-Betreiber oder Infrastrukturen von besonderem öffentlichem Interesse bereitgestellt werden

3 Datenschutz-Grundverordnung

Die seit Mai 2018 geltende DSGVO hat umfassende Anforderungen an die Informationssicherheit zum Schutz personenbezogener Daten geschaffen. Die zentrale Norm für die IT-Sicherheit stellt der Art. 32 Abs. 1 DSGVO dar. Danach ist bei der Datenverarbeitung ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Auswahl und Unterhaltung der zu treffenden technischen und organisatorischen Maßnahmen (TOM) sind der Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung und auch die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Allein diese – für alle Unternehmen geltenden – Anforderungen sind bereits technisch wie rechtlich sehr komplex. Brauchbare Hinweise der nationalen Aufsichtsbehörden zur Umsetzung gibt es (auch hierzu) nicht. Das gilt auch für die EU-Ebene.

Wie der CSA sieht auch die DSGVO Möglichkeiten zur Zertifizierung zum Nachweis datenschutzrechtlich zulässiger Datenverarbeitungen vor. Aber auch hier herrscht Unklarheit: noch immer sind Akkreditierungen von entsprechenden Zertifizierungsstellen durch die DAkkS nicht vollzogen worden. Auch die Zertifizierungskriterien, die durch das European Data Protection Board (EDPB) festgelegt werden, sind noch nicht entwickelt worden. Die DSGVO-Zertifizierungen könnten in Zukunft erheblich zur Rechtssicherheit beitragen. Dennoch sind sowohl die Voraussetzungen als auch der Zeitpunkt ihrer Nutzbarkeit noch völlig unbekannt. Damit ist es den Unternehmen derzeit nicht einmal möglich, sich auf künftige Zertifizierungen bereits jetzt vorzubereiten.

Ist das für mich als Plattformbetreiber relevant?

Die Zulässigkeit der Verarbeitung von Nutzer-, Dienstleister-, Zulieferer- oder auch Standortdaten bemisst sich in der Regel nach den Vorgaben der DSGVO, sofern es sich bei diesen Daten um personenbezogene Daten handelt. Im Gegensatz dazu ist der Anwendungsbereich der DSGVO nicht eröffnet, wenn sich die Informationen nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen. Das kann etwa bei Maschinendaten der Fall sein. Fällt die Datenverarbeitung in den Anwendungsbereich der DSGVO, sind insbesondere die Vorgaben hinsichtlich der Sicherheit der Verarbeitung nach Art. 32 Abs. 1 DSGVO zu beachten.

Relevant bei Logistikplattformen mit intelligenten Ladungsträgern?	(✓)	ja, etwa beim Tracking von Prozessen im Umfeld von Mitarbeitern oder Auslieferern, aber auch bei der Verarbeitung von Nutzer- oder Kundendaten
Relevant bei offenen Baukastensystemen für Serviceroboter?	(✓)	ja, etwa wenn Bedienerdaten ausgewertet werden, aber auch bei der Verarbeitung von Nutzer- oder Kundendaten
Relevant bei dezentrale Produktionsplattformen auf Basis der additiven Fertigung?	(✓)	ja, etwa bei der Verarbeitung von Nutzer- oder Kundendaten
Relevant bei Plattformen für das kooperative Engineering von Produkten und Industrieanlagen?	(✓)	ja, etwa bei der Verarbeitung von Bedienerdaten, nicht jedoch bei der Verarbeitung von Maschinendaten ohne Personenbezug

4 Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit

Zusätzlich zum nationalen ITSiG hat der Europäische Gesetzgeber im Rahmen seiner Cybersicherheitsstrategie die Richtlinie zur Netz- und Informationssicherheit (NIS) beschlossen, welche im April 2017 national umgesetzt wurde. Diese führte zu Anpassungen der alten Fassung des ITSiG und schuf darüber hinaus neue Pflichten für sogenannte digitale Dienste (§ 8c BSIG). Zu diesen Diensten zählen Online-Marktplätze, Online-Suchmaschinen sowie Cloud-Computing-Dienste. Seit Mitte 2018 gilt zudem eine zusätzliche, europaweit geltende Durchführungsverordnung, die die Anforderungen an die IT-Sicherheit adressierter Anbieter weiter konkretisiert.

Auch für den spezifischen Bereich der digitalen Dienste normiert der Gesetzgeber eine Erweiterung der Aufsichts- und Durchsetzungsbefugnisse des BSI, welches bereits bei Anhaltspunkten zur Nichterfüllung der Anforderungen an adressierte Online-Dienste tätig werden kann.

Neben weitreichenden Meldepflichten schuf das auf Grundlage der Anforderungen der NIS-RL erlassene Umsetzungsgesetz zudem umfassende Anforderungen an die IT-Sicherheit von Anbietern digitaler Dienste in Deutschland. Aufgrund der Kritikalität der erfassten Systeme sind diese durch geeignete und verhältnismäßige technische und organisatorische Maßnahmen zur Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen nach dem Stand der Technik zu schützen. Darüber hinaus bestehen auch hier umfangreiche Meldepflichten, § 8c Abs. 3 BSIG.

Ist das für mich als Plattformbetreiber relevant?

Die im Rahmen der NIS-Richtlinie vorgenommen Änderungen am nationalen ITSiG adressieren vorrangig Anbieter von digitalen Diensten. Plattformen müssen die neugeschaffenen Vorgaben nur erfüllen, wenn sie Anbieter eines digitalen Dienstes sind. Digitale Dienste sind Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste im Sinne von § 2 Abs. 11 Ziff. 1-3 BSIG und im Sinne der Richtlinie (EU) 2015/1535. Die umzusetzenden Maßnahmen werden durch Durchführungsrechtsakte der EU-Kommission näher bestimmt. Bei Sicherheitsvorfällen können sich für digitale Dienste auch Meldepflichten ergeben.

Relevant bei Logistikplattformen mit intelligenten Ladungsträgern?	(✓)	ggf. ja, wenn Plattform als Online-Marktplatz einzuordnen ist
Relevant bei offenen Baukastensystemen für Serviceroboter?	(✓)	ggf. ja, wenn Plattform als Cloud-Computing-Dienst einzuordnen ist
Relevant bei dezentrale Produktionsplattformen auf Basis der additiven Fertigung?	(✓)	ggf. ja, wenn Plattform als Online-Marktplatz einzuordnen ist
Relevant bei Plattformen für das kooperative Engineering von Produkten und Industrieanlagen?	(✓)	ggf. ja, wenn Plattform als Cloud-Computing-Dienst oder Online-Marktplatz einzuordnen ist

5 Zwischenfazit: neue Anforderungen an die IT-Sicherheit

Die neuen gesetzlichen Anforderungen an die IT-Sicherheit sind komplex. Insbesondere das Zusammenspiel von IT-sicherheitsrelevanten Zertifizierungen wird Unternehmen vor große Herausforderungen stellen und detailliert herauszuarbeiten sein, um rechtzeitig den Grundstein für einen effektiven und ausreichenden Aufbau einer gesetzeskonformen IT-Infrastruktur legen und die Möglichkeit entsprechender Zertifizierungen vorbereiten zu können.

Derzeit kann weder vorhergesagt werden, welche Zertifikate sich durchsetzen, noch welche Voraussetzungen diese im Einzelnen beinhalten werden. Dennoch ist es bereits jetzt wichtig sicherzustellen, dass IT-Sicherheitskonzepte ausgearbeitet werden, die eine Erfüllung der Vielzahl der IT-rechtlicher Anforderungen möglich machen und die als Grundlage zur Durchführung von Zertifizierungen genutzt werden können.

Ebenso benötigen die Unternehmen Unterstützung bei der konsolidierten, synchronen Umsetzung der diversen Gesetze mit identischen IT-Sicherheitszielen. Dazu gehören vor allem Klarstellungen durch den Gesetzgeber und handhabbare, abgestimmte Hilfestellungen der diversen zuständigen Aufsichtsbehörden (Datenschutzaufsicht, BSI bzw. branchenspezifische Fachaufsicht).

6 Urheberrecht im digitalen Binnenmarkt

Der europäische Rat hat am 15. April 2019 der Richtlinie zur Reform des Urheberrechts im digitalen Binnenmarkt mehrheitlich zugestimmt. Die Richtlinie sieht insbesondere eine Haftungsverschärfung für Plattformbetreiber für das Teilen von Online-Inhalten vor. Die Verantwortlichkeit von Online-Plattformen bei der Bereitstellung von urheberrechtlich geschützten Inhalten wurde bislang maßgeblich durch die E-Commerce-Richtlinie (ECRL) vorgegeben. Art. 14 der Richtlinie sieht eine weitreichende Haftungsprivilegierung vor. Danach sind Online-Plattformen für die von ihnen bereitgestellten Inhalte nicht verantwortlich, wenn sie keine Kenntnis von der Rechtswidrigkeit haben oder die Inhalte nach Kenntniserlangung unverzüglich entfernt oder gesperrt werden. Das hier zum Ausdruck kommende „Notice-and-take-down"-Prinzip wurde mit § 10 Telemediengesetz (TMG) in nationales Recht umgesetzt.

Das bisherige Haftungsregime der ECRL bzw. des TMG wird nach Umsetzung der neuen Urheberrechtsrichtlinie weitestgehend verdrängt und durch einen neuen (Ent)Haftungsmechanismus ersetzt. Dieser sieht vor, dass Plattformen von den Rechteinhabern eine entsprechende Erlaubnis (z.B. eine Lizenz) erwerben oder jedenfalls nachweisen, dass alle Anstrengungen zur Einholung einer Erlaubnis und zur Gewährleistung des Urheberrechtsschutzes nach Maßgabe der Richtlinie unternommen wurden. Wird keine Lizenz erteilt, muss die Plattform sicherstellen, dass geschützte Inhalte nicht öffentlich zugänglich gemacht werden. Hierfür ist es erforderlich, dass die Rechteinhaber alle einschlägigen und notwendigen Informationen zur Identifizierung von geschützten Inhalten bereitstellen. Kommt es trotz dieser Maßnahmen zu einer Veröffentlichung und erlangt die Plattform Kenntnis von der Rechtsverletzung, muss sie die Inhalte unverzüglich entfernen und auch dafür Sorge tragen, dass diese zukünftig nicht mehr hochgeladen werden. Die Plattform kann einer Haftung nur dann entgehen, wenn die vorgenannten Maßnahmen nachweislich durchgeführt wurden. Weniger strengen Haftungsregeln unterliegen Plattformen, die jünger als drei Jahre sind und weniger als 10 Millionen Euro Jahresumsatz erwirtschaften. Diese müssen sich lediglich um eine Nutzungserlaubnis bemühen und umgehend auf Takedown-Notices reagieren.

Das neue Haftungssystem adressiert vorrangig große Plattformen wie YouTube oder Facebook, deren Geschäftsmodell auf der Bereitstellung von benutzergenerierten Inhalten beruht. Fraglich ist jedoch, ob auch kleinere Plattformen von der Haftungsverschärfung betroffen sind. Entscheidend hierfür ist, ob Plattformen als „Diensteanbieter für das Teilen von Online-Inhalten" zu betrachten sind. Nach der Legaldefinition der Richtlinie fallen hierunter Anbieter deren Hauptzweck bzw. einer der Hauptzwecke darin besteht, große Mengen urheberrechtlich geschützter Werke bereitzustellen und zum Zwecke der Gewinnerzielung zu bewerben. Ausgenommen hiervon sind Online-Enzyklopädien, nicht gewinnorientierte bildungsbezogene und wissenschaftliche Repositorien, Entwicklungs- und Weitergabeplattformen für quelloffene Software, Anbieter elektronischer Kommunikationsdienste, Online-Marktplätze, zwischen Unternehmen erbrachte Cloud-Dienste sowie Cloud-Dienste, die ihren Nutzern das Hochladen von Inhalten für den Eigengebrauch ermöglichen. Plattformbetreiber sollten prüfen, ob und in welchem Umfang sie urheberrechtlich geschützte Werke oder sonstige Schutzgegenstände bereitstellen und inwieweit eine gewinnorientierte Bewerbung dieser Inhalte erfolgt. In der Regel spielt die Bereitstellung von geschützten Inhalten mit der Absicht der Gewinnerzielung bei Industrieplattformen keine bzw. eine untergeordnete Rolle, weshalb sie nicht in den Anwendungsbereich der Richtlinie fallen. Klare Abgrenzungskriterien lassen sich jedoch anhand der vorliegenden Definition nicht ableiten. Industrieplattformbetreiber sollten daher den weiteren Umsetzungsprozess mit Blick auf eine mögliche Konkretisierung durch den nationalen Gesetzgeber verfolgen.

Relevant bei Logistikplattformen mit intelligenten Ladungsträgern?	(✗)	Eher nein, da auf den Plattformen in der Regel keine urheberrechtlich relevanten Inhalte bereitgestellt werden
Relevant bei offenen Baukastensystemen für Serviceroboter?	(✓)	ggf. ja, da in den Baukastensystemen urheberrechtlich geschützte Inhalten bereitgestellt werden. Das gilt aber nur, wenn das Baukastensystem ein „Dienst für das Teilen von Online-Inhalten“ ist. Die Umsetzung der Richtlinie in nationales Recht sollte zumindest beobachtet werden
Relevant bei dezentrale Produktionsplattformen auf Basis der additiven Fertigung?	(✓)	ggf. ja, da über die Plattformen urheberrechtlich geschützte Inhalte bereitgestellt werden. Das gilt aber nur, wenn die jeweilige Plattform ein „Dienst für das Teilen von Online-Inhalten“ ist. Die Umsetzung der Richtlinie in nationales Recht sollte zumindest beobachtet werden
Relevant bei Plattformen für das kooperative Engineering von Produkten und Industrieanlagen?	(✓)	ggf. ja, da über die Plattformen urheberrechtlich geschützte Inhalte bereitgestellt werden. Das gilt aber nur, wenn die jeweilige Plattform ein „Dienst für das Teilen von Online-Inhalten“ ist. Die Umsetzung der Richtlinie in nationales Recht sollte zumindest beobachtet werden

www.paice.de