# IMPULS

## DIGITALE MARKTABSCHOTTUNG:
## AUSWIRKUNGEN VON PROTEKTIONISMUS AUF INDUSTRIE 4.0

VDMA

Stiftung für den Maschinenbau,
den Anlagenbau und die Informationstechnik

Studie von
Bird & Bird LLP
Maximiliansplatz 22
80333 München
E-Mail alexander.duisberg@twobirds.com
Telefon +49 89 35816000

Dr. Alexander Duisberg,
Lara Ueberfeldt

# DIGITALE MARKTABSCHOTTUNG: AUSWIRKUNGEN VON PROTEKTIONISMUS AUF INDUSTRIE 4.0

Dieses Forschungsvorhaben wurde gefördert

von der Impuls-stiftung des VDMA

München, September 2019

# Zu dieser Studie

Aus der digitalen Vision wird zunehmend industrielle Realität. Mit der Digitalisierung von Produktion, Produkten und Dienstleistungen gehen neue Geschäftsmodelle einher. Conditio sine qua non für die digital-vernetzte Welt ist der freie Datenverkehr. Erst auf dieser Basis lassen sich Innovationen und wettbewerbsfähige Lösungen für den Weltmarkt etablieren. Allein – weltweit verändern sich die politischen Agenden. Protektionismus und Marktabschottung gewinnen rapide an Fahrt. Die Gefahr ist groß, dass auch die digital-vernetzte Produktion zunehmend in diesen fatalen Sog gerät. Tatsächlich sind die Unternehmen vielerorts mit Restriktionen und Ausprägungen einer neuen, digitale Marktabschottung konfrontiert.

Die Liste reicht von der Tendenz zur staatlichen Kontrolle und Lokalisierung von Daten über Eingriffe in den Schutz von Betriebs- und Geschäftsgeheimnissen bis hin zu mittelbaren Auswirkungen von Handelssanktionen und einer zunehmenden Regulierung im Bereich der Cyber-Sicherheit. Mit der vorliegenden Studie hat sich die IMPULS-Stiftung auf ein noch weitgehend unbeleuchtetes Gebiet begeben, das dringend einer höheren Aufmerksamkeit bedarf. Im Fokus stehen dabei die Wirtschaftsträume EU, Russland, USA und China. Anhand eines Prüfschemas werden Relevanz und Brisanz ausgewählter Digitalisierungsbarrieren analysiert.

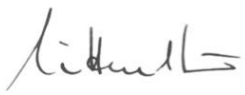
Quintessenz ist: In allen Märkten finden sich Ausprägungen einer digitalen Marktabschottung. Die Unternehmen müssen folglich mit einem asymmetrischen Regulierungsumfeld umgehen und ihre digitale Geschäftsmodelle entsprechend ausrichten. Die eine international anwendbare Lösung wird es dabei nicht geben. Gefragt sind flexible, proaktive Strategien. Wie gehabt bei IMPULS-Studien werden auch Handlungsempfehlungen formuliert: Zum einen für die Politik, wie Handelsbarrieren für einen freien Datenfluss abgebaut und künftig vermieden werden können. Zum anderen in Richtung Maschinen- und Anlagenbau, so dass die Ergebnisse dazu beitragen sollten, den Mehrwert der Digitalisierung in den Unternehmen zu realisieren.

Wir bedanken uns bei Herrn Zimmermann, der als VDMA-Themenpate Anstoß zu dieser wichtigen Studie gegeben hat. Gleichfalls bedanken wir uns bei den Autoren der Studie für die geleistete Arbeit. Unser Dank gebührt auch einem begleitenden Industriekreis, der sich im Zuge der Studienerstellung in hervorragender Weise eingebracht hat.

Der Zeitenwechsel der Digitalisierung beinhaltet immense Chancen für den Maschinen- und Anlagenbau. Wir dürfen es nicht zulassen, dass Protektionismus und Marktabschottung hierüber obsiegen. Mögen die bemerkenswerten Studienergebnisse eine fundierte Orientierung geben – für die betroffenen Unternehmen, aber auch für Politik und Gesellschaft.

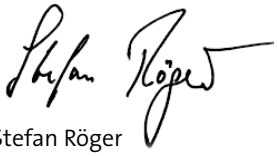
Frankfurt, September 2019

Dr. Thomas Lindner
Vorsitzender des Kuratoriums
IMPULS-Stiftung



Dr. Manfred Wittenstein
Stellv. Vorsitzender des Kuratoriums
IMPULS-Stiftung

Dr. Johannes Gernandt
Geschäftsführender Vorstand
IMPULS-Stiftung



Stefan Röger
Geschäftsführender Vorstand
IMPULS-Stiftung

# Inhalt


Zu dieser Studie 2

Inhalt 3

I. Executive Summary 5

II. Ausgangslage und Zielsetzung der Studie 7

III. Vorgehensweise 8

IV. Relevante Datenkategorien 10

1. Maschinendaten 10
2. Personenbezogene Daten 11

V. Relevante Use Cases 13

1. Einführung 13
2. Remote Access 13
3. Condition Monitoring 14
4. Datenaustauschplattform 14

VI. Überblick Prüffelder 16

1. Schutz von Geschäftsgeheimnissen 17
2. Schutz Kritischer Infrastrukturen 17
3. Vorschriften zur Datenlokalisierung 18
4. Datenschutzrecht 19
5. Regelungen der nationalen Sicherheit 19
6. Einfuhr-/Ausfuhrkontrollbestimmungen 20
7. Handelssanktionen 20

VII. Digitalisierungsbarrieren in der EU 21

1. Einführung 21
2. Schutz von Geschäftsgeheimnissen 21
3. Schutz Kritischer Infrastrukturen 22
4. Vorschriften zur Datenlokalisierung 23
5. Datenschutzgrundverordnung 24
6. Ausfuhrkontrollbestimmungen (Exportkontrolle) 25
7. Handelssanktionen 26

VIII. Digitalisierungsbarrieren in China 28

1. Einführung 28
2. Schutz von Geschäftsgeheimnissen 29
3. Schutz Kritischer Infrastrukturen 31
4. Datenschutzrecht und Schutz wichtiger nicht-personenbezogener Daten 32
5. Vorschriften zur Datenlokalisierung 33
6. Einfuhr-/Ausfuhrkontrollbestimmungen 34

IX. Digitalisierungsbarrieren in Russland 36

1. Einführung 36
2. Digital-Programm 37
3. Schutz Kritischer Infrastrukturen 38
4. Vorschriften zur Datenlokalisierung 39
5. Regelungen der nationalen Sicherheit 41
6. Einfuhrkontrollbestimmungen 43

X. Digitalisierungsbarrieren in den USA 44

1. Einführung 44
2. Schutz von Geschäftsgeheimnissen 45
3. Vorschriften zur Datenlokalisierung 45
4. Datenschutzrecht, Datensicherheit und IoT 46
5. Ausfuhrkontrollbestimmungen (Exportkontrolle) 48
6. Handelssanktionen und protektionistische Handelspolitik 49

XI. Handlungsempfehlungen und Ausblick 50

1. Handlungsempfehlungen an Unternehmen 50
2. Handlungsempfehlungen an den VDMA 52
3. Handlungsempfehlungen an die Politik 53
4. Ausblick 54

Abkürzungsverzeichnis 55

Abbildungsverzeichnis 57

Quellenverzeichnis 58

Endnoten 63

# I. Executive Summary

„Daten sind heutzutage der wichtigste Vermögensgegenstand. Sowohl die größten Chancen als auch Herausforderungen entstehen durch den globalen Fluss von Daten.“[1]

Der Erfolg der Unternehmen des Maschinen- und Anlagenbaus in der digitalen Zukunft hängt entscheidend von dem möglichst ungehinderten Fluss und unternehmensübergreifenden Austausch von personenbezogenen und nicht-personenbezogenen Daten, insbesondere Maschinendaten, ab. Zugleich sind protektionistische Tendenzen im globalen Handel zu erkennen, die sich auch auf den Austausch von Daten – unmittelbar oder mittelbar – auswirken können: In China und Russland treten verstärkt Tendenzen zur staatlichen Kontrolle und Lokalisierung von Daten und Inhalten zutage; in der EU erzeugt der weitreichende Schutz von personenbezogenen Daten hohen und zum Teil überzogenen Aufwand, während in den USA – neben einem ansteigenden Datenschutzniveau – die Auswirkungen von Handelsbarrieren womöglich auf die grundsätzlich stark im Fokus stehende Kommerzialisierbarkeit von Daten einwirken.

Hinzu treten zunehmende Regulierungen im Bereich der Cyber-Sicherheit bzw. IT-Sicherheit, die zwar primär auf den Schutz sog. „**Kritischer Infrastrukturen**“ (Anbieter von Telekommunikationsdiensten, Energieversorger, etc.) abzielen.[2] Diese können aber entweder beiläufig (soweit die Lieferbeziehung mit einem Betreiber einer Kritischen Infrastruktur besteht) oder auch unmittelbar den Bereich des Maschinen- und Anlagenbaus erfassen. Im Zuge der Überarbeitung des deutschen IT-Sicherheitsgesetzes ist damit zu rechnen, dass die Anforderungen an IT-Sicherheit im Bereich Kritischer Infrastrukturen vermehrt auch unmittelbare Bedeutung für den Maschinen- und Anlagenbau gewinnen.[3] In China können Unternehmen des Maschinen- und Anlagenbaus bereits nach der geltenden Rechtslage, die über die eigentlichen Betreiber Kritischer Infrastrukturen hinausgeht, unter den Netzwerkbetreiberbegriff und die damit verbundenen regulatorischen Auflagen fallen.[4]

Unternehmen des Maschinen- und Anlagenbaus müssen mithin mit einem asymmetrischen Regulierungsumfeld umgehen und ihre digitalen Geschäftsmodelle entsprechend ausrichten. Dies führt bereits im Ansatz zu erheblichen Herausforderungen und Kosten in der Umsetzung grenzüberschreitender Lösungen und Dienstangebote – sowohl für den eigenen Betrieb als auch im Verhältnis zu Kunden.

Für die konkret untersuchten Zielmärkte ergeben sich in aller Kürze die folgenden Schlussfolgerungen:

In der EU folgt aus dem weiten Anwendungsbereich des Datenschutzrechts, dass im Bereich der Verarbeitung von Maschinendaten, insbesondere soweit es um Daten aus der Interaktion von Mensch und Maschine geht (HMI-Daten), erhebliche, zum Teil überzogene Anforderungen an Dokumentations- und Informationspflichten und entsprechende Aufwände entstehen. Hier bedarf es weiterführender Orientierungshilfen der Datenschutzbehörden, um die Verarbeitung pseudonymisierter Daten zu erleichtern. Zudem kann es sich anbieten, auf Verbandsebene Verhaltensregeln nach Art. 40, 41 DS-GVO („*Codes of Conduct*“) zu entwickeln, um die rechtskonforme Verarbeitung pseudonymisierter Daten in den Use Cases zu erleichtern.

In China entwickelt sich in Zusammenhang mit der Cyber-Gesetzgebung ein dichtes Regelwerk, das erhebliche Auswirkungen auf den freien Datenaustausch von Maschinendaten mit z. B. einem in Deutschland ansässigen Hersteller haben kann. Angesichts der herausragenden Bedeutung des chinesischen Marktes besteht hier Bedarf für den flankierenden Dialog auf der Ebene politischer Akteure, damit die neuen digitalen Geschäftsmodelle im Bereich des Maschinen- und Anlagenbaus durch einen freien Datenfluss auch aus China in die EU gesichert sind.

In Russland können die Anforderungen an Datenlokalisierung personenbezogener Daten russischer Staatsbürger ebenso wie die Anforderungen an die Nutzung lokaler Internetknoten eine beachtliche Beschränkung darstellen. Unternehmen benötigen eine klare Strategie, wie sie mit diesen (lokalen) Beschränkungen umgehen und ggf. ihre Geschäftsmodelle anpassen können.

In den USA bestehen grundsätzlich keine erheblichen regulatorischen Beschränkungen, die sich unmittelbar auf Digitalisierungsvorhaben im Bereich des Maschinen- und Anlagenbaus auswirken. Allerdings können Regelungen der Ausfuhrkontrolle und Handelssanktionen sich mittelbar auf grenzüberschreitend angelegte Datenaustauschvorhaben – insbesondere mit Blick auf die einzusetzenden Verschlüsselungstechnologien – auswirken, wenn diese aus den USA stammen und auch in den Zielmärkten Russland und China eingesetzt werden sollen.

Insgesamt zeichnet sich ab, dass global agierende Unternehmen im digitalen Umfeld nicht auf eine einzige international anwendbare Lösung setzen sollten, sondern ihre Lösungen spezifisch auf die jeweiligen Märkte und deren regulatorische Anforderungen ausrichten bzw. in Kooperation mit lokalen Partnerunternehmen treten müssen.

# II. Ausgangslage und Zielsetzung der Studie

Mit seiner starken Exportorientierung gehören für den Maschinen- und Anlagenbau China, dicht gefolgt von den USA, zu den wichtigsten Absatzmärkten.[5] Mit ihrer Initiative „Made in China 2025“ hat die Volksrepublik China zudem ihren wachsenden Bedarf an qualitativ hochwertigen Maschinen signalisiert.[6] Für Anwender und Anbieter von Industrie 4.0 Lösungen kommt es, neben freien Marktzugängen im Allgemeinen, insbesondere auf möglichst ungehinderten Datenaustausch an.[7] Nur so können die mit der Digitalisierung beabsichtigen Vorteile – Effizienzsteigerung durch Verfügbarkeit der Informationen in Echtzeit, Flexibilität durch transparente Abläufe und die Entwicklung neuer Dienste und Funktionen – in den jeweiligen Zielmärkten und durch Anbindung an die Herkunftsländer der betreffenden Produkte und Dienste realisiert werden. Protektionistische Maßnahmen wurden besonders im Bereich der Digitalisierung bereits in zahlreichen Ländern getroffen, andere Maßnahmen befinden sich noch in der Vorbereitungsphase.

Unternehmen des Maschinenbaus müssen die verschiedenen Regulierungsansätze zum Thema Datenverarbeitung vor Augen haben, um sich auf Digitalisierungsbarrieren in den Zielmärkten einzustellen: In China und Russland zielen regulatorische Maßnahmen vorwiegend auf die Kontrolle bzw. Kontrollierbarkeit von Daten ab; in der EU liegt der Fokus auf dem Schutz von (personenbezogenen) Daten und in den USA werden Daten primär als kommerzialisierbares Handelsgut begriffen. Daraus resultieren Hindernisse, die sich im Zusammenhang mit der Digitalisierung konkret auswirken. Im Rahmen der Studie beleuchtet Bird & Bird LLP, welche Barrieren bereits existieren, bzw. für die nahe Zukunft geplant sind und wie sich diese auf global tätige Unternehmen im Maschinen- und Anlagenbau auswirken können.

Ziel dieser Studie ist es, bereits verabschiedete oder in Erarbeitung befindliche regulatorische Digitalisierungshemmnisse in den relevanten Märkten EU, China, Russland und den USA aufzuzeigen, den praxisbezogenen Einfluss dieser Hemmnisse auf Unternehmen des Maschinen- und Anlagenbaus einzuschätzen und Handlungsempfehlungen an die Industrie und Politik auszusprechen.

# III. Vorgehensweise

Die Studie nimmt die „**Use Cases**" Remote Access, Condition Monitoring und Datenaustauschplattformen in den Fokus und untersucht diese anhand verschiedener Prüffelder.[8] Die Studie orientiert sich dabei vornehmlich an der Interessenlage exportorientierter Unternehmen des deutschen Maschinen- und Anlagenbaus. Die Studie beabsichtigt, Handlungsempfehlungen für die Unternehmen hinsichtlich geeigneter Herangehensweisen und möglichen Gestaltungsspielräumen im Umgang mit Digitalisierungsbarrieren aufzuzeigen, aber auch anzusprechen, an welchen Stellen der VDMA im Rahmen seiner übergreifenden Interessenvertretung und die zuständigen politischen Handlungsträger im internationalen Rahmen helfen und unterstützen sollten.

**Relevante Use Cases**

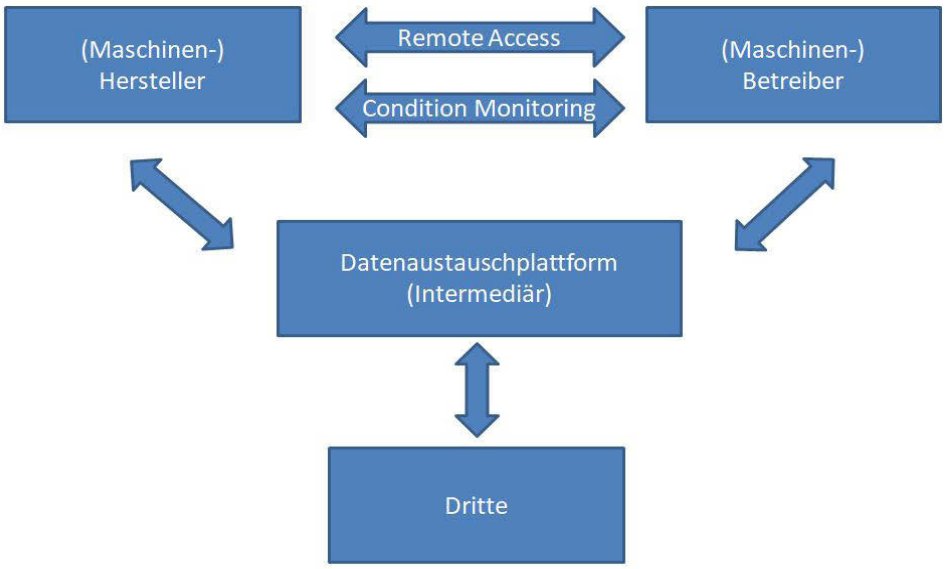
- Beim Fernzugriff („**Remote Access**") können (industrielle) Nutzer, also sowohl die Hersteller als auch die Betreiber (als Kunden), von internetfähigen Geräten mit einer räumlich entfernten Maschine Kontakt aufnehmen und – je nach Berechtigung des Nutzers – Daten einsehen sowie mit spezieller Einwilligung auch technisch eingreifen und Anweisungen erteilen („*schaltender Zugriff*"). Remote Access ermöglicht die globale Fernwartung von Maschinen („**Remote Maintenance**").

- Mit der Zustandsüberwachung („**Condition Monitoring**") können die Hersteller ihre Maschinen präzise und effizient überwachen und durch die ggf. in Echtzeit analysierten Daten ein verlässliches Wartungs- und Sicherheitssystem etablieren. Mittels vorausschauender Wartung werden Maschinen und Anlagen proaktiv gewartet, um Ausfallzeiten niedrig zu halten („**Predictive Maintenance**"). Dabei werden häufig im Rahmen des Condition Monitoring in den Maschinen enthaltene oder generierte sensitive Informationen übertragen. Remote Access ist die Voraussetzung für Condition Monitoring, weswegen die beiden Use Cases nur schwer voneinander abzugrenzen sind und Grenzen zwischen diesen beiden Use Cases oft verschwimmen. Gleiches gilt für den Aspekt der Datenkommunikation auch für die unterschiedlichen Wartungsformen, z. B. Remote Maintenance und Predictive Maintenance.

- Bei einem (Technologie-)Datenmarktplatz („**Datenaustauschplattform**") findet ein übergreifender Datenaustausch zwischen unterschiedlichen Akteuren statt. Daten fließen nicht nur bilateral von einem Hersteller zu einem oder mehreren Betreibern und umgekehrt. Vielmehr tritt ein Intermediär (als Datenaggregator, Diensteanbieter) zwischen die Anbieter und Anwender von datenbasierten Diensten (also z. B. den Maschinenhersteller und den Maschinenbetreiber), um einen mehrseitigen, multipolaren Markt unterschiedlicher Datenanbieter und Datennutzer einschließlich weiterer Endnutzer (bis hin zu B2B2C Nutzungsmodellen) zu realisieren.

  Remote Access und Condition Monitoring sind bereits seit vielen Jahren praktischer Alltag für eine Mehrzahl der Maschinen- und Anlagenbauer. Allerdings zeichnet sich im Zuge der Digitalisierung auf breiterer Basis die Relevanz eigenständiger Geschäftsmodelle mit zusätzlichen Dienstangeboten und einem damit verbundenen eigenständigen Wertschöpfungsbeitrag ab. Entsprechend stärker fallen auch etwaige regulatorische Hemmnisse ins Gewicht.

**Abbildung 1: Datenströme**




**Durchführung einer Befragung zu Digitalisierungsbarrieren**
Im Rahmen der Studie führte Bird & Bird LLP in Zusammenarbeit mit der IMPULS-Stiftung eine nicht repräsentative Befragung durch, die erste Einblicke in die Praxis der Unternehmen und Erkenntnisse darüber liefern konnte, was die Befragten im Hinblick auf die zunehmende Digitalisierung beschäftigt. In der Zeit von Oktober 2018 bis Januar 2019 wurden 28 Verbandsmitglieder des VDMA mithilfe eines Fragebogens u. a. zu Angaben über grenzüberschreitenden Datenaustausch mit ihren Kunden befragt. Die Befragung lieferte indikative Erkenntnisse zum aktuellen und geplanten Digitalisierungsstand der Unternehmen, die durch Einzelgespräche mit ausgewählten Unternehmen weiter vertieft wurden. Des Weiteren führten Bird & Bird LLP und die IMPULS-Stiftung im Januar 2019 einen Workshop mit ausgewählten Unternehmen durch, um Erkenntnisse aus unterschiedlichen Marktsegmenten des Maschinen- und Anlagenbaus zu beleuchten und konkrete Erfahrungen mit Digitalisierungsbarrieren beispielhaft in diese Studie einfließen zu lassen.

# IV. Relevante Datenkategorien

Mit Blick auf die unterschiedlichen gesetzlichen Regelungen zu personenbezogenen und nicht-personenbezogenen Daten differenziert diese Studie zwischen den unterschiedlichen Datenkategorien.

Entgegen dem Schwerpunkt der öffentlichen und unternehmerischen Diskussion, der seit der im Mai 2018 in Kraft getretenen Europäischen Datenschutz-Grundverordnung (DS-GVO) vorwiegend auf personenbezogenen Daten liegt, setzt die Studie ihren Schwerpunkt auf Maschinendaten, die keinen Personenbezug aufweisen.[9]

## 1. Maschinendaten

Der Fokus dieser Studie liegt auf Maschinendaten, die im Rahmen der eigenen Produktion der Unternehmen bzw. bei der Bereitstellung eigener Produkte und Dienstleistungen bei den Kunden anfallen bzw. erhoben und verarbeitet werden. Maschinendaten sind die von einer Maschine automatisch erzeugten Daten über deren Zustand, Funktionsprozesse, Bedienung und alle weiteren maschineninternen Vorgänge, welche digital verarbeitet, gespeichert und weitergeleitet werden.[10] Darunter fallen etwa diejenigen Daten und Messwerte, die beim Maschinenlauf wie auch in Stillstandphasen anhand der Sensorik erzeugt und erfasst werden und die ggf. zur Überwachung und Optimierung

**Abbildung 2: Beispiele für Maschinendaten in der Automatisierungstechnik**


Quelle: Präsentation des AK Steuerungstechnik des VDMA, Industrie 4.0 – Wertschöpfung aus Maschinendaten, Claus Kühnl, 25.02.2019.

des Maschineneinsatzes genutzt werden, wie auch z. B. Wartungsdaten von Industrierobotern.[11] Zudem kann dies auch Daten aus anderen Systemen, z. B. aus ERP-Systemen oder CAD-Systemen, erfassen, die ggf. in geschützten Bereichen liegen und über geeignete Datenaustauschmittel auf die Anlage übertragen werden.

Unter dem Oberbegriff der Maschinendaten sind unterschiedliche Datenkategorien zu verstehen.[12] Neben den in Abbildung 2 beschriebenen Datenkategorien zählen auch „Konfigurationsdaten" zu den Maschinendaten. Konfigurationsdaten enthalten Parameter, mit denen eine Maschine für eine bestimmte Art der Bearbeitung oder ein bestimmtes Material konfiguriert werden kann.[13] Bei Laserschneidmaschinen sind dies beispielsweise Fokuspunkt, Vorschubgeschwindigkeit oder Schneidgaszufuhr. Bei der Auslieferung einer Maschine steht oft nur ein Grundumfang an Konfigurationsdaten für Standard-Anwendungen zur Verfügung. Für weitere Anwendungen der Maschine müssen die notwendigen Konfigurationsdaten selbst entwickelt oder von Dritten beispielsweise über eine Datenaustauschplattform bezogen werden.[14]

Konfigurationsdaten stellen die Grundlage für die Durchführung und Steuerung des eigentlichen technologischen Bearbeitungsprozesses in den Produktionsstätten dar. Ändern sich Randbedingungen wie Rohmaterial, geforderte Prozessqualität oder Bearbeitungsgeschwindigkeit, so sind Anpassungen oder auch neue Konfigurationsdatensätze notwendig. Diese Daten sind typischerweise das Ergebnis umfangreicher Testläufe und Erprobungen.

## 2. Personenbezogene Daten

„Personenbezogene Daten" sind mit der Definition der DS-GVO grundsätzlich alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DS-GVO). Eine natürliche Person ist dann identifizierbar, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung (z. B. Namen, Kennnummer, Standortdaten) oder anderen Merkmalen identifiziert werden kann. Ähnliche Definitionen finden sich auch in anderen Rechtsordnungen weltweit.[15]

Im Bereich des Maschinen- und Anlagenbaus stellen sich personenbezogene Daten typischerweise eher als „Beifang" dar. Allerdings spielen sie z. B. zum einen immer dann eine Rolle, wenn es um die Verwaltung einzelner Teilnehmer und Akteure auf einer Datenaustauschplattform geht, wie etwa beim Account-Management von Teilnehmerregistrierungen auf der Kundenseite (Account-Management etwa bzgl. Nutzerkonten, NutzerIDs oder personalisierten Log-In-Daten), sowie zum anderen auch immer dann, wenn z. B. über die Plattformen Aufzeichnungen von Maschinenlaufzeiten in Verbindung mit einer Mensch-Maschine-Interaktion zum Tragen kommen (bei rein unternehmensbezogenen Internet of Things (IoT)-Anwendungen entfällt dies wiederum). Im Rahmen des Remote Access und Condition Monitoring ist ebenfalls die Verarbeitung personenbezogener Daten insbesondere bei Zugriffen auf die Schnittstelle der

Mensch-Maschine-Kommunikation besonders relevant. Sowohl bei Dienstleisterunternehmen, also Unternehmen, die Remote Access und Condition Monitoring durchführen, als auch bei Kundenunternehmen, also Unternehmen, auf deren Maschinen mittels Remote Access und Condition Monitoring zugegriffen wird, fallen wie im Rahmen der Datenaustauschplattform personenbezogene Daten an, wenn die Zugriffe auf die Maschinen und Anlagen bzw. deren Nutzung mit einzelnen Nutzern verknüpft werden kann (z. B. wie oben beschrieben über Nutzerkonten, etc.). Zudem erfordern gerade die Datensicherheitsanforderungen oder Compliancеregeln eines Unternehmens eine klare Nachvollziehbarkeit, welche Nutzer zu welchem Zeitpunkt auf bestimmte Maschinen zugegriffen haben oder bestimmte Einstellungen vorgenommen haben.

Aus datenschutzrechtlicher Sicht ergeben sich daraus einige Maßgaben: Unternehmen sollten sicherstellen, dass sie individualisierte Accounts und NutzerIDs nur dort einsetzen, wo dies zwingend erforderlich ist, um die Verarbeitung personenbezogener Daten einzugrenzen. Des Weiteren sollten Maschinen- und Anlagenbauer die Möglichkeiten der Pseudonymisierung von personenbezogenen Daten – insbesondere solcher, die im „Beifang“ anfallen – sorgfältig prüfen.[16]

# V. Relevante Use Cases

## 1. Einführung

Maschinen- und Anlagenhersteller überwachen je nach Digitalisierungsgrad schon seit langem oder nun vermehrt ihre Maschinen bzw. Produkte und befassen sich zunehmend mit datengetriebenen Geschäftsmodellen mittels Auswertung von Maschinendaten. Wenn auch dieser Digitalisierungsprozess bei weitem nicht abgeschlossen ist (und etliche Unternehmen damit auch erst am Anfang stehen), stellt er für kleine und mittlere Unternehmen (KMU) eine erhebliche Herausforderung dar, die ggf. durch regulatorische Digitalisierungsbarrieren in den Zielmärkten EU, China, Russland und USA zusätzlich belastet wird.[17]

Zugleich nimmt der Druck zur Umstellung auf digitalisierte Produktionsabläufe und den Einsatz digitalisierter Produkte stetig zu. Die Teilnehmer der Befragung zu dieser Studie ließen erkennen, dass sie sowohl der Digitalisierung der eigenen Produktionsabläufe wie auch der Digitalisierung der kundenseitig angebotenen Produkte und Dienstleistungen über die nächsten 5 Jahre eine entscheidende Bedeutung zuweisen.

Die Digitalisierung wird unter anderem durch den Einsatz von Cloud-Technologie als skalierbare IT-Infrastruktur, RFID, Sensorik, mobilen Endgeräten, Real-Time-Location-Systemen, Big Data zur Speicherung und Auswertung von Echtzeitdaten, integrierten Mensch-Maschine-Benutzerschnittstellen (HMI), Augmented Reality, Maschine-zu-Maschine-Kommunikation, integrierten Lieferketten durch Datenaustausch, eingebetteten IT-Systemen, digitalen Zwillingen oder Interoperabilität vorangetrieben.

In Erweiterung ihrer bewährten Geschäftsmodelle (Produktverkauf und darauf bezogene Wartungs- und Reparaturleistungen) richten innovationsorientierte Maschinen- und Anlagenbauer ihr Augenmerk auf neue (datenbasierte) Geschäftsmodelle, indem sie verstärkt IT- und Software-Lösungen in den Produkten selbst durch Cyber-Physical-Systems, Auswertung von Maschinendaten und produktbezogene IT-Services vorsehen, um einer sich ändernden Nachfrage nach neuen digitalen Lösungen zu entsprechen. Mit intelligenten Lösungen können die Betreiber ihre Kosten reduzieren und ihre Produktivität steigern, wenn z. B. Predictive Maintenance dazu führt, dass der Betreiber seine Ersatzteillagerbestände herunterfahren kann oder Stillstandzeiten der Anlage vermieden werden können.

Des Weiteren kann die Digitalisierung und Vernetzung von Maschinen dabei helfen, Funktionen der Maschine vor Plagiaten zu schützen, wenn diese z. B. aus einer geschützten Cloud bezogen werden. Dies kann zu einem Know-how-Schutz ausgebaut werden, wenn z. B. Software nur über eine Cloud genutzt werden kann und somit keine Weitergabe erfolgt, die für Reengineering missbraucht werden könnte. Für den Maschinen- und Anlagenbau könnte z. B. das Ersatzteilgeschäft eines Herstellers geschützt werden, indem vernetzte Maschinen nur mit freigegebenen Ersatzteilen funktionieren oder eine Onlinefreigabe der verbauten Ersatzteile durch den Hersteller zur Nutzung des Ersatzteils erforderlich ist. Weiterhin könnten Regressansprüche an den Hersteller online daraufhin überprüft werden, ob z. B. falsche Ersatzteile verbaut wurden oder die Maschine bestimmungsgemäß verwendet wird.

## 2. Remote Access

Mittels Remote Access können Maschinenhersteller und Maschinenbetreiber effizient auf weltweit verteilte Maschinen und Anlagen (z. B. in Niederlassungen oder bei Kunden) zugreifen. Durch Remote Access ist die Bedienung der Maschinen und Anlagen nicht mehr ausschließlich ortsgebunden, sondern kann von jedem z. B. mittels Internet verbundenen Geräts ausgeführt werden. Durch Remote Access können unter anderem Installations-, Inbetriebnahme-, Diagnose- und Servicearbeiten schneller und effizienter als bisher durchgeführt werden. Je nach Konfiguration und dem tatsächlichen Zugriff müssen sich Nutzer entsprechend dem Konzept von „Industrie 4.0“ künftig nicht mehr manuell mit den Maschinen und Anlagen verbinden, sondern können diese aus der Ferne nach Bedarf direkt ansteuern. Sie führen dann – so die Vision – mithilfe von integrierten Wissensplattformen und Virtual-Reality-Tools Remote Maintenance effizienter durch. Je nach Konfiguration des Remote Access können die unterschiedlichen

mittels Remote Access zur Verfügung stehenden Dienstleistungen, z. B. zyklische Wartung, Inspektion oder Reparaturunterstützung, einzeln zu- und abgeschaltet werden. Gerade klein- und mittelständische Unternehmen führen die verschiedenen Dienste oft nicht in optimaler und damit sicherer Weise zusammen, sondern verbinden beispielsweise pragmatisch einen VPN-Tunnel mit einem Remote-Desktop.

Einer der Schlüsselfaktoren beim Remote Access ist, eine sichere Verwaltung der Kommunikationsbeziehungen zwischen der Zentrale, den installierten Anlagen und ggf. den Servicetechnikern zu gewährleisten. Die Verwaltung sicherer Verbindungen geht dabei Hand in Hand mit der Gewährleistung sicherer digitaler Identitäten. In der Regel wird vor dem Zugriff auf die Maschine die Identität der Teilnehmer ermittelt (z. B. über einen Zertifikatsaustausch), um einen unautorisierten Zugriff auf das Firmennetzwerk, in dem die Anlage oder Maschine eingebunden ist, zu unterbinden und dadurch die Sicherheit zu erhöhen. Hier kommt es ggf. auch zu einer Verarbeitung personenbezogener Daten, wenn über die jeweiligen Nutzerkonten oder Nutzer-IDs einzelne natürliche Personen identifiziert werden können. Der Einsatz ausreichender Verschlüsselung ist dafür von wesentlicher Bedeutung, um die Vertraulichkeit und Integrität des Firmennetzwerkes und der übermittelten Informationen effektiv zu schützen, muss aber zugleich etwaigen regulatorischen Anforderungen (aus Exportkontrolle oder Sicherheitsvorschriften) genügen.

## 3. Condition Monitoring

Mit dem Condition Monitoring verfolgen Maschinen- und Anlagenbauer in der Regel zwei Ziele: Maschineneffizienz und Betriebssicherheit. Durch Condition Monitoring ist eine präzise und effiziente Instandhaltung der betreffenden Maschinen möglich. Das Condition Monitoring ist zwingende Voraussetzung für eine zustandsorientierte Instandhaltung und löst die bisher übliche reaktive oder präventive Instandhaltung ab. Bei Letzterer wurde die betreffende Maschine in festen Zeitabständen heruntergefahren, um Bauteile zu überprüfen bzw. auszutauschen. Dabei wurden häufig intakte Bauteile ausgetauscht und somit vorhandene Restlaufzeiten verschenkt.

Mittels Condition Monitoring können unterschiedliche Faktoren, z. B. Zeitabläufe an der Maschine und Systemvariablen wie Motorströme und Temperaturverläufe, aufgezeichnet werden. Durch einen Abgleich von Referenzverlauf und aktuellem Systemzustand können Abweichungen schnell erkannt und an die Maschinenbetreiber oder Bediener gemeldet werden. Hierdurch können Maschinenhersteller und -betreiber eingreifen, bevor die Maschine ausfällt.[18] Insbesondere beim Einsatz von Maschinen verschiedener Hersteller, für die eine bestimmte Verfügbarkeit gewährleistet werden muss, ist Condition Monitoring essenziell.

Stillstandzeiten der Maschinen entstehen nicht nur bei Wartungs- und Störungszeiten, sondern auch beim Rüsten und Umrüsten. Dabei muss eine gewisse Anlagenverfügbarkeit beständig gewährleistet werden. Ungeplante Stillstände können durch eigenständige Instandhaltung des Maschinenbedieners und durch progressive Instandhaltung mittels Wartungsplänen vermieden werden. Durch Condition Monitoring werden Instandhaltungstätigkeiten besser und länger im Voraus planbar und die Maschinenverfügbarkeit verbessert.

Basierend auf den ggf. in Echtzeit analysierten Daten kann ein schnell reagierendes automatisches Sicherheitssystem, z. B. eine Notabschaltung, realisiert werden. Zudem ermöglicht Condition Monitoring eine anschließende und umfassende Analyse der Störfaktoren, die das Sicherheitssystem ausgelöst haben.

## 4. Datenaustauschplattform

Der Begriff „Datenaustauschplattform“[19] beschreibt im Kern eine Plattform für einen (produktions-, fabrik- und/oder unternehmens-) übergreifenden Datenaustausch zwischen unterschiedlichen Akteuren.[20] Die Datenaustauschplattform ermöglicht es, die für einen Herstellungsprozess benötigten oder dort entstandenen Daten bedarfsgerecht in einem Ökosystem auch Dritten zur Verfügung

zu stellen und diese ggf. zu handeln bzw. zu monetarisieren. Nicht bei allen Datenaustauschplattformen steht jedoch der Handel mit Daten im Vordergrund. Ziel kann etwa auch sein, dass ein Unternehmen seine Daten für „Forschung und Entwicklung" zur Verfügung stellt und dafür keine monetäre Gegenleistung erhält. Daneben ist über Datenaustauschplattformen auch der Austausch von Maschinenfunktionen vorstellbar, die vom jeweiligen Anbieter, in der Regel dem Maschinenhersteller, in einer Cloud gepeichert und den Maschinenbetreibern direkt aus der Cloud zur Verfügung gestellt werden.

Datenaustauschplattformen werden von Unternehmen des Maschinen- und Anlagenbaus bislang nicht vergleichbar intensiv eingesetzt, wie dies für die anderen beiden Use Cases der Fall ist. Das Bundesministerium für Wirtschaft und Energie sieht jedoch Plattformen als zentrale Knoten für die Entwicklung der Wirtschaft.[21] Auch das Förderprogramm der EU Kommission hat ausdrücklich die Entwicklung der nächsten Generation digitaler industrieller Plattformen hervorgehoben, u. a. um die Entwicklung intelligenter Fabriken voranzubringen.[22] Die Politik setzt damit einen klaren Schwerpunkt, mit dem sich Maschinen- und Anlagenbauer auseinandersetzen sollten, um die möglichen Potentiale von Datenaustauschplattformen künftig voll ausnutzen zu können.

Durch die Einführung einer Datenaustauschplattform kann der Aufwand der Erfassung von Maschinendaten, z. B. Anschaffung und Aufrechterhaltung von Anlagen zur digitalen Speicherung von Maschinendaten, erheblich reduziert werden. Ähnlich wie in einem App-Store können die benötigten Daten und Maschinenfunktionen (aus der Sicht des Maschinenbetreibers) über eine Cloud-basierte Plattform abrufbar gehalten, bedarfsgerecht lizenziert und auf der Maschine verwendet werden.[23] Mit zunehmendem Ausbau von datenbasierten Geschäftsmodellen auch im Maschinen- und Anlagenbau können über eine Datenaustauschplattform neben Daten ggf. auch bestimmte Anwendungen bereitgestellt oder auf der Plattform von den Beteiligten entwickelt werden.[24]

Der Betreiber einer Datenaustauschplattform muss dabei nicht zwangsläufig ein neutraler Dritter sein. So gibt es bereits mehrere praktische Beispiele in denen der Maschinenhersteller eine Plattform für Kunden (d. h. Maschinenbetreiber) und Lieferanten (z. B. Komponentenhersteller) bereitstellt, um – neben dem übergreifenden Ziel der Vernetzung der Produktion entlang der gesamten Lieferkette – neue Dienste und Mehrwert für seine Kunden zu schaffen. Dies gilt jedenfalls dann, wenn der Kunde selbst keine Datenanalysen durchführen möchte, sondern auf die technische Befähigung und das Expertenwissen (etwa durch Big Data Analytics) des Maschinenherstellers vertraut. Aber auch die entgegengesetzte Konstellation ist in praktischer Umsetzung: Der Kunde bzw. Maschinenbetreiber stellt eine Datenaustauschplattform bzw. Schnittstellen bereit, um dem Maschinenhersteller bestimmte Funktionalitäten wie das Aufzeichnen und Auswerten von Daten nur gegen Bezahlung zu gestatten.

Im Bereich des Maschinen- und Anlagenbaus gibt es bereits eine ganze Reihe von proprietären Plattformen, die sich um den Aufbau des entsprechenden Ökosystems bemühen und möglichst viele Marktbeteiligte veranlassen möchten, ihre Daten in die Plattform einzubringen.[25] Maßgeblich für die Bereitschaft zum Teilen von Daten ist dabei vor allem Vertrauen der Datenerzeuger, z. B. der Maschinenbetreiber, in den Plattformbetreiber und die Nutzungsberechtigten, welches durch hohe Sicherheitsstandards und eine effektive Nutzungskontrolle abgesichert werden muss. Der Plattformbetreiber muss dazu sicherstellen, dass der Datengeber die Steuerung („*Usage Control*") über die von ihm eingebrachten Daten behält, sowohl durch passende vertragliche Datennutzungsvereinbarungen als auch die Möglichkeit eines Widerrufs bzw. der Rückübertragung der von ihm eingebrachten Daten.[26]

# VI. Überblick Prüffelder

Die folgenden abstrakten Digitalisierungsbarrieren bilden den Rahmen für die Prüfung. Die Studie untersucht, ob und ggf. welche der aufgeführten Digitalisierungsbarrieren mit Blick auf die relevanten Märkte EU, China, Russland und die USA zum Tragen kommen bzw. auf die Umsetzung der einzelnen Use Cases Einfluss nehmen und sich damit ggf. als regulatorische Hemmnisse darstellen.

Auf sektorspezifische Zusatzregelungen, z. B. besondere Anforderungen für die Hersteller von Medizinprodukten oder strengere Hygienevorschriften in der Lebensmittelproduktion, geht diese Studie nicht ein. Es ist also möglich, dass ein Unternehmen des Maschinen- und Anlagenbaus weitere branchenspezifische Regulierung im Blick haben muss.

## Methodik

**Prüffelder**
Zu Beginn der Studie wurden sieben Prüffelder bestimmt, aus denen sich Digitalisierungsbarrieren in den einzelnen Märkten ergeben könnten. Die folgenden Prüffelder sind zunächst nur abstrakt umrissen, um ihre Relevanz in den einzelnen Zielmärkten näher zu beleuchten.

| Prüffeld | EU | China | Russland | USA |
|---|---|---|---|---|
| Schutz von Geschäftsgeheimnissen | 🟡 | 🔴 | ○ | 🟢 |
| Schutz Kritischer Infrastrukturen | 🟡 | 🟡 | 🔴 | ○ |
| Vorschriften zur Datenlokalisierung | 🟢 | 🟡 | 🔴 | 🟢 |
| Datenschutzrecht | 🔴 | 🔴 | ○ | 🟡 |
| Regelungen der nationalen Sicherheit | ○ | ○ | 🔴 | ○ |
| Einfuhr- / Ausfuhrkontrollbestimmungen | 🟡 | 🔴 | 🟡 | 🟡 |
| Handelssanktionen | 🟢 | ○ | ○ | 🔴 |

- 🔴 Starke Auswirkungen
- 🟡 Mögliche Auswirkungen im Einzelfall zu prüfen, Änderungen beobachten
- 🟢 Aktuell keine oder wenige Einschränkungen
- ○ Die freien Feldern werden für den jeweiligen Zielmarkt im Rahmen dieser Studie nicht besprochen.[27]

**Zielmärkte**
Die Studie legt den Fokus auf vier Zielmärkte mit besonderer Relevanz für den Maschinen- und Anlagenbau: die EU, China, Russland und die USA. Während der Ausarbeitung der Studie wurde deutlich, dass bestimmte Prüffelder für einzelne Zielmärkte keine oder nur geringe Relevanz haben. In den Kapiteln zu den einzelnen Zielmärkten werden deswegen nur diejenigen Prüffelder thematisiert, die aus Sicht der im Rahmen der Studie befragten Unternehmen und Experten sowie nach dem Gesamteindruck von Bird & Bird LLP zum Zeitpunkt der Veröffentlichung der Studie für den Maschinen- und Anlagenbau – gegenwärtig oder in naher Zukunft – von besonderer Bedeutung sind.

## 1. Schutz von Geschäftsgeheimnissen

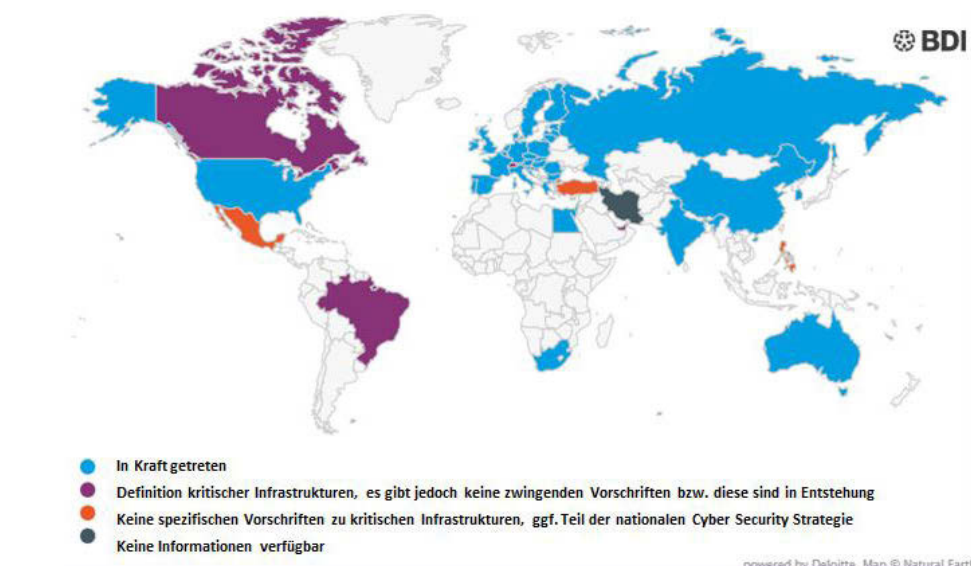
Der Schutz von Geschäftsgeheimnissen ist heterogen geregelt und an unterschiedliche Voraussetzungen geknüpft, wie dies z. B. im Rahmen der Umsetzung der EU „Trade Secrets Richtlinie“ einschließlich der Anforderung an die Implementierung angemessener Geheimhaltungsmaßnahmen zum Tragen kommt.[28] Die Anforderungen an diese Geheimhaltungsmaßnahmen können unter Umständen Digitalisierungsbarrieren darstellen, wenn das Schutzniveau in einem Land niedriger liegt als dies – aus Sicht europäischer Unternehmen – zu Hause der Fall ist.

## 2. Schutz Kritischer Infrastrukturen

Kritische Infrastrukturen sind Einrichtungen, Anlagen oder Teile davon, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind. Durch ihren Ausfall oder ihre Beeinträchtigung würden erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten. Infrastrukturen im Allgemeinen und Kritische Infrastrukturen im Besonderen sind die unverzichtbaren Lebensadern moderner, leistungsfähiger Gesellschaften. Hierzu zählen beispielsweise: Energie- und Wasserversorgung, Transport und Verkehr, Informationstechnik und Telekommunikation und medizinische Versorgung. Die Gewährleistung des Schutzes dieser Infrastrukturen ist eine Kernaufgabe staatlicher und unternehmerischer Sicherheitsvorsorge. Maschinenhersteller und insbesondere Maschinenbetreiber, die in diesen Bereichen tätig sind, unterliegen möglicherweise strengen Regelungen hinsichtlich von Datensicherheitsanforderungen und Meldepflichten.

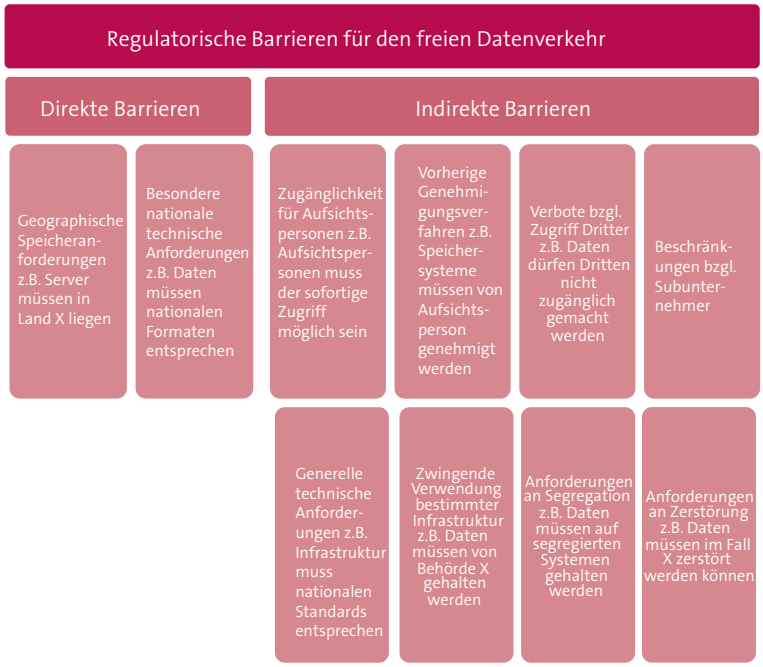
Ob Unternehmen als Betreiber von Kritischen Infrastrukturen betrachtet werden, ergibt sich aus den jeweiligen landesspezifischen gesetzlichen Regelungen. Mit Ausnahme der USA gibt es in sämtlichen Zielmärkten Regelungen zum Schutz Kritischer Infrastrukturen (siehe Abbildung 3).

**Abbildung 3: Übersicht Regelungen zum Schutz Kritischer Infrastrukturen**




Quelle: BDI und Deloitte. 2019. Cyber Landscapes; https://bdi.eu/themenfelder/digitalisierung/cyber-landscapes/.

**Abbildung 4: Regulatorische Hemmnisse für den freien Datenfluss**




Quelle: Studie zu "Cross-border data flow in the Digital Single Market: data localisation restrictions", S. 5 (SMART 2015/0054).

## 3. Vorschriften zur Datenlokalisierung

Vorschriften zur Datenlokalisierung legen fest, dass bestimmte Datensätze oder Datenarten (z. B. personenbezogene Daten) lokal, d. h. in einem bestimmten Land, vorgehalten werden müssen. Soweit Datenlokalisierungsvorschriften bestehen, dienen sie in der Regel dem Ziel, die Zugriffsmöglichkeit lokaler Behörden zu gewährleisten oder jedenfalls zu erleichtern.[29]

Für Maschinen- und Anlagenbauer kann daraus folgen, dass sie die Daten entweder ausschließlich durch eine eigene Niederlassung oder in Zusammenarbeit mit einem externen lokalen Partner, etwa dem Betreiber eines Rechenzentrums vor Ort, lokal halten müssen. Selbst wenn lokalisierte Daten in kopierten Datensätzen gespiegelt und ggf. an die Muttergesellschaft (etwa in Deutschland) übertragen werden dürfen (wie in Russland), um eine weitergehende zentralisierte Datenverarbeitung zu ermöglichen, führt dies typischerweise zu höheren Kosten und kann sich damit mittelbar als Markteintrittsbarriere auswirken.[30] Neben dem unmittelbaren Aufwand zur Umsetzung regulatorischer Vorgaben können Einschränkungen in der Nutzung skalierbarer Technologie zur grenzüberschreitenden Datenverarbeitung Kostennachteile begründen; zudem steht das finanzielle Risiko aus Sanktionen im Fall der Nichteinhaltung regulatorischer Vorgaben im Raum.[31]

Auf die einzelnen Erscheinungsformen von Datenlokalisierungspflichten wird im Rahmen dieser Studie nur insoweit eingegangen, als diese Relevanz für den Maschinen- und Anlagenbau haben. Datenlokalisierungsvorschriften greifen in der Regel nicht umfassend, sondern nur für bestimmte Datenkategorien. Dabei handelt es sich überwiegend um Datenkategorien, die aus regulatorischer und unternehmerischer Sicht als sensibel betrachten werden und die für (Aufsichts-)Behörden der einzelnen Mitgliedstaaten einfach verfügbar sein sollen. Die bestehenden Datenlokalisierungsvorschriften greifen dabei vorrangig in Bezug auf Daten von Kreditinstituten (z. B. Luxemburg), Steuerunterlagen (z. B. Deutschland) oder Daten öffentlicher Einrichtungen (z. B. Spanien).[32] Im Fall von Maschinendaten

greifen Datenlokalisierungsvorschriften in der Regel nur, soweit diese mit personenbezogenen Daten verknüpft sind.

## 4. Datenschutzrecht

Im Anwendungsbereich der DS-GVO, d. h. innerhalb der EU/dem Europäischen Wirtschaftsraum (EWR), ist grenzüberschreitend die Verarbeitung und der Austausch personenbezogener Daten unproblematisch möglich, soweit den allgemeinen Anforderungen an die Datenverarbeitung genügt wird (Art. 5, 6 ff. DS-GVO). Potentielle Digitalisierungsbarrieren können sich jedoch bei Übermittlungen personenbezogener Daten aus und in Drittländer, d. h. Länder außerhalb des EWR, ergeben. Dabei greifen Datenschutz und Datenlokalisierungsvorschriften (siehe oben VI.3) oft ineinander.

Aus den Regelungen des Beschäftigtendatenschutzes, soweit für die Datenerhebung in der industriellen Fertigung relevant, können sich gesonderte Digitalisierungsbarrieren ergeben.

Das Datenschutzrecht ist auf die Verarbeitung personenbezogener Daten beschränkt, also solcher Daten, die eine natürliche Person identifizieren oder identifizierbar machen. Personenbezogene Daten sind insbesondere dann Teil von Maschinendaten, wenn sich im Rahmen des Condition Monitoring Rückschlüsse auf das Verhalten und die Leistung von jenen Mitarbeitern ergeben, die die Maschinen bedienen. Bei der Kombination von personenbezogenen und nicht-personenbezogenen Daten, d. h. bei „gemischten Datensätzen", in denen die Daten untrennbar miteinander verbunden sind, greifen die Regelungen des Datenschutzrechts auch dann, wenn die personenbezogenen Daten nur einen kleinen Teil des jeweiligen Datensatzes ausmachen.[33] Gemischte Datensätze sind z. B. Analysen von Betriebslog-Daten von Produktionsanlagen der verarbeitenden Industrie.[34]

In der Folge bedarf es entweder einer Anonymisierung der verarbeiteten Daten, um diese außerhalb des Anwendungsbereichs des Datenschutzes verwenden zu können, oder besonderer technischer und organisatorischer Maßnahmen, um personenbezogene Daten ausreichend zu schützen. Hierunter fallen neben regulären IT-Sicherheitsmaßnahmen (z. B. Passwortschutz) auch die Verschlüsselung und Pseudonymisierung der personenbezogenen Daten, sowohl bei Übertragung als auch bei Speicherung.

## 5. Regelungen der nationalen Sicherheit

Des Weiteren gibt es eine Vielzahl von Regelungen zu Datenlokalisierungsvorschriften aus Gründen der nationalen Sicherheit, Maßnahmen der Gefahrenprävention und Strafverfolgung.[35] Dies ist z. B. für bestimmte Datenarten und Datenbanken im Bereich des Polizei- und Ordnungsrechts der Fall.[36]

Nationale Behörden und Regierungen können ggf. aus Gründen der nationalen Sicherheit auf bestimmte Daten zugreifen oder deren Übermittlung beschränken oder verhindern.

Im Rahmen des Betriebs einer Cloud-basierten Datenaustauschplattform können Genehmigungspflichten etwa bei der Datenverlagerung auf Server in Drittländern (z. B. außerhalb des EWR) oder bei Ermöglichung des Zugriffs auf Daten aus einem Drittland bestehen.[37] Wenn lokale Regierungen oder Behörden den Daten einen hohen Wert, z. B. mit Blick auf Aspekte der nationalen Sicherheit zuschreiben, können zusätzliche Anforderungen an IT-Sicherheit („*Cyber Security*") und Verschlüsselung hinzutreten.[38] Diese Regelungen betreffen in der Regel allerdings Daten öffentlicher Stellen, Steuer- und Buchhaltungsdaten oder Finanzdaten, die als solche nicht im Zusammenhang mit den auf Maschinendaten basierenden Use Cases stehen.[39]

Außerdem können Transparenzpflichten der Unternehmen gegenüber lokalen Behörden bestehen, die es erfordern, über die Art und Zwecke bestimmter Datenübermittlungen zu informieren.[40] Ihre Auswirkungen als potentielles Digitalisierungs-Hemmnis sind im Zusammenspiel mit Datenlokalisierungsvorschriften[41] und dem Zugriff auf bzw. Schutz von Geschäftsgeheimnissen[42] zu sehen.

## 6. Einfuhr-/ Ausfuhrkontrollbestimmungen

Einfuhr- bzw. Ausfuhrkontrollbestimmungen für Hardware und Software bzw. Datenträger können auch bestimmte Datenarten und -inhalte betreffen, wenn sie in Verbindung mit bestimmter Hard- und Software und Sicherheitsanforderungen stehen (z. B. Verschlüsselungstechniken im Rahmen der Dual-Use-Verordnung).[43] Dies führt ggf. zu erhöhten Kosten und entsprechendem Verwaltungsaufwand und limitiert möglicherweise, in welchem Umfang bestimmte Daten übermittelt werden dürfen. Beschränkungen und Verbote des freien Datenverkehrs sind denkbar, wenn sie dem Schutz höherrangiger Güter und Interessen dienen. Im Rahmen der Ausfuhrkontrolle ist dies regelmäßig die Verhinderung der Bedrohung des jeweiligen Landes oder Wirtschaftsraums oder seiner Bündnispartner durch konventionelle Waffen und Massenvernichtungswaffen bzw. das Interesse, dass Exporte in Krisengebiete nicht konfliktverstärkend wirken.[44] Maschinen- und Anlagenbauer betrifft dies in der Regel über die „Dual-Use-Verordnung", d. h. mit Blick auf solche Güter, Software und Technologien, die auch für militärische Zwecke eingesetzt werden könnten. Einzelheiten ergeben sich aus den gesetzlichen Regelungen zur Ausfuhrkontrolle, z. B. der europäischen Verordnung über die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchfuhr von Gütern mit doppeltem Verwendungszweck.[45] Maschinen- und Anlagenbauer unterliegen der Exportkontrolle, wenn sie genehmigungspflichtige Güter ausführen oder Güter in exportrechtlich kritisch eingestufte Länder ausführen oder der Ausfuhrzweck exportrechtlich untersagt ist.[46]

## 7. Handelssanktionen

Durch Handelssanktionen und protektionistischen Maßnahmen wie Embargos, (Straf-)Zölle oder Einfuhrverbote können Staaten den freien Außenwirtschaftsverkehr gegenüber bestimmten Ländern aus außen- oder sicherheitspolitischen Gründen beschränken. Die Regelungen bzw. Güterbeschreibungen in den Embargos respektive ihren Anlagen gehen den allgemeineren ausfuhrrechtlichen Regelungen vor und sind stets zu überprüfen. Soweit ein Embargo zugleich die Umsetzung digitaler Geschäftsmodelle für bestimmte Warenklassen (also etwa im Bereich des Maschinen- und Anlagenbaus) betrifft, wirken diese Maßnahmen unmittelbar als Digitalisierungsbarrieren. Oftmals wenden sich die Handelssanktionen jedoch nicht direkt gegen digitale Geschäftsmodelle oder Datenströme, sondern beeinflussen diese lediglich mittelbar. Die Handelssanktionen können sich dabei entweder abstrakt-generell oder auch im Rahmen von sogenannten „Blacklists" konkret gegen einzelne Unternehmen[47] oder Länder[48] richten.

# VII. Digitalisierungsbarrieren in der EU

## 1. Einführung

Die EU Kommission hat die Notwendigkeit eines stabilen und berechenbaren Rechtsrahmens angesichts der Komplexität der Digitalisierung der Wirtschaft erkannt. Insbesondere hängt die Wettbewerbsfähigkeit und Produktivität der EU entscheidend von der Fähigkeit ab, digitale Innovationen in allen Wirtschaftssektoren, einschließlich der traditionellen europäischen Stärken im Fahrzeugbau, der Automatisierung, dem Maschinenbau oder dem Finanzwesen, zu generieren, zu vergrößern und effektiv zu nutzen.[49] Als Teil ihrer Strategie für den digitalen Binnenmarkt („*Digital Single Market*“) hat die EU Kommission deswegen den „Freien Datenverkehr“ („*Free Flow of Data*“) als neue Grundfreiheit vorgestellt.[50] Durch die Sicherstellung des freien Datenverkehrs innerhalb der EU sollen Nutzer von Datenverarbeitungsdiensten mit den in den verschiedenen EU-Märkten gesammelten Daten ihre Produktivität und Wettbewerbsfähigkeit verbessern können.[51] Nach der Zielvorstellung der EU Kommission lassen sich hierdurch Größenvorteile des großen EU-Marktes vollumfänglich nutzen, um die globale Wettbewerbsfähigkeit der Nutzer und die Vernetzung der europäischen Datenwirtschaft zu verbessern.[52] Hiervon können auch nicht in der EU ansässige Unternehmen profitieren, sofern sie den Anforderungen der EU-Gesetzgebung, einschließlich ggf. einschlägiger europäischer Mindestanforderungen genügen.

Mit Blick auf die Regulierung von Software sind diese Eintrittsschwellen in der EU sowohl für europäische als auch nicht in der EU ansässige Unternehmen eher gering. Die EU hat bislang keine einheitliche Gesetzgebung hinsichtlich der technischen und sicherheitstechnischen Anforderungen von Software getroffen. Unternehmen können in diesem Zusammenhang bislang weitgehend frei agieren. Dabei ist jedoch zu beachten, dass die mittels der Software generierten Daten ggf. den maßgeblichen Anforderungen der DS-GVO genügen müssen.

## 2. Schutz von Geschäftsgeheimnissen

Die **Richtlinie zum Schutz von Geschäftsgeheimnissen**[53] befindet sich derzeit in der Umsetzungsphase durch die Mitgliedstaaten[54]. Mit der Richtlinie werden ein einheitlicher Begriff des Geschäftsgeheimnisses definiert, die Anforderungen an den Schutz zur Absicherung des zugrundeliegenden wirtschaftlichen Werts eines Geschäftsgeheimnisses in Europa vereinheitlicht und die insoweit bestehende Fragmentierung des Binnenmarktes zum Schutz von Geschäftsgeheimnissen abgebaut (auch wenn keine Vollharmonisierung erfolgt).

Zukünftig fallen nur solche Informationen unter den Geschäftsgeheimnisschutz, die geheim, d. h. „[weder] allgemein bekannt [noch] ohne Weiteres zugänglich“, durch ausreichende Sicherheitsvorkehrungen geschützt und, weil sie geheim sind, von kommerziellem Wert sind.[55] Dabei ist insbesondere durch den Gesetzgeber und nachgelagert die Gerichte abzuklären, ab wann Informationen „nicht ohne Weiteres zugänglich“ sind. Unsicherheiten darüber wie hoch die Anforderungen an die Zugänglichkeit zu Informationen sein müssen, könnten sonst zu einem „Wettrüsten“ an Sicherheitsmechanismen und damit einer Behinderung des freien Datenverkehrs führen. Zudem können sich Digitalisierungsbarrieren über asymmetrische Sicherheitsanforderungen ergeben, die einer skalierten Lösung im Wege stehen. Notwendig wären hier klare Vorgaben der EU oder der nationalen Behörden, welche Schutzmechanismen jedenfalls als Mindeststandard ausreichend sind, um den Schutz im Rahmen der Richtlinie und jeweiligen nationalen Umsetzung zu gewährleisten. Dies könnte z. B. durch die Erarbeitung eines europäischen Standards für den technischen und organisatorischen Mindestschutz für Geschäftsgeheimnisse geschehen.

## Übersicht zu Prüffeldern in der EU

| Schutz von Geschäftsgeheimnissen | Schutz Kritischer Infrastrukturen | Vorschriften zur Datenlokalisierung | Datenschutzrecht | Ausfuhrkontrollbestimmungen | Handelssanktionen |
|---|---|---|---|---|---|
| 🟡 | 🟡 | 🟢 | 🔴 | 🟡 | 🟢 |

- 🔴 Starke Auswirkungen
- 🟡 Mögliche Auswirkungen im Einzelfall zu prüfen, Änderungen beobachten
- 🟢 Aktuell keine oder wenige Einschränkungen

**Top-Themen zu europäischen Digitalisierungsbarrieren**:

- Starker Schutz und starke Regulierung kann Innovation hemmen.
- Neue Anforderungen an den Geschäftsgeheimnisschutz.
  - Geheimnisschutz künftig nur mit Schutzmechanismen.
- Fehlende Kriterien zur Anonymisierung und Pseudonymisierung von personenbezogenen Daten.

## 3. Schutz Kritischer Infrastrukturen

Maschinenbetreiber und -hersteller müssen sich mit der Frage auseinander setzen, ob und inwieweit sie bzw. ihre Kunden Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber) sind. Kritische Infrastrukturen sind Einrichtungen, Anlagen oder Teile davon, die unter anderem den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, oder Ernährung angehören und deren Ausfall oder Beeinträchtigung eine Gefahr für die öffentliche Sicherheit darstellen oder zu erheblichen Versorgungsengpässen führen würden.[56] Im Zuge der Schaffung eines einheitlichen europäischen Rechtsrahmens[57] zur Erhaltung und Gewährleistung eines hohen Sicherheitsniveaus bei KRITIS-Betreibern wurden unter anderem Mindestsicherheitsanforderungen und Meldepflichten für KRITIS-Betreiber kodifiziert. Deutschland hat in der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung) detailliert geregelt, welche Tätigkeiten betroffen bzw. Schwellenwerte erfüllt sein müssen, damit ein Unternehmen als KRITIS-Betreiber einzustufen ist.

Die Umsetzung der Forderungen nach einem höheren Maß an IT-Sicherheit geht dabei zum Teil mit einer Einschränkung des freien Datenverkehrs einher. Digitalisierungsbarrieren für die digitalen Dienste von Maschinen- und Anlagenbauern können sich ergeben, wenn ein Datentransfer IT-sicherheitsrechtlich relevante Schnittstellen berührt. Ferner können Doppelbelastungen für nationale Hersteller und Marktbarrieren für ausländische Hersteller entstehen, wenn die Mitgliedsstaaten innerhalb ihrer nationalen Gesetzgebung von der NIS-Richtlinie divergierende (striktere) Sonderwege eingegangen sind.

Im März 2019 hat das Bundesministerium des Innern, für Bau und Heimat einen Referentenentwurf für ein zweites Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0) veröffentlicht.[58] Hierdurch soll der Kreis der betroffenen Unternehmen wie auch die ihnen auferlegten Pflichten erweitert werden und das Bundesamt für Sicherheit in der Informationstechnik (BSI) weitreichende zusätzliche Kompetenzen erhalten. Zudem wird die Höhe möglicher Bußgelder drastisch erhöht – sie soll auf DS-GVO-Niveau steigen. Zu den neuen Adressaten unter dem Referentenentwurf, d. h. den Betreibern Kritischer Infrastrukturen, sollen zukünftig auch Einrichtungen des Entsorgungs-Sektors zählen.[59] Des Weiteren sollen „Infrastrukturen im besonderen öffentlichen Interesse“ den gleichen Pflichten unterliegen

wie Kritische Infrastrukturen. Unter diese neue Kategorie sollen Unternehmen der Rüstungswirtschaft und bestimmte nach der Börsenordnung der Frankfurter Wertpapierbörse regulierte Infrastrukturen genauso gehören wie Unternehmen im Bereich Kultur und Medien, wobei die Einzelheiten durch Rechtsverordnung bestimmt werden sollen.[60] Die Gesetzesbegründung zählt auch die Automobil- und Chemiebranche hinzu; diese finden sich aber nicht im eigentlichen Referentenentwurf. Des Weiteren soll das BSI Betreibern mit „Cyber-Kritikalität" im Einzelfall Pflichten auferlegen können. Darunter fallen nicht nur Unternehmen, die wegen ihrer unzureichenden Bedeutung nicht unter den Begriff „Kritische Infrastrukturen" fallen, sondern auch Unternehmen, die insbesondere wegen des hohen Grades an Vernetzung der eingesetzten Informationstechnik, zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der betroffenen Dienstleistungen insgesamt führen würden, z. B. Betreiber von Anlagen der Kommunikationsinfrastruktur oder IT-Infrastruktur für die Trinkwasserversorgung.[61] Dies kann Maschinen- und Anlagenbauer entweder unmittelbar oder mittelbar als Zulieferer für die jeweiligen Anlagenbetreiber treffen.

## 4. Vorschriften zur Datenlokalisierung

**Verordnung über den freien Datenverkehr nicht-personenbezogener Daten**
In Ergänzung zur DS-GVO hat die EU 2018 die Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der EU[62] finalisiert. Die Verordnung zielt auf den Abbau von Datenlokalisierungsvorschriften in den Mitgliedsstaaten und darauf, die Entstehung neuer Lokalisierungsvorschriften innerhalb der EU zu verhindern, soweit diese nicht aus besonderen Gründen (etwa der nationalen Sicherheit) zwingend erforderlich sind. In der Regel greifen die bestehenden Datenlokalisierungsvorschriften nicht für Maschinendaten.[63] Die Erleichterung von Anbieterwechsel und die Übertragbarkeit solcher Daten für industrielle Nutzer von Datenspeicherungsdiensten, z. B. Cloud-Anbietern, sind komplementäre Bestandteile dieses Regelungsansatzes.

**Initiative zu (Datenaustausch-)Plattformen**
Im April 2018 hat die EU Kommission eine „Initiative zu Online-Plattformen zur Gewährleistung eines fairen, vorhersehbaren, tragfähigen und vertrauenswürdigen Geschäftsumfelds für die Online-Wirtschaft" beschlossen, um das Funktionieren des digitalen Binnenmarkts weiter zu verbessern.[64] Ziel der neuen Bestimmungen ist die Schaffung eines fairen, transparenten und vorhersehbaren Geschäftsumfelds für kleinere Unternehmen und Händler, die für den Ausbau ihrer Geschäftstätigkeit Online-Plattformen nutzen.[65] Mit diesem weiteren Schritt der EU Kommission auf dem Weg zum digitalen Binnenmarkt adressiert sie zwar vorrangig den E-Commerce-Bereich; es sind aber auch Auswirkungen auf Datenaustauschplattformen im Rahmen der digitalisierten Produktion abzusehen. Insbesondere Maschinenhersteller, die eigene Datenaustauschplattformen planen und diese unter Umständen einzelnen kleineren Komponentenlieferanten öffnen wollen, sollten diese Initiative im Auge behalten und sich ggf. mit ihren Anliegen in die Diskussion einbringen. Durch eigene Beiträge können interessierte und engagierte Unternehmen Einfluss auf die Initiative nehmen, um ihre eigenen Vorstellungen als (Industrie-)Standards zu fixieren und eventuell daraus hervorgehende regulatorische Vorgaben nach den eigenen Interessen zu gestalten. Solche Plattformen sind dabei im Zusammenspiel mit Remote Access Dienstleistungen und Condition Monitoring zu sehen, um die allen Use Cases inhärente verstärkte Vernetzung im Maschinenbau zu fördern. Die mittels Remote Access und Condition Monitoring generierten Daten können auf der (Datenaustausch-)Plattform umfassend analysiert werden. Konkret könnten solche Plattformen als proprietäre Lösung auch von einem größeren Unternehmen aufgesetzt werden, um als skalierbare Lösung Kostenvorteile an KMU weiterzugeben, wenn diese ihre Maschinendaten für Remote Access bereitstellen und ggf. im Rahmen des Condition Monitoring nutzen lassen, sowie auch Erleichterung hinsichtlich einschlägiger regulatorischer Anforderungen zu bieten. Teilweise werden solche Datenaustauschplattformen über eine Vereinsstruktur für die Community ergänzt, damit die Plattformbetreiber im Dialog mit den Teilnehmern die Plattform gemeinsam weiterentwickeln können.

## 5. Datenschutz-grundverordnung

Soweit im Zuge der Use Cases Maschinendaten verarbeitet werden, die zugleich personenbezogene Daten enthalten, z. B. NutzerIDs oder Daten, die Rückschlüsse auf das Verhalten und die Leistung von Mitarbeitern zulassen, müssen Maschinen- und Anlagenbauer die Anforderungen der DS-GVO erfüllen. Um nicht dem strengen Schutzregime des europäischen Datenschutzes zu unterfallen, können Maschinen- und Anlagenbauer technische und organisatorische Maßnahmen, z. B. Anonymisierungsmaßnahmen ergreifen.

**Anonymisierung**
Gelingt die Anonymisierung der personenbezogenen Daten, ist der Anwendungsbereich der DS-GVO bereits nicht eröffnet. Allerdings ist die Schwelle hoch, ab der Daten wirklich als anonym gelten. Die Art.-29-Datenschutzgruppe[66] weist etwa ausdrücklich darauf hin, dass es zum zuverlässigen Ausschließen einer Identifizierung nicht ausreicht, wenn die Elemente, die eine direkte Identifizierung erlauben, entfernt werden.[67] Für eine wirksame Anonymisierung wird gefordert, dass keine Partei in der Lage ist, eine Person aus einem Datenbestand herauszugreifen, eine Verbindung zwischen zwei Datensätzen eines Datenbestands (oder zwischen zwei unabhängigen Datenbeständen) herzustellen oder durch Inferenz Informationen aus einem solchen Datenbestand abzuleiten.[68] Häufig werden weitere Maßnahmen erforderlich sein, wobei weder die DS-GVO, noch die Art.-29-Datenschutzgruppe konkrete Kriterien bezüglich der Ausgestaltung dieser Maßnahmen festlegen. Insbesondere in Zeiten von Big Data stellt dies Unternehmen vor die schwierige Frage, mit welchen Mitteln in den Augen der Datenschutzbehörden eine effektive Anonymisierung erreicht werden kann.

**Pseudonymisierung**
Im Gegensatz zu anonymen Daten, sind pseudonymisierte Daten[69] eine Untergruppe der personenbezogenen Daten für die die DS-GVO vollumfänglich Anwendung findet. Pseudonymisierungsmaßnahmen ermöglichen eine erleichterte Verarbeitung der Daten, indem die Datenverarbeitung durch die gezielte Verschleierung der Identität für die betroffene Person weniger eingriffsintensiv ist, als eine Verarbeitung ohne Pseudonymisierung. Entsprechend fällt die Festellung und Abwägung des „Berechtigten Interesses“ (Art. 6 Abs. 1 f) DS-GVO) leichter zugunsten des Verantwortlichen aus.[70] Für eine DS-GVO-konforme Pseudonymisierung müssen zwei Voraussetzungen erfüllt sein: Erstens muss diese so gestaltet sein, dass ohne Kenntnis der jeweiligen Zuordnungsregel zwischen Kennzeichen und Person praktisch keine Möglichkeit mehr besteht, die Daten einer spezifischen betroffenen Person zuzuordnen.[71] Zweitens ist sicherzustellen, dass die zusätzlichen Informationen, mit denen die personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, gesondert aufbewahrt werden.[72]

**Verhaltensregeln**
Ein geeignetes Mittel, um mehr (Rechts-) Sicherheit für Unternehmen des Maschinen- und Anlagenbaus hinsichtlich effektiver und rechtmäßiger Anonymisierungs- und Pseudonymisierungsmaßnahmen zu schaffen, ist z. B. die Ausarbeitung von Verhaltensregeln („*Code of Conducts*“), die die Anwendung der DS-GVO konkretisieren. In die Konkretisierung sollen branchenspezifische Besonderheiten und besondere Bedürfnisse von kleinen und mittleren Unternehmen einfließen. Damit wird die Initiative zur Selbstregulierung der Wirtschaft gestärkt. Verhaltensregeln sollen gerade Unternehmen, die als Verantwortliche im Sinne der DS-GVO[73] personenbezogene Daten verarbeiten, bei der Umsetzung der Regelungen der DS-GVO in ihren Geschäftsmodellen unterstützen.

Verbände können in Zusammenarbeit mit maßgeblichen Interessenträgern Verhaltensregeln ausarbeiten und die Anwendung der DS-GVO, z. B. in Bezug auf die Pseudonymisierung, branchenspezifisch konkretisieren (Art. 40 Abs. 2 DS-GVO). Der Vorteil solcher – von der zuständigen Datenschutzaufsichtsbehörde und dem Europäischen Datenschutzausschuss zu genehmigenden – Verhaltensregeln zu Anonymisierungs- und Pseudonymisierungsmaßnahmen bestünde z. B. für Maschinen- und Anlagenbauer darin, dass sie ihre internen Prozesse und technischen und organisatorischen Maßnahmen bei der Verarbeitung

personenbezogener Daten entsprechend der Verhaltensregeln ausrichten und dabei branchenspezifische Gegebenheiten des Maschinen- und Anlagenbaus abbilden. Dabei ist zu beachten, dass ein Unterschreiten der in der DS-GVO getroffenen Regelungen zur Verarbeitung personenbezogener Daten nicht zulässig ist. Die Verhaltensregeln müssen nach dem jeweiligen Recht des Mitgliedsstaates, in dem die zuständige Aufsichtsbehörde ihren Sitz hat, förmliche Genehmigungsverfahren durchlaufen. Sinnvoll ist deswegen bereits eine frühe Abstimmung mit den zuständigen Datenschutzbehörden, um zu gewährleisten, dass die ausgearbeiteten Verhaltensregeln den relevanten Verfahren entsprechen.

## 6. Ausfuhrkontroll-bestimmungen (Exportkontrolle)

Auf europäischer Ebene regelt die EG-Dual-Use-Verordnung die Ausfuhr von Dual-Use-Gütern. Daneben sind nationale Vorschriften wie diejenigen des deutschen Außenwirtschaftsgesetzes (AWG) und der Außenwirtschaftsverordnung (AWV) sowie die derzeit bestehenden 35 länderbezogenen Embargos relevant.[74]

**EG-Dual-Use-Verordnung**
Maschinen- und Anlagenbauer unterliegen der Exportkontrolle nach der EG-Dual-Use-Verordnung, wenn sie gemäß der Güterliste Anhang I zur EG-Dual-Use-Verordnung genehmigungspflichtige Güter oder Güter in exportrechtlich kritisch eingestufte Länder ausführen oder der Ausfuhrzweck exportrechtlich untersagt ist.[75] Aufgrund der Öffnungsklauseln der EG-Dual-Use-Verordnung[76] sind nationale Abweichungen möglich, etwa eine Ausweitung auf nicht in Anhang I gelistete Güter.[77] Eine Genehmigungspflicht besteht auch für nicht gelistete Güter, wenn die kundenseitig vorgesehene Verwendung im Zusammenhang mit der Herstellung, Entwicklung, Wartung oder Verbreitung von Massenvernichtungswaffen steht („*Catch-All-Klausel*").[78] Die bloß theoretische Möglichkeit einer militärischen Einsetzbarkeit von Gütern ist dabei ausreichend.

**Exportkontrolle bei Software und Technologie**
Exportkontrollvorschriften können im Einzelfall Digitalisierungshemmnisse begründen, da Ausführgüter neben physischen Maschinen auch Software und Technologie erfassen, die für die Herstellung oder Verwendung der jeweiligen Dual-Use-Güter entwickelt worden ist.[79] Mit Blick auf die Use Cases ist etwa die Ausfuhr von Dual-Use-Verschlüsselungsprodukten relevant. Diese unterfallen dann der Exportkontrolle, wenn sie unter die Kryptotechnik-Anmerkung der EG-Dual-Use-Verordnung fallen. Grundsätzlich gilt dies – unabhängig von der Schlüssellänge – nicht für frei zugängliche Verschlüsselungsprodukte („*Public Domain*" und „*Shareware*").[80] Eine Genehmigungspflicht kann sich dann allenfalls über die Catch-All-Klausel ergeben.

**Exportkontrolle in den Use Cases**
Im Zuge des Remote Access und Condition Monitoring generierte Daten können eine ausfuhrrechtliche Genehmigungspflicht nach sich ziehen, wenn ein Datentransfer von (gelisteten) Daten oder Software von einem Server aus einem Mitgliedsstaat in ein Drittland stattfindet und damit eine Ausfuhr im Sinne der Dual-Use-Verordnung vorliegt. Die Art und Weise der elektronischen Datenübertragung ist dabei unerheblich, insbesondere muss der Datentransfer nicht zwingend Ländergrenzen überwinden. Eine Ausfuhr liegt vielmehr bereits durch das Bereitstellen vor, das heißt durch die bloße Möglichkeit des Zugriffs auf (gelistete) Software, Daten oder Technologien, einschließlich Datenverarbeitungsprogrammen mittels elektronischer Medien von außerhalb der EU.[81] Der Zugriff aus dem Ausland muss dabei jedoch durch den Ausführer beabsichtigt gewesen sein.[82]

Bei Remote Access und Condition Monitoring, insbesondere, wenn diese über Cloud-basierte Systeme (z. B. „Infrastructure as a Service" („*IaaS*") oder „Software as a Service" („*SaaS*")) stattfinden, ist maßgeblich, wohin ein Datentransfer im Einzelfall erfolgt und wer wem Zugriff auf die (gelisteten) Daten einräumt. Ein Datentransfer von (gelisteten Daten) vom Inland in eine Cloud im Ausland ist eine Ausfuhr in Form einer „elektronischen Übertragung".[83] Das Verschaffen von Zugriffsmöglichkeiten aus

dem Ausland auf einen Server im Inland ist eine Ausfuhr in Form des „Bereitstellens". Auf den Standort des Servers kommt es für die exportrechtliche Verantwortung nicht an, sondern nur auf den Standort desjenigen, der die Einräumung der Zugriffsmöglichkeiten beherrscht und veranlasst. Daher ist auch die Einräumung der Zugriffsmöglichkeiten auf einen in einem Drittland befindlichen Server als Bereitstellen in diesem Sinne zu verstehen.[84]

Wird Software (z. B. bei der Nutzung von SaaS) bei einem externen IT-Dienstleister betrieben, ist das Einstellen von gelisteter Anwendungssoftware auf einen Server in einem Drittland eine klassische Ausfuhr. Auch das Aufspielen von Softwareaktualisierungen, z. B. wenn Datenverlagerungen von Deutschland nach China erfolgen, oder das Einräumen des Zugriffs für einen (z. B. chinesischen) Betreiber auf (gelistete) Herstellerdaten in Deutschland, damit dieser Aktualisierungen eigenständig vornehmen kann, stellen eine Ausfuhr dar.[85] Während Updates zum Zwecke der reinen Fehlerbehebung exportrechtlich grundsätzlich zu vernachlässigen sein dürften, können Upgrades auf eine höherwertige Konfiguration der Basissoftware durchaus relevant sein. Werden im Zuge von Wartungsarbeiten Betreiberdaten aus dem Ausland abgefragt, diese sodann vom Hersteller verarbeitet und in Form eines Statusberichtes als (gelistete) Ergebnisdaten an den ausländischen Betreiber transferiert, handelt es sich hierbei ggf. um eine exportrechtlich relevante technische Unterstützung.[86] Sofern ein Hersteller Personen aus dem Ausland Zugriff auf unbedenkliche, nicht im Zusammenhang mit den Güterlisten stehende Daten verschaffen will, ist dies kein exportrechtlich relevanter Vorgang.[87] Verlangt wird dann, dass er verfügbare Sicherheitsmaßnahmen trifft, um unbefugte Zugriffe effektiv zu unterbinden. Eine Ausfuhr liegt auch nicht vor, wenn gelistete Software ausschließlich der Verschlüsselung des Übertragungsweges zwischen der SaaS-Applikation und dem Nutzer dient und die Unterbindung einer anderweitigen Nutzung sichergestellt wird.[88]

Beispiel[89]: Eine gelistete Software wird zur Effizienzsteigerung von Maschinen und Anlagen von einem Hersteller auf einem Server in einem Drittland bereitgestellt und sodann mit (gelisteten) Messdaten gespeist. Die gebündelten Ergebnisse werden dann maschinell in das Land transferiert, indem sich der anfragende Hersteller befindet. Hier ist das Einstellen der Software auf dem Server im Drittland der erste Ausfuhrtatbestand. Die Einräumung der Zugriffsrechte auf die Software aus dem Ausland stellt den zweiten Ausfuhrtatbestand dar. Das Vorhaben des die Software einstellenden Herstellers wäre genehmigungspflichtig.

Ob sodann für die Ausfuhr der Maschinen und Anlagen und/oder zusätzlich für den Transfer (gelisteter) Software/Daten jeweils eine Einzelausfuhrgenehmigung oder eine allgemeine Genehmigung oder eine Sammelausfuhrgenehmigung erforderlich ist, ist vom Einzelfall abhängig und muss im Zweifel mit den national zuständigen Behörden für die Ausfuhrkontrolle evaluiert werden.[90]

## 7. Handelssanktionen

Embargovorschriften der EU bzw. Güterbeschreibungen in den entsprechenden Anlagen[91] gehen, soweit sie einschlägig sind, als Spezialregelungen den allgemeinen Ausfuhrkontrollbestimmungen der Dual-Use-Verordnung oder des Außenwirtschaftsgesetzes vor. Sollten die Voraussetzungen der Embargovorschriften auf einen Sachverhalt nicht zutreffen, ist stets die Dual-Use-Verordnung bzw. die etwaig bestehende zusätzliche nationale Gesetzgebung zu berücksichtigen. Neben Waffenembargos, die sich gegen einzelne Länder richten, können aber auch jede sonstige Art von Gütern (Software, Technologie, Maschinen) von Embargos betroffen sein.

Diese sonstigen Ausfuhrverbote und -beschränkungen sind im Gegensatz zur allgemeinen Exportkontrolle nicht an die Güterliste der Dual-Use-Verordnung gebunden und die Embargos dienen auch nicht der Bekämpfung

von Gefahren für höherrangige Schutzgüter. Vielmehr werden im Rahmen von Embargovorschriften außen-, wirtschafts- und sicherheitspolitische Interessen verfolgt und originäre Listen mit detaillierten Beschreibungen der vom Embargo betroffenen Waren oder Warengruppen erstellt und veröffentlicht.

So stehen die Maßnahmen der US-Administration gegen chinesische Netzwerkausrüster vor dem Hintergrund einer umfassenden wirtschafts- und sicherheitspolitischen Auseinandersetzung um die Schlüsseltechnologie der 5G-Netze. Die regulatorischen Auswirkungen sind dabei vielfältig und einschneidend. Die Bundesregierung hat im Zuge der Diskussion eine Anpassung der Sicherheitsanforderungen der Betreiber von Telekommunikationsdiensten beschlossen.[92]

Im Ergebnis ist jeweils im Einzelfall zu prüfen, ob sich aus Handelssanktionen zusätzliche Beschränkungen für die Use Cases ergeben können. Während dies für den innereuropäischen Verkehr offensichtlich unproblematisch ist, sind die Auswirkungen auf Aktivitäten in den Zielmärkten China und Russland zum Teil erheblich.

# VIII. Digitalisierungsbarrieren in China

## 1. Einführung

Chinas Fertigungsindustrie erlebt einen tiefgreifenden Wandel zur Automatisierung, der die Nachfrage nach Industrie 3.0 Technologien und „Made in Germany“ antreibt.[93] Um auch den Ausbau von Industrie 4.0 in China dynamisch zu entwickeln, setzt China u. a. auf Data Analytics, Cloud-Technologien sowie Machine Learning in der verarbeitenden Industrie. Dabei besteht aus chinesischer Sicht im Bereich der industriellen Fertigung noch erheblicher Aufholbedarf.[94] In zahlreichen Teilbereichen der Industrie 4.0 verzeichnete China bislang ein zweistelliges jährliches Wachstum, z. B. für Industriesensoren, Industriesoftware und drahtlose Sensornetzwerke.[95] Die dynamisch ansteigende Nachfrage eröffnet ganz erhebliche Geschäftschancen für ausländische, insbesondere deutsche Technologieanbieter.[96] Aufgrund des erklärten Ziels der chinesischen Industriepolitik, in Anlehnung an die deutsche Industrie 4.0-Strategie, eine umfassende Digitalisierung und Automatisierung der industriellen Produktion vorzunehmen[97], ergeben sich kurz- und mittelfristig erhebliche Chancen für den Maschinenbau, den chinesischen Markt mit technologisch hochqualitativen Produkten zu versorgen.[98] Insbesondere Unternehmen, die auf Nischenprodukte spezialisiert sind und über ausgewiesene Kompetenz für die

### Übersicht zu Prüffeldern in China

| Schutz von Geschäftsgeheimnissen | Schutz Kritischer Infrastrukturen | Datenschutzrecht | Vorschriften zur Datenlokalisierung | Einfuhrkontrollbestimmungen |
|---|---|---|---|---|
| ● | ● | ● | ● | ● |

● Starke Auswirkungen

● Mögliche Auswirkungen im Einzelfall zu prüfen, Änderungen beobachten

● Aktuell keine oder wenige Einschränkungen

**Top-Themen zu chinesischen Digitalisierungsbarrieren:**

- Beachtliches Risiko: Maschinen- und Anlagenbauer gelten als Netzwerkbetreiber im Sinne des Cyber-Security-Gesetzes.
  - Sicherheitsbewertungen durch Unternehmen selbst oder in Zusammenarbeit mit der zuständigen Behörde.
  - Datenlokalisierungspflichten.
- Risiko für Hersteller: Zulassungspflichtige Netzwerkprodukte.
- Weiter Begriff der „personenbezogenen“ oder „wichtigen“ Daten.
  - Auch Maschinendaten können betroffen sein.
- Risiko des Zugriffs auf Geschäftsgeheimnisse durch die chinesische Regierung.

Entwicklung individualisierter Kundenlösungen verfügen, können in den kommenden Jahren aller Voraussicht nach stark davon profitieren,[99] wobei dies mittel- bis langfristig allerdings mit dem Risiko des Abflusses von Know-how verbunden sein kann.[100] In dem Zusammenhang bietet die Coud-basierte Vernetzung von Maschinen und der Einsatz von Verschlüsselungstechnologien eine maßgebliche Chance dar, den Abfluss von Know-how zu verhindern.[101]

**„Made in China 2025“**

Die Herausforderungen des chinesischen Markts und Rechtsrahmens sind für Unternehmen seit jeher komplex. Mit Blick auf das Industrieprogramm „Made in China 2025“ und das erklärte Ziel der chinesischen Regierung, die inländische und globale Marktführerschaft in zehn Zukunftstechnologien zu erreichen, werden diese Herausforderungen auch in Zukunft bestehen bleiben. Aus Sicht des Maschinen- und Anlagenbaus sind insbesondere Schlüsseltechnologien im Bereich Landtechnik und Maschinenbau/Roboter zu nennen: Robotik und CNC-gesteuerte Werkzeugmaschinen sind prominent in der Strategie vertreten. Einbezogen in die Strategie sind auch Maschinen und Geräte für die Landwirtschaft, wie etwa hocheffiziente Traktoren, Erntemaschinen und Düngersaatmaschinen, sowie Kernkomponenten, darunter Dieselmotoren, Antriebstechnik, Navigations- und Lenksysteme.[102] Bei Kontroll- und Steuerungssystemen, Industriesensoren und Halbleiterfertigungssystemen für die intelligente Fertigung will China seine Innovationsfähigkeiten stark ausbauen.[103] Chinesische Regierungskreise diskutieren ferner die Ausweitung von Made in China 2025 auf weitere Industrien.[104] Im Gespräch sind Baumaschinen, Maschinen zur Erdölverarbeitung und Haushaltsgeräte. Falls diese in die Liste der Schlüsseltechnologien aufgenommen werden, wird die chinesische Regierung auch hier Maßnahmen ergreifen, um ihre Industrien und heimischen Hersteller zu fördern. Unternehmen des Maschinen- und Anlagenbaus müssen in diesen Marktsegmenten folglich damit rechnen, dass sich der regulatorische Rahmen und damit einhergehende Digitalisierungsfragen an diese strategische Ausrichtung anpassen werden.

Unternehmen des Maschinen- und Anlagenbaus, die in China datenbasierte Geschäftsmodelle realisieren möchten, müssen sich – sowohl hinsichtlich personenbezogener Daten als auch der Maschinendaten – darauf einrichten, speziell auf die chinesischen Regulierungen zugeschnittene Lösungen vorzuhalten, die nicht oder jedenfalls nicht einheitlich in eine global skalierbare Lösung zu integrieren sind.[105]

## 2. Schutz von Geschäftsgeheimnissen

Die Lieferung von innovativen Produkten, die aufgrund des darin verkörperten oder zur Produktion erforderlichen Know-hows nur schwer substituiert werden können, und High-End-Produkten nach China unterliegt dem Risiko eines unbeabsichtigten bzw. nicht kontrollierbaren Know-how-Abflusses, dem ein relativ geringes Maß an effektivem Rechtsschutz gegenübersteht.[106] Dies gilt sowohl für China als weiterhin bedeutsamen Produktionsstandort, als Absatzmarkt, wie auch zunehmend als Forschungs- und Entwicklungsstandort.[107] Viele Unternehmen sehen zudem ihre Geschäftsgeheimnisse durch mögliche Zugriffsrechte der chinesischen Behörden, als auch im Rahmen der Zusammenarbeit mit lokalen Kooperationspartnern gefährdet. Hinzu kommt die Besorgnis, dass Daten beim Einsatz chinesischer Netzwerktechnologie (einschließlich der 5G-Technologie), oder aufgrund lokaler technologischer oder regulatorischer Vorgaben nicht vor unerwünschten Regierungszugriffen geschützt sind.[108]

So hat beispielsweise das Vorgehen Chinas im Jahr 2017 gegen die Bereitstellung nicht ausdrücklicher von den chinesischen Behörden genehmigter („illegaler“) internationaler VPN-Dienste Bedenken internationaler Unternehmen, die auf VPN-Dienste für die Datenübermittlung zwischen ihren chinesischen und ausländischen Niederlassungen angewiesen sind, verstärkt und insgesamt zu einer Unsicherheit im Markt geführt. Teil der angesprochenen Besorgnis ist zudem, dass damit staatlich gelenkte Zugriffe auf Datenverkehr, insbesondere auf Geschäftsgeheimnisse der betroffenen Unternehmen, auch in den zur Rede stehenden Use Cases eröffnet werden könnten (insbesondere, da

die einzigen Unternehmen, die derzeit für die Erbringung „legaler“ internationaler VPN-Dienste zugelassen sind, staatliche Telekommunikationsunternehmen sind).

Der Maschinenbau steht damit vor einem grundlegenden Dilemma: Um in China weiterhin erfolgreich zu sein, müssen sich die Unternehmen auf den technologischen Wandel in China einlassen und neue Geschäftsmodelle vor Ort ausprobieren und realisieren. Gleichzeitig gilt es jedoch, ihr Know-how, eingesetzte Schlüsseltechnologien und Innovationen angemessen zu schützen.[109]

**Cyber-Security-Gesetz**

Chinas „**Cyber-Security-Gesetz**” hat bei in China engagierten Unternehmen bereits zu erheblicher Verunsicherung geführt.[110] Das im Juni 2017 in Kraft getretene Gesetz beschränkt unter anderem den Transfer von sogenannten „wichtigen“ und personenbezogenen Daten ins Ausland und öffnet weitreichende Möglichkeiten zur staatlichen Inspektion von teilweise sensiblen Unternehmensdaten. Das Cyber-Security-Gesetz ist der erste Schritt zu einer umfassenden Regelung digitaler Sachverhalte, auf dessen Grundlage die chinesische Regierung weitere detaillierte Regelungen zu unterschiedlichen Themenbereichen mit Relevanz für datenbasierte Geschäftsmodelle erlassen wird. Im weltweiten Vergleich gelten die chinesischen Barrieren im Umgang mit (personenbezogenen und nicht-personenbezogenen) Daten insgesamt als die restriktivsten, dicht gefolgt von den Regulierungen aus Russland.[111]

Nach dem strikten Wortlaut des Cyber-Security-Gesetzes ist es mit Ausnahme des berechtigten Empfängers niemandem, auch nicht der chinesischen Regierung, gestattet, auf den Inhalt von Nachrichten, die über Telekommunikationsnetze in China gesendet werden, für andere Zwecke als die der Netzwerksicherheit zuzugreifen.[112] Mit anderen Worten, das Cyber-Security-Gesetz gibt der chinesischen Regierung kein pauschales Zugriffsrecht für sämtliche Zwecke. Ausnahmen greifen dann, wenn der Zugriff auf die Telekommunikationsdaten der Aufdeckung von Straftaten dient. Des Weiteren enthält das Cyber-Security-Gesetz ausdrückliche Bestimmungen, die es den Regulierungsbehörden untersagen, Daten, auf die sie zugreifen können, für andere Zwecke als der Netzwerksicherheit zu verwenden. Es besteht große Skepsis, dass sich die chinesische Regierung und Behörden an diese Regelungen halten werden. Bereits in der Vergangenheit führte die chinesische Regierung nach allem Anschein umfangreiche Wirtschaftsspionage zum direkten Vorteil ihrer eigenen Wirtschaft, einschließlich militärischer und verteidigungspolitischer Fähigkeiten, durch.[113] Daran dürfte Chinas aktuelle Wirtschaftspolitik wenig ändern. Vielmehr deutet vieles darauf hin, dass China in der Umgestaltung der wirtschaftlichen Ordnung die Rolle, Kontrolle und Steuerung durch den Staat nicht zurücknehmen, sondern im Endergebnis voraussichtlich noch intensivieren wird.[114]

**Praktische Konsequenzen**

Für Unternehmen des Maschinen- und Anlagenbaus, die Bedenken hinsichtlich der Sicherheit ihrer Geschäftsgeheimnisse haben, ergeben sich daraus im Rahmen digitalisierter Anwendungen folgende praktische Konsequenzen: Unternehmen sollten

- geeignete Verschlüsselungstechnologien beim Datentransfer bzw. im Rahmen von Datenzugriffen verwenden, wobei zu beachten ist, dass die Verwendung ausländischer Verschlüsselungstechnologie und -ausrüstung der staatlichen Kontrolle unterliegt. Zur Orientierung unterhält Chinas „*State Cryptography Administration*“ (SCA) eine öffentlich zugängliche Online-Datenbank mit einer Liste der zugelassenen Verschlüsselungstechnologien. Soweit eine Genehmigungspflicht vorliegt, stellt es einen Verstoß dar, in China nicht zugelassene Verschlüsselungstechnologie zu verwenden;

- „chinesische“ Daten in China speichern, wenn keine entsprechende Freigabe oder Zulassung zur Datenübertragung bzw. -speicherung im Ausland beantragt wurde; [115] und

- die nach China „importierten“ Geschäftsgeheimnisse soweit wie möglich begrenzen. Unternehmen sollten insbesondere prüfen, ob eine Datenübertragung für den Betriebsprozess wirklich notwendig ist.[116]

## 3. Schutz Kritischer Infrastrukturen

Das jetzige Bündel von geplanten Regulierungen des Cyber-Security-Gesetzes richtet sich an Netzwerkbetreiber und Betreiber Kritischer Infrastrukturen. Unternehmen des Maschinen- und Anlagenbaus müssen sich deswegen mit der Frage auseinandersetzen, ob und inwieweit das Cyber-Security-Gesetz auf sie unmittelbare Anwendung findet bzw. ob es kundenseitig greift und sich daraus entsprechende Auswirkungen auf die Zulieferleistungen ergeben. Kritische Infrastrukturen sind nach chinesischer Definition Infrastrukturen, deren Zerstörung, Funktionsverlust oder mögliche Verletzungen die nationale Sicherheit, die chinesische Wirtschaft, die Lebensgrundlagen von Menschen und das öffentliche Interesse Chinas ernsthaft gefährden können.[117] Dies wird insbesondere für Infrastrukturen in einer Reihe von Schlüsselsektoren, wie öffentliche Kommunikation, Energie, Verkehr und Finanzdienstleistungen, vermutet.

**Netzwerkbetreiber**

Der Begriff „Netzwerkbetreiber“ im Sinne des Cyber-Security-Gesetzes ist weit zu verstehen und umfasst nicht nur traditionelle Telekommunikationsanbieter. Netzwerkbetreiber sind vielmehr Eigentümer und Verwalter eines Netzwerks oder Netzwerkdienstleisters.[118] Ein „Netzwerk“ ist ein System, das aus Computern, Endgeräten und weiteren zugehörigen Ausrüstungsgeräten besteht, die Informationen nach spezifischen Regeln und Verfahren sammeln, speichern, übertragen, austauschen und verarbeiten.[119] Mit anderen Worten, ein Unternehmen des Maschinen- und Anlagenbaus, das ein eigenes unternehmensinternes IT-System betreibt, ist danach voraussichtlich ebenfalls als Netzwerkbetreiber zu betrachten. Die im April 2017 veröffentlichten „**Maßnahmenentwürfe**“ der „*Cyberspace Administration of China*“ (CAC)[120] führen zudem zu einer Ausweitung der Datenlokalisierungspflichten für Netzwerkbetreiber, denen sonst lediglich Betreiber von Kritischen Infrastrukturen unterliegen.[121] Zum Zeitpunkt der Veröffentlichung der Studie sind die Maßnahmenentwürfe noch nicht offiziell verkündet und es bleibt abzuwarten, inwieweit diese die Regelungen des Cyber-Security-Gesetzes tatsächlich verschärfen. Prinzipiell würde unter den Maßnahmenentwürfen jeder Betreiber eines Computernetzwerks – einschließlich interner Firmennetzwerke – zum Netzwerkbetreiber.

Würden die Maßnahmenentwürfe in ihrer derzeitigen Form als verbindlich bestätigt, so könnten sie ein direktes Hindernis für grenzüberschreitenden Remote Access, Condition Monitoring oder Datenaustauschplattformen darstellen. Die damit verbundene Regulierung der Datenströme würde insbesondere das Condition Monitoring und die Datenaustauschplattformen unmittelbar betreffen, wenn in diesen Fällen Daten aus den in China eingesetzten Maschinen an Hersteller und/oder Plattformbetreiber und sonstige Intermediäre nach Deutschland fließen. Für die in China tätigen Maschinenbauer und Anlagenbetreiber stellt sich mithin die Frage, welche regulatorischen Einschränkungen oder auch Risiken mit Blick auf die Absicherung vertraulicher Informationen bestehen, die sich aus den Anforderungen des Cyber-Security-Gesetzes an die Datenspeicherung (ggf. lokal) und Datenübermittlung ergeben (durch die Verpflichtung zur Nutzung von von China vorgegebener VPN-Technologie der staatlichen Telekommunikationsanbieter).

**Kritische Infrastrukturen**

Lässt man die Maßnahmenentwürfe außer Acht, gelten die schärferen Regelungen, einschließlich der Datenlokalisierungspflichten, nach dem Wortlaut des Cyber-Security-Gesetzes nur für Betreiber Kritischer Infrastrukturen. Aktuell wird weder der Maschinen- und Anlagenbau noch die industrielle Fertigung ausdrücklich in den relevanten gesetzlichen Bestimmungen genannt.[122] Allerdings ist die im Cyber-Security-Gesetz enthaltene Liste der Kritischen Infrastrukturen nicht als vollständig zu verstehen. Dementsprechend können unter Umständen auch Infrastrukturen in anderen Sektoren ebenfalls als Kritische Infrastrukturen angesehen werden. Das Cyber-Security-Gesetz sieht vor, dass der Staatsrat zu gegebener Zeit zusätzliche Maßnahmen, z. B. einen

Leitfaden, zur Identifizierung von Infrastrukturen veröffentlichen wird, die als Kritische Infrastrukturen im Sinne des Cyber-Security-Gesetzes anzusehen sind.

Aus einem inoffiziellen internen Leitfaden[123] der chinesischen Behörden ergibt sich, dass Infrastrukturen und Systeme, wie z. B. Unternehmensbetriebssysteme, Smart Manufacturing Systeme (z. B. IoT Manufacturing Systeme, Smart Equipment) und Überwachungssysteme für Hoch-Risiko-Fertigungsanlagen, potentiell als Kritische Infrastrukturen zu betrachten sind. Dies soll insbesondere dann gelten, wenn die jeweilige Infrastruktur bestimmte quantitative Grenzwerte erfüllt, z. B. wenn ein Sicherheitsproblem der jeweiligen Infrastruktur zu einem potenziellen Verlust von etwa USD 7,2 Millionen (RMB 50 Millionen) oder zur Offenlegung von personenbezogenen Daten von mehr als 1 Million Betroffenen führen kann. Zwar dürften diese recht hohen Schwellenwerte seitens einer größeren Anzahl von Maschinen- und Anlagenbauer selbst nicht zum Tragen kommen; es ist aber natürlich keineswegs ausgeschlossen, dass diese Schwellenwerte auf der Betreiber- bzw. Kundenseite in der einen oder anderen Konstellation – ggf. auch im Fall der Datenaustauschplattform – erreicht werden oder diese Schwellenwerte zukünftig nach unten angepasst werden.

**Überprüfungen vor grenzüberschreitenden Übermittlungen**

Die Folge sind Berichts- und Überprüfungspflichten. Betreiber Kritischer Infrastrukturen bzw. Netzwerkbetreiber, die den beschriebenen Datenlokalisierungspflichten unterliegen, sind verpflichtet, vor einer grenzüberschreitenden Datenübermittlung zu überprüfen, ob diese für die Erfüllung von geschäftlichen Interessen erforderlich ist. Ist dies der Fall, hat das Unternehmen – selbst oder ab bestimmten Schwellenwerten[124] in Zusammenarbeit mit den Behörden – zusätzlich eine Sicherheitsbewertung der grenzüberschreitenden Datenübermittlung durchzuführen. Unternehmen, die unterhalb der Schwellenwerte liegen, müssen die von ihnen selbstständig durchgeführte Risikobewertung bei der zuständigen Behörde vorlegen. Die Datenübermittlung ist nur dann zulässig, wenn die Risiken der Datenübermittlung, die im Rahmen der Sicherheitsbewertung zu Tage treten, als gering eingestuft werden können. Genaue Vorschriften und nationale Normen für die Sicherheitsbewertung bei der grenzüberschreitenden Datenübermittlung befinden sich aktuell noch im Entwurfsstadium und sind – soweit überhaupt zugänglich – noch nicht rechtsverbindlich. Betroffene Unternehmen sollten trotzdem mit der Vorbereitung von Formularen und Prozessen für interne Sicherheitsbewertungssysteme beginnen, um die Sicherheitsbewertung (soweit erforderlich) zeitnah und ggf. in Zusammenarbeit mit der zuständigen Behörde durchführen zu können bzw. der jeweiligen Behörde bereitzustellen. In diesem Fall ist nach rechtlicher Beratung und in Konsultation der chinesischen Behörden zu prüfen, ob ähnliche Lösungsansätze, wie sie Unternehmen im Umgang mit Datenlokalisierungsvorschriften in Russland (Vorhalt der Originaldaten auf lokalen Server-Anlagen und Spiegelung von relevanten Daten aus Russland hinaus)[125] einsetzen, auch im Rahmen der chinesischen Regulierung zweckmäßig und akzeptabel sein können. Dabei ist allerdings zu beachten, dass es sich bei einer Spiegelung der relevanten Daten, selbst bei Verbleib der Originaldaten in China, ebenfalls um eine grenzüberschreitende Datenübermittlung handelt, die die beschriebenen Verpflichtungen auslöst.

## 4. Datenschutzrecht und Schutz wichtiger nicht-personenbezogener Daten

Das chinesische Datenschutzrecht basiert auf den Sicherheitsspezifikationen für personenbezogene Daten („**Spezifikationen**"), die vom Technischen Komitee für die Normung der nationalen Informationssicherheit („**Technisches Komitee**")[126] im Dezember 2017 veröffentlicht wurden und am 1. Mai 2018 in Kraft getreten sind. Diese Spezifikationen haben keinen unmittelbaren Rechtsnormcharakter, sondern spiegeln die von den Behörden erwartete „Best Practice" wieder. In der Praxis kommt ihnen aber erhebliche Bedeutung für die Verarbeitung personenbezogener Daten zu. Insbesondere legen die Spezifikationen detailliert dar, wie die allgemeinen gesetzlichen Anforderungen an den Schutz personenbezogener Daten, die im Cyber-Security-Gesetz enthalten sind, zu verstehen sind

und eingehalten werden können. So legen die Spezifikationen die Voraussetzungen fest, unter denen ein Unternehmen personenbezogene Daten erheben und verarbeiten darf, z. B. auf welche Rechtsgrundlagen sich Unternehmen bei der Verarbeitung personenbezogener Daten stützen können. Gemäß den Spezifikationen werden bestimmte Daten in jedem Fall als personenbezogene Daten angesehen, ungeachtet dessen, ob mittels der Daten tatsächlich eine Identifizierung der jeweiligen betroffenen Person möglich ist.[127] Dies gilt beispielsweise für Standortdaten oder Geräteidentifikationsnummern von Mitarbeitern oder Firmentransportfahrzeugen. Maschinen- und Anlagenbauer, die solche Mittel und Tools einsetzen, sind gut beraten, diese Spezifikationen umzusetzen und einzuhalten.

Im April 2019 haben das *Cyber-Security-Büro des Ministeriums für Öffentliche Sicherheit* („**MPS**“)[128], die *Beijing Network Industry Association* und das *Dritte Forschungsinstitut* des MPS[129] Richtlinien zum Schutz personenbezogener Daten im Internet herausgegeben („**Richtlinien**“). Die Richtlinien stehen teilweise im Widerspruch zu den Spezifikationen und es ist bislang unklar, in welchem Verhältnis die beiden Regelungen zueinander stehen, insbesondere ob die Spezifikationen oder die Richtlinien vorrangig gelten.[130]

**Änderungsentwurf der Spezifikationen**
Am 1. Februar 2019 hat das Technische Komitee einen Änderungsentwurf für die Spezifikationen veröffentlicht, der bis Anfang März zur öffentlichen Diskussion frei gegeben war. Nach diesem Entwurf müssen Unternehmen in Zukunft auch für Verarbeitungszwecke, bei denen aggregierte personenbezogene Daten verarbeitet werden, Sicherheitsbewertungen zur Einschätzung der Risiken vornehmen. Des Weiteren müssen Unternehmen, die über Datenaustauschplattformen Dritten (z. B. Lieferanten oder Kunden) Daten zur Verwendung für eigene Zwecke bereitstellen, bestimmte Anforderungen erfüllen. Dies gilt nur, wenn über die Plattform personenbezogene Daten ausgetauscht werden. Neben die Sicherheitsbewertung tritt als zusätzliche Anforderung, dass die Parteien eine schriftliche Vereinbarung abschließen müssen, in der die jeweiligen datenschutzrechtlichen Verpflichtungen der Parteien dargelegt werden. Ähnlich wie nach der DS-GVO werden damit die Dokumentationsanforderungen des Datenschutzes an die Parteien verstärkt.

Am 25. Juni 2019 wurde ein weiterer Änderungsentwurf für die Spezifikationen veröffentlicht, der bis Anfang August 2019 zur öffentlichen Diskussion freigegeben war. Unter anderem werden darin die Anforderungen an die Einwilligung zur Verarbeitung von personenbezogenen Daten, die Vorgaben bei Profiling und weitere allgemeine datenschutzrechtliche Themen behandelt. Eine wesentliche Änderung ist, dass die ursprüngliche Meldepflicht von datenschutzrechtlichen Verstößen in diesem Änderungsentwurf nicht mehr enthalten ist.

## 5. Vorschriften zur Datenlokalisierung

Die chinesische Regierung arbeitet in Ergänzung zum Cyber-Security-Gesetz an verschärften Regelungen, einschließlich Datenlokalisierungsvorschriften, für personenbezogene Daten sowie nicht-personenbezogenen Daten, die als „wichtig“ erachtet werden[131]. Personenbezogene Daten können in digitalisierten Produktionsabläufen, z. B. im Rahmen der Mensch-Maschine-Kommunikation zum Tragen kommen. Der Begriff „wichtige Daten“ („*important data*“) umfasst Daten hinsichtlich der nationalen Sicherheit, wirtschaftlichen Entwicklung und solche, für die ein soziales und öffentliches Interesse besteht. In dem Ende Mai 2019 vom CAC veröffentlichten Maßnahmenentwurf wird die Definition konkretisiert und klargestellt, dass Produktions-, Betriebs-, interne Management- sowie personenbezogene Daten keine „wichtigen Daten“ darstellen.[132] Unternehmen können jedoch noch nicht aufatmen, da der

Wortlaut der Maßnahmenentwürfe mehrdeutig formuliert ist und damit die Unsicherheit bleibt, ob diese Daten nicht doch als „wichtige Daten" gelten könnten. Zudem befinden sich die Maßnahmenentwürfe noch im Entstehungsprozess und sind zum Zeitpunkt der Veröffentlichung der Studie noch nicht verabschiedet. Gemäß dem Änderungsentwurf sind „wichtige (nicht-personenbezogene) Daten" beispielsweise:

- in der chemischen Industrie: Layoutpläne der Fabrikgebäude, Standorte der Lager, Größe, Kapazität, Jahresverbrauch; und
- in der Nichteisenmetallindustrie: Art, Häufigkeit und Anzahl der von Großkunden bezogenen Tonnen Metall.

Konkrete Beispiele für „wichtige Daten" mit Blick auf digitale Produkte und Geschäftsmodelle sind bislang noch nicht bekannt.

## 6. Einfuhr- / Ausfuhrkontrollbestimmungen

**Einfuhrkontrollbestimmungen für Maschinen mit Verschlüsselungssoftware**
Nicht alle Verschlüsselungstechnologien unterliegen der Einfuhrkontrolle. Die SCA stellte bereits im Jahr 2000 in einer Mitteilung klar, dass nur spezielle Produkte mit Verschlüsselung als Kernfunktion den Anforderungen der Einfuhrkontrolle unterliegen.[133]

Soweit Produkte der Einfuhrkontrolle unterfallen, finden die 1999 erlassenen Verwaltungsvorschriften zur kommerziellen Verschlüsselung Anwendung. Art. 13 der Verwaltungsvorschriften sieht vor, dass für die Einfuhr von Verschlüsselungsprodukten oder Produkten, in die eine Verschlüsselungstechnologie eingebettet wurde, eine Einfuhrgenehmigung bei der SCA einzuholen ist. Art. 14 der Verwaltungsvorschriften sieht ferner vor, dass jeder Person in China die Verwendung von außerhalb Chinas hergestellter Verschlüsselungstechnologie untersagt ist. Diese Bestimmungen bilden die rechtliche Grundlage dafür, dass nur „*Foreign Invested Enterprises*" (FIE) in China Verschlüsselungstechnologien verwenden dürfen, die im Ausland hergestellt und anschließend importiert werden.

Maschinenhersteller, in deren Produkten Verschlüsselungssoftware eingebettet ist, sollten demnach prüfen, ob ihre Produkte unter den Katalog der Produkte mit Verschlüsselung als Kernfunktion fallen, für die eine Einfuhrgenehmigung erforderlich ist, um die Sicherheit des Datenflusses von China zu einem Ort außerhalb Chinas zu gewährleisten. Des Weiteren sollten sie prüfen, ob der jeweilige Kunde eine inländische chinesische Gesellschaft oder eine FIE ist, um den unterschiedlichen Anforderungen angemessen gerecht zu werden. Wenn es sich um eine inländische chinesische Gesellschaft handelt, sollte die Verwendung einer inländischen Verschlüsselungstechnologie in Betracht gezogen werden, die in China hergestellt und von der SCA zugelassen ist.

**Generelle Zulassungsanforderungen nach dem Cyber-Security-Gesetz**
Darüber hinaus sollten Maschinen- und Anlagenbauer überprüfen, ob sie in ihren Maschinen zulassungspflichtige Systeme und Komponenten verbauen. Dies gilt insbesondere für „kritische Netzwerkausrüstung" und „spezialisierte Netzwerksicherheitsprodukte".[134] Entsprechende Listen werden vom CAC herausgeben und können unter anderem über die EU Handelskammer in China eingesehen werden. Die einzureichenden Angaben für die Zulassung bestehen unter anderem aus technischen Indikatoren der Systeme bzw. Komponenten, einer ausführlichen Produktbeschreibung, Informationen über die Entwicklung, Leitfäden und Testergebnissen. Das Erfordernis, den Quellcode im Zulassungsprozess offenzulegen, wird aus den uns zur Verfügung stehenden behördlichen Dokumenten nicht ersichtlich. Allerdings lässt sich mit Blick auf die intransparenten behördlichen Anforderungen das Risiko nicht ausschließen, dass Unternehmen zur Offenlegung des Quellcodes aufgefordert werden könnten.[135]

**Sicherheitsbewertung für den Datenexport**
Das CAC hat am 13. Juni 2019 einen zweiten Entwurf der Maßnahmen zur Sicherheitsbewertung beim Export personenbezogener Daten („*Maßnahmenentwurf*") veröffentlichicht und binnen Monatsfrist die Möglichkeit zur Beteiligung der Öffentlichkeit gegeben.

Die Maßnahmen und Leitlinien sind, anders als unter dem Cyber-Security-Gesetz nicht nur auf Betreiber Kritischer Infrastrukturen, sondern auf alle Netzwerkbetreiber anzuwenden. Darunter fallen auch Unternehmen, die außerhalb Chinas tätig sind, aber personenbezogene Daten von Personen in China über das Internet oder auf anderem Wege erheben und verarbeiten. Aus diesem Grund sollten die betroffenen Unternehmen ihre Ansprechpartner in China konsultieren, um die entsprechenden Verpflichtungen zu erfüllen.

Die Netzwerkbetreiber sind im Rahmen des Maßnahmenentwurfs verpflichtet, einen Antrag auf Durchführung einer Sicherheitsbewertung in Bezug auf den Export personenbezogener Daten zu stellen. Hierbei ist für jeden Datenempfänger ein gesonderter Antrag zu stellen. Eine erneute Antragstellung ist jedoch nicht erforderlich, wenn mehrere Datentransfers an denselben Empfänger vollzogen werden und hierfür eine Genehmigung bereits vorliegt. Die Genehmigung muss entweder alle zwei Jahre, oder bei einer Änderung des Zwecks der Übertragung, der Datenkategorien oder der Aufbewahrungsfrist erneuert werden. Bei Antragstellung muss ein Anmeldebericht, der entsprechende Vertrag über den Datenexport mit dem Datenempfänger, ein Bewertungsbericht über die Sicherheitsrisiken, Schutzmaßnahmen in Zusammenhang mit dem Datenexport und weiterer Informationen, die der CAC möglicherweise anfordert, eingereicht werden. Darüber hinaus müssen die Netzwerkbetreiber den Export der personenbezogenen Daten für einen Zeitraum von fünf Jahren dokumentieren und jährlich eine Stellungnahme über die Dokumentation und die Vertragsbeziehung zu dem Datenempfänger abgeben. Außerdem muss jeder datenschutzrechtliche Verstoß dem CAC mitgeteilt werden.

Der Maßnahmenentwurf beinhaltet auch sämtliche Regelungen über den obligatorischen Vertragsinhalt zwischen dem Netzwerkbetreiber und dem Datenempfänger; hierunter zählt z. B., dass die Art der exportierten personenbezogenen Daten beschrieben ist und eine Klausel, dass der Netzwerkbetreiber die betroffenen Personen über die Ausfuhr der Daten informieren wird.

Aufgrund des erhöhten administrativen Aufwands sollten sich betroffene Unternehmen im Voraus mit den Anforderungen an den Datenexport vertraut machen.

Der Maßnahmenentwurf beinhaltet keine Regelungen für den Export von besonderen personenbezogenen Daten. Demnach ist in Kürze mit einem weiteren Maßnahmenentwurf des CAC mit Maßnahmen und Leitlinien zu rechnen.

# IX. Digitalisierungsbarrieren in Russland

## 1. Einführung

Die gesetzlichen Regelungen zu Fragen der digitalen Wirtschaft in Russland befinden sich im Umbruch. 2017 hat die russische Regierung eine großangelegte Initiative gestartet, um Regelungen für Schlüsseltechnologien und Konzepte wie IoT, Big Data, künstliche Intelligenz („**KI**“) und Sensorkomponenten zu schaffen („Programm zur Digitalwirtschaft in Russland“ („**Digital-Programm**“)).[136]

Das Hauptziel des Digital-Programms liegt in der Entwicklung und Förderung einer (eigenständigen) Digitalwirtschaft, in der Daten das Schlüsselelement in allen Bereichen des verarbeitenden Gewerbes darstellen und eine effiziente (grenzüberschreitende/internationale) Interaktion zwischen Unternehmen, Wissenschaft, Bildungseinrichtungen, dem Staat und Einzelpersonen ermöglichen. Darüber hinaus befasst sich das Digital-Programm auch mit der Beseitigung von Hindernissen und Einschränkungen bei der Gründung oder Entwicklung von High-Tech-Unternehmen. Das Digital-Programm

### Übersicht zu Prüffeldern in Russland

| Schutz Kritischer Infrastrukturen | Vorschriften zur Datenlokalisierung | Regelungen der nationalen Sicherheit | Einfuhrkontrollbestimmungen |
|---|---|---|---|
| ● | ● | ● | ● |

- ● Starke Auswirkungen
- ● Mögliche Auswirkungen im Einzelfall zu prüfen, Änderungen beobachten
- ● Aktuell keine oder wenige Einschränkungen

**Top-Themen zu russischen Digitalisierungsbarrieren:**

- Digital-Programm prägt künftige Gesetzgebung.
  - Einflussnahme durch Verbände auf Gesetzgebungsverfahren.
- Viele Anforderungen betreffen nur in Russland eingetragene Unternehmen.
  - Mittelbare Auswirkungen (z. B. kundenseitig) für Maschinen- und Anlagenbauer.
- Datenlokalisierungspflichten bei personenbezogenen Daten.
  - Hohe Relevanz im Bereich Mensch-Maschine-Interaktion.
  - Nicht zu unterschätzender Kostenfaktor und Verwaltungsaufwand.

stellt unter anderem Big Data, KI, Roboter- und Sensorkomponenten, Distributed-Ledger-Technologie, IoT, drahtlose Telekommunikationsdienste und Virtual Reality/Augmented Reality als wichtige digitale Technologien in den Fokus der weiteren Entwicklung Russlands.

## 2. Digital-Programm

Im Rahmen des Digital-Programms sollen künftig eine Vielzahl an Rechtsvorschriften geändert und verabschiedet werden. Zum Zeitpunkt der Veröffentlichung der Studie befindet sich die Gesetzgebung noch in der Planungs- und Entwurfsphase, so dass noch keine abschließenden Aussagen zu möglichen Folgen und Digitalisierungsbarrieren insbesondere für ausländische Unternehmen getroffen werden können. Die avisierten gesetzlichen Regelungen sollen aber auf den folgenden Grundsätzen der Informationssicherheit aufbauen:

- Einsatz russischer Technologien zur Gewährleistung der Vollständigkeit, Vertraulichkeit, Authentifizierung und Verfügbarkeit der übertragenen Informationen bei der Datenverarbeitung;
- Bevorzugter Einsatz russischer Softwareprodukte und Geräte;
- Anwendung von Informationsschutztechnologien nach russischen Verschlüsselungsstandards.[137]

**Maßnahmenkatalog des Föderationsrats**
Diese Grundsätze wurden zuletzt Ende März 2018 durch die Empfehlungen des Föderationsrats des russischen Parlaments bekräftigt und näher begründet.[138] Der Föderationsrat äußerte sich kritisch dazu, dass Produkte, die die Entwicklung der Digitalwirtschaft in Russland vorantreiben, in hohem Maße auf im Ausland entwickelter Software und Hardware beruhen. Nach russischer Lesart könnte dies zu einer Gefährdung nationaler Interessen führen, wenn Lieferungen und Supportleistungen für diese Produkte eingestellt würden, ohne dass es hierzu entsprechende russische Produkte bzw. Auffanglösungen gibt. Des Weiteren stammen viele der Produkte und Systeme, die in Russland für die Kommunikation und Organisation digitaler Dienste genutzt werden, aus dem Ausland. Russland würde sich damit von Verarbeitungssystemen außerhalb des Zugriffs der russischen Gerichtsbarkeit abhängig machen. Es bestehe die Gefahr, dass der Zugriff auf bestimmte Systeme, auf denen sich erhebliche Datenmengen mit potentiellem Marktwert befinden, etwa über russische Unternehmen und andere Akteure der russischen Wirtschaft, einseitig verwehrt werden könnte. Durch die Verarbeitung dieser Daten wären Einblicke in demographische Kennzahlen und den Status bestimmter Wirtschaftssektoren möglich. Dies könnte sich nachteilig auf die Interessen Russlands auswirken, zum Beispiel dann, wenn diese Informationen von ausländischen Unternehmen zur Gewinnerzielung mithilfe unlauterer Wettbewerbsvorteile missbraucht würden. Der Föderationsrat sprach daher gegenüber der russischen Regierung folgende Handlungsempfehlungen aus:

- Entwicklung von Anforderungen, dass alle in Russland produzierten Daten auf russischen Geräten gespeichert werden;
- Gesetzesentwurf über die Bevorzugung von russischen Computer-, Server- und Telekommunikationsgeräten und Produkten der IT-Sicherheit bei der staatlichen und kommunalen Auftragsvergabe, einschließlich der im Rahmen der Digitalwirtschaft neu entstehenden Branchen;
- Gesetzesentwurf zur Festlegung von Schlüsselparametern des IoT, einschließlich von Regelungen über die Grundsätze der Offenlegung von Daten auf den verwendeten Geräten, des sicheren Funktionierens der Geräte, der Haftung für verursachte Schäden und der Festlegung eines Informationsumfangs auf Endnutzergeräten (der ohne Zutun des einzelnen Nutzers durch den Telekommunikationsanbieter festgelegt wird).

Der vorstehende Maßnahmenkatalog deutet auf ein – aus russischer Sicht – durchaus nachvollziehbares Anliegen, die Abhängigkeit von globalen ausländischen Technologiedienstleistern in bestimmten Bereichen zu reduzieren. Mit ihr würde sich aber – je nach gesetzlicher Ausgestaltung – zugleich in hohem Maße ein

protektionistischer Ansatz realisieren, auf den sich Unternehmen des Maschinen- und Anlagenbaus bei der Umsetzung digitaler Geschäftsmodelle einrichten müssen. Dies gilt insbesondere, wenn sie international verfügbare Technologien einsetzen, um Remote Access, Condition Monitoring und Datenaustauscplattformen in skalierbarem Umfang zu realisieren. Es ist derzeit nicht abzusehen und zumindest fraglich, ob alternative Technologieangebote aus Russland tatsächlich den benötigten Funktionsumfang abbilden und auch die entsprechende Akzeptanz bei Herstellern und Betreibern erzielen können oder ob es sich letztlich um eine programmatische, aber in der Praxis nur beschränkt durchsetzbare Gesetzgebung handelt. Jedenfalls ist aber für alle Marktteilnehmer unverzichtbar, die weitere Gesetzgebung aufmerksam zu verfolgen.

Die autonome, nicht kommerzielle Organisation „Tsifrovaya Ekonomika“ (übersetzt: „Digitale Wirtschaft“) hat für diese Zwecke eine Reihe von Arbeitsgruppen und Kompetenzzentren entwickelt, an denen auch ausländische Unternehmen teilnehmen und mitwirken können. Zu ihren Aufgaben gehören unter anderem die Beurteilung der Umsetzungseffektivität des Digital-Programms und die Sicherstellung eines produktiven Dialogs zwischen Wirtschaft und Staat.[139]

## 3. Schutz Kritischer Infrastrukturen

Des Weiteren hat die russische Regierung regulatorische Maßnahmen[140] getroffen, die Sicherheit Kritischer Infrastrukturen zu schützen, die sich ggf. durch Einschränkungen und Verbote auf die Use Cases Remote Access und Condition Monitoring und damit die Übermittlung von Maschinendaten vom Betreiber zum Hersteller einer Maschine auswirken können. Maschinenhersteller sollten in Erfahrung bringen, ob sie selbst (mit Blick auf ihre digitalisierte Produktion) und/oder ihre Kunden als Betreiber einer Kritischen Infrastruktur nach russischem Recht gelten. Nach dem föderalen Gesetz Nr. 187-F3 vom 26. Juli 2017 gelten russische juristische Personen oder Einzelunternehmer als Betreiber Kritischer Infrastrukturen, wenn sie Eigentümer der folgenden Infrastrukturen sind, oder diese gemietet haben: Informationssysteme, Informations- und Telekommunikationsnetze, automatisierte Steuerungssysteme in den Bereichen Gesundheitsversorgung, Wissenschaft, Transport, Telekommunikation, Energie, Banken- und Finanzwesen, Kraftstoffe, Nuklearenergie, Verteidigung, Raumfahrt, Bergbau und Chemie.

**Sicherheitsstandards für Betreiber Kritischer Infrastrukturen**

Die Kritischen Infrastrukturen unterliegen nach dem „Föderalen Gesetz über die Sicherheit Kritischer Infrastrukturen“ („**Russisches KRITIS-Gesetz**“) jeweils spezifischen Sicherheitsstandards, die den Einsatz zertifizierter Tools und Lösungen zum Informationsschutz erfordern (einschließlich zertifizierter Verschlüsselungstools).[141] Darüber hinaus dürfen Software oder kombinierte Software-Hardware-Lösungen, die in Kritischen Infrastrukturen eingesetzt werden, nicht verwendet werden, um:

- anderen Personen als Mitarbeitern des Betreibers der jeweiligen Infrastruktur zu gestatten, mittels Remote Access zu Kontroll- und Wartungszwecken auf die betreffende Kritische Infrastruktur zuzugreifen;
- den unkontrollierten Zugriff unbefugter Dritter vor Ort zuzulassen;
- Informationen, einschließlich technischer Informationen, an unbefugte Dritte zu übermitteln. Dies gilt auch für Datenübermittlungen an die Entwickler oder Hersteller der verwendeten Software bzw. kombinierten Software-Hardware-Lösungen sowie Tools zum Schutz der Informationen, die nicht der Kontrolle des Betreibers der Kritischen Infrastruktur unterliegen.[142]

Verantwortlich für die Einhaltung der genannten Anforderungen an die Kritische Infrastruktur und entsprechend haftbar ist das jeweilige russische Unternehmen, da nur dieses Adressat der gesetzlichen Regelungen ist. Ausländische Maschinenhersteller sind allenfalls mittelbar betroffen, wenn sie ihre (digitalisierten) Produkte den Anforderungen russischer Kunden anpassen müssen. Daraus folgt, dass ausländische Maschinenhersteller mit Blick auf Remote Access und Datenübermittlungen ins

Ausland im Rahmen des Condition Monitoring dann in einer Konfliktlage mit den Anforderungen stehen, wenn sie Betreiber Kritischer Infrastrukturen als Kunden bedienen möchten. Vor diesem Hintergrund hatte das russische Energieministerium noch vor Inkrafttreten des Russischen KRITIS-Gesetzes Bedenken geäußert, die darauf abzielten, beispielsweise die Übermittlung von Maschinenrohdaten aus dem Betrieb in russischen Kraftwerken eingesetzter Turbinen ausländischer Hersteller (GE, Siemens und Alstom) zu limitieren. Indem die Turbinen eine Echtzeitüberwachung des Anlagenzustands und der Parameter des Anlagenbetriebs ermöglichten, befürchtete das Ministerium, könnte die direkte Datenübermittlung dazu führen, dass ausländische Turbinenhersteller Zugriff auf die Kraftwerke erhalten und deren Steuerung übernehmen könnten. Diese Bedenken führten letztlich zu der strengen gesetzlichen Regelung. Für nicht-russische Unternehmen ist es in solchen Konstellationen empfehlenswert, ihre datenzentrischen Dienste über lokale Dienstleister aufzubauen.

Maschinenhersteller, die selbst nicht unter diese Beschränkungen fallen, sollten mit betroffenen Kunden vertraglich festlegen, wie die betroffenen Daten in Übereinstimmung mit den russischen Gesetzesanforderungen ausgetauscht und genutzt werden können.

Unternehmen, die in Russland tätig sind oder russische Kunden haben, müssen mithin aufmerksam prüfen, ob ihre Produkte den Regelungen zur Sicherheit kritischer Infrastrukturen unterfallen und ob die Use Cases dann überhaupt oder ggf. in modifizierter Form implementiert werden können. Alternativ könnten Unternehmen ihre technischen Systeme so aufbauen, dass ein schaltender Zugriff[143] von außen technisch unmöglich ist (z. B. mit Datendioden).

## 4. Vorschriften zur Datenlokalisierung

Legt man den Fokus auf Datenlokalisierung, Speicherung und Transfer von Daten, weist dem „*Digital Trade Restrictiveness Index*“ zufolge Russland die meisten restriktiven Regelungen auf, dicht gefolgt von China.[144] Seit September 2015 gibt es in Russland Datenlokalisierungspflichten für personenbezogene Daten. In Russland tätige (russische und ausländische) Unternehmen müssen personenbezogene Daten[145] zunächst über Datenbanken verarbeiten (d. h. erheben und speichern), die sich in Russland befinden.[146] Hiervon dürfen nur unter engen Voraussetzungen Ausnahmen gemacht werden.[147] Die Lokalisierung nicht-personenbezogener Daten ist nur in Einzelfällen erforderlich, etwa bei Betreibern Kritischer Infrastrukturen.[148] Ausländische Unternehmen haben in den vergangenen Jahren diverse Lösungsansätze verfolgt, um diesen Anforderungen gerecht zu werden. Dazu gehören u. a.:

- die Modifikation der gesamten Datenverarbeitungsstruktur, um eine Erstverarbeitung in Russland zu ermöglichen;
- der Aufbau lokaler Schnittstellen zu globalen IT-Systemen;
- das Outsourcing der Erstverarbeitung an lokal ansässige Dritte;
- die Errichtung eines zusätzlichen Rechenzentrums für die Erhebung und Speicherung personenbezogener Daten in Russland. Die Daten müssen dabei nicht ausschließlich in Russland gespeichert werden, vielmehr ist es zulässig, eine Kopie der Daten auch außerhalb Russlands zu speichern;
- die Segmentierung von Datenbanken, wodurch russische Unternehmen bzw. Tochtergesellschaften nur bestimmte Daten lokal abspeichern können oder der Einsatz einer Cloud-Lösung in Verbindung mit einem dauerhaft zugewiesenen Server, der speziell für die Datenspeicherung zur Verfügung steht.

Die Datenlokalisierungsvorschriften gelten nach derzeitiger Gesetzeslage nicht für die Verarbeitung von Maschinendaten im Rahmen der Use Cases, es sei denn, dass diese z. B. als Daten aus der Mensch-Maschine-Interaktion (auch) einen Personenbezug haben, wie die Verarbeitung von Login-, Passwort- und Standortdaten der Teilnehmer auf einer Datenaustauschplattform. Etwas anderes gilt etwa dann, wenn im Rahmen des Remote Access sogenannte

„Rendezvous-Systeme“[149] verwendet werden, die in Russland betrieben werden. In diesem Fall greifen für die russischen Server die lokalen Anforderungen. Grundsätzlich ist auch im Rahmen der Datenlokalisierungspflicht eine Übermittlung der Daten ins (nicht-russische) Ausland möglich. Dies gilt allerdings nicht, soweit die Daten als Staatsgeheimnis einzustufen sind. In diesem Fall ist eine Genehmigung seitens der für das jeweilige Staatsgeheimnis zuständigen Behörde erforderlich, die den ausländischen Dritten zum Empfang der Daten und der Durchführung seiner Dienstleistungen unter Wahrung der Geheimhaltung ermächtigt.[150] Unternehmen des Maschinen- und Anlagenbaus können aber grundsätzlich davon ausgehen, dass diese Regelungen für sie nicht zum Tragen kommen.

Für viele nicht-russische Unternehmen hat die Datenlokalisierung Einfluss auf ihre Geschäftsstrategie und die technische Implementierung, allein schon, weil die Datenlokalisierung typischerweise zu erhöhten Kosten in der Datenhaltung führt und die Möglichkeit einschränkt, den russischen Markt als neuen Markt zu erschließen.[151] Hinzu tritt das Risiko von Rechtsverfolgungskosten eines russischen Verfahrens bei Verstoß gegen die Datenlokalisierungsanforderungen.[152]

In der Praxis sollten Unternehmen prüfen, ob sie die von ihnen geplanten Use Cases (Remote Access, Condition Monitoring, Datenaustauschplattform) auch ohne Verarbeitung personenbezogener Daten realisieren können, um so den Datenlokalisierungsanforderungen und den daraus resultierenden Folgen vor vornherein zu entgehen. Ist dies nicht möglich, müssen ausländische Unternehmen entweder eigene technische Vorrichtungen zur Datenlokalisierung vor Ort schaffen, oder mit lokalen Partnern zusammenarbeiten, um die Datenlokalisierung auf deren IT-Systemen und -Produkten entsprechend den russischen Anforderungen zu gewährleisten.

**Telekommunikationsvorschriften**
Verbindliche Anforderungen an die Datenlokalisierung, die unmittelbar nur für in Russland eingetragene und lizenzierte Anbieter von Telekommunikationsdiensten gelten, könnten sich mittelbar auf den Export von Daten aus Russland im Rahmen der digitalisierten Produktion auswirken. Ein lizenzierter Telekommunikationsanbieter ist nämlich verpflichtet, bestimmte Informationen der Nutzer von Telekommunikationsdiensten in Russland zu speichern:

- Informationen über Verkehrsdaten, d. h. Empfang, Übermittlung, Zustellung und Verarbeitung von (Sprach-, Text-, Bild-, Audio- und Video-)Nachrichten des Nutzers für einen Zeitraum von drei Jahren ab dem Zeitpunkt des Abschlusses der genannten Handlungen; und

- seit 1. Juli 2018 Nutzungsdaten, d. h. (Sprach-, Text-, Bild-, Audio- und Video-)Nachrichten des Nutzers für einen Zeitraum von bis zu sechs Monaten.[153]

Ein Telekommunikationsanbieter ist verpflichtet, diese Daten in Russland zu speichern. Die dargestellte Liste ist dabei vom Gesetzgeber bewusst umfangreich gehalten, um alle Daten zu erfassen, die die IT-Systeme des Telekommunikationsanbieters durchlaufen und dieser zur Leistungserbringung verwendet. Ein Export der Daten außerhalb Russlands ist trotz dieser Lokalisierungspflicht möglich und vereinbar, solange die Daten auch in Russland vorgehalten werden.

Wie bei den Betreibern Kritischer Infrastrukturen sind auch hier nur russische Unternehmen Regelungsadressaten und damit für die Einhaltung der genannten Anforderungen verantwortlich und haftbar. Ausländische Maschinenhersteller sind mittelbar betroffen, wenn die russischen Kunden mit ihren (digitalisierten) Produkten Adressaten der entsprechenden Regelungen sind. Unternehmen des Maschinen- und Anlagenbaus, die in Russland selber tätig sind oder russische Kunden aus dem Ausland heraus bedienen, sollten aufmerksam prüfen, ob Regelungen für Telekommunikationsanbieter für ihre digitalisierte Produktion oder ihre digitalisierten Produkte relevant sind und wie ggf. konforme Produkte und Mechanismen in den Geschäftsbetrieb oder das Geschäftsmodell implementiert werden können.

## 5. Regelungen der nationalen Sicherheit

Die russische Regierung hat den Erwerb von ausländischen Waren und Dienstleistungen für staatliche und kommunale Auftraggeber beschränkt[154] und begründet dies mit dem erforderlichen Schutz der russischen Verfassung, zur Gewährleistung der Verteidigung und Sicherheit des Landes, zum Schutz des russischen Binnenmarktes, zur Entwicklung der Volkswirtschaft und zur Unterstützung der russischen Produzenten.[155]

Eine Ausnahme gilt etwa dann, wenn die beschaffende Stelle nachweisen kann, dass keine vergleichbare russische Software existiert, oder die Funktionalitäten der russischen Software denjenigen der ausländischen Software deutlich unterlegen sind.[156] Maschinenhersteller müssen daher im Vorfeld eines Verkaufs an öffentliche russische Stellen prüfen, ob beispielsweise die Steuerungssoftware einer beim Betreiber eingesetzten Maschine (inkl. etwaiger Cloud-basierter Komponenten auf der Infrastrukturebene) diesem Verbot unterliegt, und ihre Produkte ggf. entsprechend lokal ausrichten und/oder vertragliche Rücktrittsrechte für solche Fälle vereinbaren. Alternativ können Maschinenhersteller diese Pflicht zur Prüfung der Maschine und ggf. die Offenlegung der Software durch vertragliche Vereinbarungen dem Kunden, d. h. dem Maschinenbetreiber, auferlegen.

In der Praxis sollten ausländische Maschinenhersteller, die Maschinen unter Verwendung nicht-russischer Software (z. B. als Betriebssystem) an russische Staatsbehörden vertreiben möchten, die Anforderungen an die russische Software und die Bedingungen für die Aufnahme der Software in das Register untersuchen. Dies würde unter anderem (i) einen Kooperationspartner in Russland voraussetzen, um sicherzustellen, dass der Inhaber von IP-Rechten an der Software russisch ist und (ii) erfordern, dass die Software keine zwingenden Updates aus dem Ausland benötigt oder eine Verwaltung aus dem Ausland ermöglicht. Des Weiteren sollte die Software den Anforderungen des eurasischen Registers standhalten. Dies ist ein vom Kommunikationsministerium geführtes Sonderregister, welches erlaubte ausländische Software dokumentiert.[157]

Des Weiteren sind Unternehmen, die personenbezogene Daten in Russland aufbewahren, verpflichtet, diese ggf. auf Anfrage der Behörden offenzulegen. Dies soll der nationalen Sicherheit dienen, um auf diesem Wege z. B. Informationen über terroristische Gruppierungen zu erhalten. Sollte das Unternehmen nicht mit den Behörden kooperieren, droht die Abschaltung des Dienstes.[158] Mit einer möglichen Offenlegungsanfrage sollten Unternehmen, die personenbezogene Daten in Russland verarbeiten, demnach jederzeit rechnen.

**Gesetzesentwurf über das „souveräne Internet“**
Ein weiteres Beispiel für die verstärkt protektionistische Politik der russischen Regierung und die zunehmende staatliche Kontrolle kritischer Internetressourcen ist der Gesetzesentwurf zum „souveränen Internet“ („souveränes RuNet“) durch den das russische Internet vor externen Gefahren geschützt werden soll.[159] Gleichzeitig führt der Gesetzesentwurf zur Territorialisierung und Lokalisierung von Informationsströmen. Im Ergebnis soll das Projekt Russland ermöglichen, sich im Falle einer „Bedrohung“ vom globalen Internet zu entkoppeln. Es soll zum einen sichergestellt werden, dass die russischen Online-Dienste auch dann funktionieren, wenn ausländische Regierungen und Staaten im Konfliktfall die Verbindungen von Russland nach außen unterbrechen. Zum anderen sollte die zuständige Behörde sicherstellen, dass der interne russische Datenverkehr, beispielsweise in Form von E-Mails, im Land verbleibt und nicht abgefangen und analysiert werden kann.

Welche weitreichenden Folgen der Gesetzesentwurf in der Praxis haben wird, ist zum Zeitpunkt der Veröffentlichung der Studie noch nicht erkennbar. Insbesondere müssen unbestimmte Rechtsbegriffe, z. B. was unter einer „Bedrohung der Stabilität“ zu verstehen ist, noch von der russischen Regierung ausgefüllt werden.

**„Roskomnadsor“**
Der Gesetzesentwurf verpflichtet alle russischen Internetprovider zur Installation von spezifischen technischen Mitteln, sowie andere Telekommunikationsanbieter und Eigentümer von Kommunikationsnetzen, Internetzugangspunkten und/oder Telekommunikationsleitungen zur Einhaltung von verbindlichen Anweisungen der Medienaufsichtsbehörde „*Roskomnadsor*“. Diese kann den Datenverkehr im Falle der Bedrohung der Stabilität, Sicherheit oder integralen Kontinuität des Internets und des öffentlichen Telekommunikationsnetzes von russischem Gebiet aus steuern und kontrollieren. Wie genau die erwähnten technischen Mittel aussehen werden, ist zum Zeitpunkt der Veröffentlichung dieser Studie noch nicht erkennbar; diese werden jedenfalls von der russischen Regierung finanziert und den Telekommunikationsdienstleistern kostenlos zur Verfügung gestellt. Klar ist, dass sich sämtliche Soft- und Hardwaresysteme, die zur Bereitstellung der Telekommunikationsdienste und elektronischen Kommunikationsnachrichten verwendet werden, einschließlich Vermittlungsknoten und Server in Russland befinden müssen, um Roskomnadsor Zugang und Kontrolle zu den Systemen zu ermöglichen.

Roskomnadsor wird dabei nicht nur den Datenverkehr überwachen, sondern auch große Datenmengen über die Projektbeteiligten sammeln, z. B. Informationen über das Internetzugangspunkteregister, Telekommunikationsleitungen, die aus Russland hinausführen, Datenverkehrswege sowie Netzinfrastruktur der Projektbeteiligten. Jedem Projektbeteiligten wird aus Übersichtlichkeitsgründen jeweils eine sogenannte „autonome Systemidentifikationsnummer“ zugeteilt. Geplant ist, dass auch bei der täglichen Übertragung von Daten und elektronischen Kommunikationsnachrichten zwischen den Telekommunikationsdienstleistern und den Eigentümern von Kommunikationsnetzen, denen eine „autonome Systemidentifikationsnummer“ zugeteilt wurde, die bei Roskomnadsor registrierten Internetzugangspunkte verwendet werden. Hierdurch droht die Gefahr, dass der Datenverkehr ausschließlich über Russland abgewickelt wird und Fälle, in denen der Datenfluss ins Ausland oder aus dem Ausland nach Russland geleitet wird, eingeschränkt werden. Inwieweit diese Gesetzgebung auch Auswirkungen auf durch Russland verlegte Datenleitungen haben wird, z. B. Datenleitungen von China nach Europa, ist zum Zeitpunkt der Veröffentlichung der Studie nicht ersichtlich.

**Deep Packet Inspections**
Zwar bezieht sich der Gesetzesentwurf nicht ausdrücklich auf die Verwendung von DPI-Filtern („Deep Packet Inspection“),[160] doch können einige Bestimmungen durchaus so ausgelegt werden, dass sie den Einsatz dieser Technologie nahelegen.[161] Die russische Wirtschaftspresse berichtete Ende März 2019, dass Roskomnadsor sich an eine Reihe von Telekommunikationsdienstleistern gewandt hat, um ein russisches DPI-System in ihren Netzwerken zu testen. Ziel des Tests war es herauszufinden, ob das DPI-System Inhalte aus den nach dem Roskomnadsor-Register als verboten deklarierten Quellen filtern kann. Darüber hinaus sollte überprüft werden, ob Datenverkehr grundsätzlich priorisiert und die Zugriffsgeschwindigkeit auf bestimmte Quellen reduziert werden kann.[162]

**Auswirkungen auf ausländische Unternehmen**
Der Gesetzentwurf gilt auf den ersten Blick nicht für grenzüberschreitende Anwendungsfälle, ist aber insbesondere dann von Unternehmen des Maschinen- und Anlagenbaus zu beachten, wenn diese beabsichtigen, ihre Use Cases vor Ort beim Kunden einzurichten und gegebenenfalls Verbindungsknoten für die Übertragung zum Hauptsitz bzw. in die Zentrale in Deutschland nicht mehr frei wählen können. Zur verbesserten Anwendung des Gesetzesentwurfs werden Roskomnadsor und die russische Regierung in Zukunft zahlreiche Nebengesetze erlassen. Maschinen- und Anlagenbauer sollten die weitere Entwicklung, insbesondere den Anwendungsbereich der Nebengesetze im Blick behalten, um ggf. die festgelegten Anforderungen erfüllen zu können.

## 6. Einfuhrkontroll-bestimmungen

Russland ist Mitglied der Eurasischen Wirtschaftsunion (EAWU), die über nichttarifliche Export- und Importkontrollvorschriften verfügt, die unter anderem für den Import ausländischer Verschlüsselungstechnologien nach Russland gelten. Der Beschluss des Kollegialrates der Eurasischen Wirtschaftskommission vom 21. April 2015 Nr. 30 über Maßnahmen der nichttariflichen Regulierung sieht ein detailliertes Verfahren zur Erlangung einer Einfuhrkontrollfreigabe in Form einer Lizenz oder einer Mitteilung in Bezug auf bestimmte aufgelistete Soft- und Hardwaresysteme/Tools vor. Vor der Einfuhr von Produkten nach Russland, die Softwareverschlüsselungswerkzeuge verwenden, sollten Maschinenhersteller und -betreiber diese Produkte daraufhin überprüfen, ob sie unter die bestehenden Einfuhrbeschränkungen fallen und damit eine Einfuhrkontrollabfertigung erfordern. Drucker, Kopierer, Faxgeräte und ihre elektronischen Module sowie Computer – sofern diese Verschlüsselungsfunktionen aufweisen – fallen unter die Anforderungen der Importkontrolle.

# X. Digitalisierungsbarrieren in den USA

## 1. Einführung

Mit einem Volumen von rund 143 Milliarden Euro sind die USA der größte einzelne Ländermarkt im Welthandel mit Maschinen.[163] Mit einem Exportvolumen in die USA von 18 Milliarden Euro liegt Deutschland auf dem vierten Platz der Maschinenimporte.[164] Das Wachstum der weltweiten Maschinenimporte in die USA lag zuletzt bei rund 7 Prozent.[165]

Im Gegensatz zur EU, China und Russland, die international gesehen jeweils eine ausführliche Digitalstrategie verfolgen, ist Ähnliches im gleichen Maßstab für die USA nicht zu erkennen. Am ehesten kann man aus dem traditionell regulierungsaversen Ansatz eine Grundüberzeugung ableiten, der digitalen Innovation und Kommerzialisierung von Daten in hoher Geschwindigkeit entsprechende Freiräume zu verschaffen. Allerdings gewinnt auch in den USA insbesondere das Datenschutzrecht – wenn auch in einem fragmentierten und nicht bundesstaatlich einheitlichen Ansatz – zunehmend an Bedeutung.[166] Auf Ebene der Bundesstaaten gibt es verschiedene Gesetze und Gesetzesentwürfe zum Datenschutz, Cyber Security und Datenlokalisierungsanforderungen.

Dem marktorientierten, regulierungsaversen Ansatz der USA steht trotz fehlender übergreifender Digitalstrategie nicht entgegen, dass industriepolitische Ziele und Interessen gezielt verfolgt und entsprechende Regulierungsinstrumente eingesetzt werden. Die Handelssanktionen sind dafür das im nicht-digitalen Bereich offensichtliche Beispiel. Die Auswirkungen auf digitale Geschäftsmodelle sind weniger offensichtlich, gleichwohl wird das Thema Regulierung von Datenströmen im Rahmen der Politik der US-Administration zu Handelsverträgen inzwischen zunehmend deutlich thematisiert.[167] Hinzu tritt in jüngster Zeit ein dezidiertes Vorgehen gegen chinesische Netzwerkausrüster im Bereich der 5G-Technologie.

### Übersicht zu Prüffeldern in den USA

| Schutz von Geschäftsgeheimnissen | Vorschriften zur Datenlokalisierung | Datenschutzrecht | Ausfuhrkontrollbestimmungen | Handelssanktionen |
|---|---|---|---|---|
| 🟡 | 🟡 | 🔴 | 🟡 | 🟢 |

- 🔴 Starke Auswirkungen
- 🟡 Mögliche Auswirkungen im Einzelfall zu prüfen, Änderungen beobachten
- 🟢 Aktuell keine oder wenige Einschränkungen

**Top-Themen zu amerikanischen Digitalisierungsbarrieren**:

- Geringe Regulierung, wenig Barrieren.
- Orientierung an Best Practices, z. B. für „*Smart Factories*“.
- Handelssanktionen und Auswirkungen auf Aktivitäten in Drittmärkten.
- Zunehmende Relevanz datenschutzrechtlicher Regelungen (fragmentierter Regelungsansatz).

Unternehmen stellt sich insbesondere die Frage, welchen Einfluss der Handelsstreit zwischen den USA und China bzw. Handelssanktionen gegen Russland für die datengetriebenen Geschäftsmodelle von Unternehmen hat oder haben wird, wenn sie sowohl in die USA als auch in China bzw. Russland exportieren bzw. Kundenbeziehungen dorthin unterhalten.

## 2. Schutz von Geschäftsgeheimnissen

Diverse US-Gesetze befassen sich mit dem Schutz von Geschäftsgeheimnissen und Wirtschafts- oder Industriespionage. Dabei liegt der Fokus überwiegend auf dem Schutz vor unberechtigtem Zugriff durch andere Unternehmen bzw. durch ausländische (d. h. nicht-US) Regierungsvertreter.[168] So ermächtigt beispielsweise § 1637 des „National Defense Authorization Act" den Präsidenten, „alle Transaktionen im Eigentum" einer Person zu verbieten, die nach Ansicht des Präsidenten „wissentlich an Wirtschafts- oder Industriespionage im Cyberspace beteiligt ist".[169]

Seit März 2018 gilt der „*Clarifying Lawful Overseas Use of Data Act*" (CLOUD Act), ein US-Gesetz, welches den amerikanischen Behörden Zugriff auf Daten ermöglicht, die von amerikanischen Anbietern von Telekommunikationsdiensten im Ausland gespeichert werden. Die Implementierung des Gesetzes soll unter anderem zum Schutz der öffentlichen Sicherheit dienen. Für die Offenlegungsverpflichtung ist nicht von Relevanz, ob die Daten in einer Cloud oder in einem in- oder ausländischen Datenzentrum gespeichert werden. Selbst bei Bestehen eines lokalen, d. h. nicht-US-amerikanischen, gesetzlichen Verbots über die Weitergabe von Daten, sind amerikanische Telekommunikationsanbieter bei Vorliegen der Anforderungen des CLOUD Acts grundsätzlich zur Offenlegung der Daten verpflichtet. Anbieter von Telekommunikationsdiensten haben jedoch die Möglichkeit, innerhalb von 14 Tage nach Eröffnung des Verfahrens auf Offenlegung einen Antrag auf Änderung oder Aufhebung zu stellen. Dies erfordert, dass (i) der Kunde des Anbieters kein amerikanischer Staatsbürger ist und keinen Wohnsitz in den USA unterhält, sowie (ii) die erforderliche Offenlegung ein erhebliches Risiko für den Anbieter darstellt, z. B. wenn er gegen lokale, d. h. nicht-US-amerikanische, Gesetze verstoßen würde.[170]

Für viele europäische Unternehmen des Maschinen- und Anlagenbaus dürfte die US-Gesetzgebung mit Blick auf den Schutz von Geschäftsgeheimnissen zu kurz greifen, da sie primär die Zugriffe amerikanischer Behörden, etwa unter dem CLOUD Act, beim Einsatz amerikanischer Technologien – etwa im Rahmen des Remote Access oder Condition Monitoring – fürchten. Betreiber von Datenaustauschplattformen könnten in Zukunft die Dienstleistungen unterschiedlicher Anbieter in Anspruch nehmen (z. B. ein amerikanischer Cloud-Anbieter (IaaS) und ein europäischer Plattformtechnologieanbieter („Platform as a Service" (*PaaS*)), um sich nicht einseitig abhängig zu machen und amerikanischer Einflussnahme auszusetzen. Letztlich kann durch eine Umverteilung auf verschiedene Anbieter eine direkte Einflussnahme der amerikanischen Regierung und Behörden bei einer Tätigkeit in den USA, z. B. durch das Anbieten von Condition Monitoring an amerikanische Maschinenbetreiber, nicht vollständig verhindert werden.

In den USA tätige Unternehmen können zudem unter bestimmten Voraussetzungen im Fall der Verletzung von Geschäftsgeheimnissen, einschließlich Herstellungsverfahren, Formeln, Computeralgorithmen, Industriedesigns, Geschäftsstrategien und Kundenlisten, Rückgriffsansprüche gegen ausländische Unternehmen haben.[171] US-Unternehmen, auf deren Geschäftsgeheimnisse unbefugt zugegriffen wird, steht danach ein privates Klagerecht auf Bundesgerichtsebene zu, um Schutz gegen die Veröffentlichung ihrer Geschäftsgeheimnisse zu erlangen.

## 3. Vorschriften zur Datenlokalisierung

In einer Studie der „*U.S. International Trade Commission*" wurden Datenlokalisierungsvorschriften, wie z. B. die Anforderung Daten auf lokalen Servern aufzubewahren, von US-Unternehmen am häufigsten als digitale Handelsbarrieren

identifiziert.[172] Dementsprechend planen die USA im Gegensatz zu China und Russland zum Zeitpunkt der Veröffentlichung der Studie keine Verschärfung der amerikanischen Datenlokalisierungsregelungen. Im Gegenteil: Der Kongress untersuchte im März 2019 globale Digitalisierungsbarrieren, um Lösungen zu entwickeln, wie den weltweiten protektionistischen Tendenzen entgegen getreten werden könnte.[173]

Auch die US-Handelskammer empfiehlt der US-Regierung, mittels Handelsabkommen und über multilaterale Foren wie die G7, G20, OECD, APEC, die Vereinten Nationen und die WTO weiterhin auf den weltweiten Abbau von Datenlokalisierungsvorschriften hinzuwirken und einheitliche Regelungen einzuführen.[174] Weiter empfiehlt die US-Handelskammer, dass die *National Telecommunications and Information Association* (NTIA) mit den relevanten Interessengruppen zusammenarbeitet, um mit einem ganzheitlichen Ansatz den Prioritäten der USA im digitalen Bereich (einschließlich der in diesen Sektor tätigen weltweit führenden Unternehmen) möglichst umfassend Geltung zu verschaffen. Dazu gehört, dass die USA ihre bislang nur punktuell, z. B. sektorspezifischen, Datenlokalisierungsvorschriften vereinheitlichen oder abschaffen. Die Handelskammer wünscht insbesondere, dass sich die US-Regierung bei ihren Bemühungen auf die Vorteile und die Notwendigkeit grenzüberschreitender Datenflüsse hin zu einer modernen Digitalwirtschaft konzentriert und darauf, wie politische Prioritäten durch andere regulatorische oder politische Maßnahmen erfüllt werden können, die keine Datenlokalisierung erfordern.[175] Ziel der zukünftigen amerikanischen Digitalisierungspolitik soll es vielmehr sein, in einem globalen Vorgehen grenzüberschreitenden Datenverkehr zu fördern und Digitalisierungsbarrieren abzubauen.[176]

## 4. Datenschutzrecht, Datensicherheit und IoT

**Datenschutzrecht**

Im Bereich des Datenschutzes liegt der Fokus des US-Gesetzgebers weitgehend auf Verbraucherdaten und nicht auf solchen Daten, wie sie typischerweise von Maschinen- und Anlagenbetreibern erhoben werden.[177] Dementsprechend wenig Einfluss hat die im Folgenden skizzierte Gesetzgebung zum Zeitpunkt der Veröffentlichung der Studie auf die Geschäftspraktiken von Maschinen- und Anlagenbauern. Da die Idee eines Datenschutzgesetzes auf Bundesebene, das der DS-GVO ebenbürtig ist und als Rahmen zur Lösung verschiedener Probleme im digitalen Bereich dienen könnte, immer mehr Schwung aufnimmt,[178] sollten Maschinen- und Anlagenbauer diese Entwicklung jedoch im Blick behalten.

Mangels einer einheitlichen bundesstaatlichen Regelung haben derzeit die meisten Bundesstaaten eigene Regelungen zum Umgang mit Datenschutzverletzungen.[179] Zur Förderung eines einheitlicheren Ansatzes hat die US-Regierung das *National Institute of Standards and Technology* (NIST) beauftragt, datenschutzrechtliche Rahmenbestimmungen zu entwickeln; die NTIA arbeitet entsprechend an einer Reihe von Datenschutzgrundsätzen, um einen nationalen rechtlichen und politischen Ansatz zu verfolgen.[180] In der Zwischenzeit haben einige Bundesstaaten damit begonnen, schärfere Datenschutzgesetze für bestimmte Bereiche, z. B. biometrische Daten, zu erlassen.[181] Kalifornien gilt als Paradebeispiel des amerikanischen Datenschutzes und hat das strengste Datenschutzgesetz der USA verabschiedet („*California Consumer Privacy Act*"), das einige der wesentlichen Anforderungen der DS-GVO übernimmt und am 1. Januar 2020 in Kraft tritt.[182] Diese Gesetze sind nur für Maschinenbetreiber mit direktem Verbraucherkontakt relevant und dürften damit keine (hemmende) Wirkung für die Mehrzahl der Maschinen- und Anlagenbauer entfalten.[183]

Einige Bundesstaaten haben zudem Gesetze zu formalen Richtlinien der Informationssicherheit im Rahmen der Verarbeitung personenbezogener Daten erlassen.[184] Im Laufe des Jahres 2018 haben fast 35 Staaten insgesamt mehr als 265 Gesetzesvorlagen oder Resolutionen zum Thema Cyber-Security eingebracht oder berücksichtigt.[185] Einige Staaten, wie z. B. Massachusetts, verlangen von jeder Person oder Gesellschaft, die personenbezogene Daten besitzt oder lizenziert, die Implementierung eines umfassenden Informationssicherheitsprogramms.[186] Allerdings gelten diese Anforderungen ausschließlich für

bestimmte Arten von personenbezogenen Daten von US-Bürgern und nicht für nicht-personenbezogene Daten, z. B. Maschinendaten.

**Gesetzliche Regelungen zu IoT**
Auch mit Blick auf das Thema IoT gibt es bislang nur fragmentierte Regelungen einzelner Staaten, die sich mit Datenerfassung, Privatsphäre und Sicherheit von vernetzten Geräten („*Connected Devices*“) befassen. So hat beispielsweise Kalifornien kürzlich ein Gesetz erlassen, das einen Hersteller eines vernetzten Geräts verpflichtet, das Gerät mit angemessenen Sicherheitsvorkehrungen auszustatten, die der Art und Funktion des Geräts entsprechen und die alle im Gerät enthaltenen Informationen vor unbefugtem Zugriff, Zerstörung, Verwendung, Änderung oder Offenlegung schützen sollen.[187] Wenn auf das Gerät außerhalb eines lokalen Netzwerks mit einem Passwort zugegriffen werden kann, muss es entweder mit einem eindeutigen Passwort für jedes Gerät ausgestattet sein oder die Benutzer zwingen, bei der ersten Verbindung ihr eigenes Passwort festzulegen. Während dieses Gesetz vorwiegend „verbraucherorientiert“ ist und sich damit nicht direkt an Maschinenhersteller richtet, können ggf. kundenseitig Maschinenbetreiber betroffen sein, die ihre Produkte nun auf die neue Gesetzgebung anpassen müssen. Relevant ist dies beispielsweise für Maschinenbetreiber, die ihre Produkte mittels Remote Access überwachen, um diese ggf. zu aktualisieren und/oder Fehler zu beheben.

**Gesetzliche Anforderungen an Cyber-Security**
In Ermangelung rechtlicher standardisierter Cyber-Security-Anforderungen haben Unternehmen Best Practices und Industriestandards, einschließlich Risikomanagement-Frameworks, implementiert.[188] Hierzu zählt z. B. das „*Cybersecurity Framework*“ des NIST, das Unternehmen einen Richtlinienrahmen für Cyber-Security zur Verfügung stellt.[189] Unternehmen müssen darauf vorbereitet sein, mit den Strafverfolgungsbehörden des Bundes und der Bundesstaaten in Fragen der nationalen Sicherheit, einschließlich Verschlüsselung, zusammenzuarbeiten.[190]

Insbesondere für Maschinenbetreiber, die mit dem Internet verbundene Maschinen einsetzen, Cloud Computing nutzen oder Daten zwischen oder mit anderen Unternehmen teilen, ist Cyber-Security ein kritisches Thema. In den USA legt das NIST nationale Mess- und Interoperabilitätsrahmen fest. Bis heute gibt es keinen einheitlichen Cyber-Security-Standard, obwohl Wissenschaftler und Ingenieure des NIST eine Reihe von Richtlinien zusammengestellt haben, die von Herstellern berücksichtigt werden sollten.[191] Das NIST hat zudem einen internen Bericht veröffentlicht, um Unternehmen dabei zu helfen, die mit ihren IoT-Geräten verbundenen Cyber-Security- und Datenschutzrisiken während ihres gesamten Lebenszyklus besser zu verstehen und zu verwalten. Der Entwurf enthält auch Empfehlungen, wie Risikoüberlegungen für diese Geräte angegangen werden können.[192]

**Cyber-Security Best Practices für “Smart Factories”**
Demnach umfassen allgemeine Best Practices für die Cyber-Security für Maschinenbetreiber:

- Beurteilung der Cyber-Security-Reife und der Abwehrmaßnahmen des Betreibers;
- Inventarisierung aller industriellen Netzwerkanlagen und Überwachung des Systems des Betreibers in Echtzeit auf Bedrohungen und Risiken;
- Schulung der Mitarbeiter über industrielle Netzwerke und bewährte Verfahren zur Cyber-Security;[193]
- Wenn der Betreiber eine Cloud-Infrastruktur nutzt, sollten alle Cyber-Security-Protokolle Maßnahmen zur Datenintegrität und Datenvertraulichkeit beinhalten;
- Überprüfung von Reaktionsplänen und Durchführung von Übungen/Tests zur Förderung der Compliance.

Derzeit erstellen US-Beratungsunternehmen und Unternehmensstrategieunternehmen Studien zu Bedrohungsszenarien und Best Practices der Branche.[194] Des Weiteren wurde ein Entwurf des Implementierungsleitfadens „NISTIR 8183A“ für das *Cybersecurity Framework*

*(CSF) Manufacturing Profile Low Security Level* entwickelt, um Maschinenhersteller bei der Handhabung ihres Cyber-Security-Risikos zu unterstützen. Der Leitfaden ist konkret auf die Ziele und Bedürfnisse des Fertigungssektors sowie Best Practices der Industrie ausgerichtet.[195]

## 5. Ausfuhrkontroll-bestimmungen (Exportkontrolle)

Ähnlich wie für die anderen Zielmärkte kann US-Exportkontrollrecht die Übermittlung von Daten an und von bestimmten Unternehmen und Regionen einschränken.[196] Die „*Export Control Reform Initiative*“[197] („**Reforminitiative**“) der US-Administration führte zu einer grundlegenden Reform des bisherigen Exportkontrollsystems mit dem Ziel, die nationale Sicherheit der USA zu erhöhen und die USA darin zu stärken, Bedrohungen wie der Verbreitung von Massenvernichtungswaffen zu begegnen. Das US-Exportkontrollrecht greift dann nicht, wenn Maschinen- und Anlagenbauer ihre Maschinen in den USA betreiben, Produkte in den USA verkaufen und keine Produkte/Technologien exportieren und keine der anfallenden Maschinendaten im Rahmen von Remote Access, Condition Monitoring und Datenaustauschplattformen über die Grenzen der USA hinweg übermitteln.

**EAR und BIS**

Soweit Maschinenbetreiber technische Daten, Geräte oder Software aus den USA exportieren möchten, kann dies die „*International Traffic in Arms Regulation*“ (ITAR) auslösen, wodurch Maschinenbetreiber eine Genehmigung oder die „*Export Administration Regulation*“ (EAR) Freigabe durch das „*Bureau of Industry and Security*“ (BIS) benötigen.

Das BIS schränkt den Import/Export von Verschlüsselungstechnologien aus einem Nicht-US-Gebiet in ein anderes Nicht-US-Gebiet dann vollständig ein, wenn eine vergleichbare Technologie in die USA und gleichzeitig in ein (durch das BIS identifizierte) „*bad actor*“ Land importiert/exportiert wird.[198] Hintergrund sind dabei die der Kontrolle zugrundeliegenden nationalen Sicherheitsinteressen der USA. Wann eine EAR Freigabe erforderlich ist, hängt stark von den jeweiligen Eigenschaften der Technologie ab, z. B. von der Art, Funktionsweise und dem Verwendungszweck der Verschlüsselung (oder Verschlüsselungssoftware) sowie der verwendeten Komponenten. Um einschätzen zu können, ob kommerzielle Software/Verschlüsselungstechnologien aufgrund ihrer Klassifizierung der Exportkontrolle nach den EARs unterliegen, ist eine Betrachtung der funktionalen Merkmale der Software/Verschlüsselungstechnologien erforderlich.

**Verschlüsselungstechnologien, die nicht unter die Exportkontrolle fallen**

Grundsätzlich beschränkt die US-Regierung ihre Kontrolle von Verschlüsselungssoftware auf die „Verschlüsselung zur Vertraulichkeit von Daten“ (“*Cryptography for Data Confidentiality*”). Viele gängige Verschlüsselungsarten und -funktionen unterfallen dabei nicht der Exportkontrolle. Kurz gesagt, die US-Regierung kontrolliert die Verschlüsselungstechnologien, die die Verschlüsselung von Daten zulassen, aber nicht solche Verschlüsselungstechnologien, die nur zur Überprüfung der Benutzeridentität, zur Bestätigung der Herkunft oder Integrität von Daten oder zum Schutz dessen verwendet wird, was bereits aus anderen rechtlichen Gründen geschützt ist, wie urheberrechtlich geschützte Werke oder vertrauliche medizinische Unterlagen.[199] Beispielsweise unterliegen die folgenden Arten der Verschlüsselungssoftware/-technologie in der Regel nicht den US-Exportkontrollbestimmungen:

- Authentifizierungsverschlüsselung: Diese Art der Verschlüsselung dient der Überprüfung der Identität eines Benutzers, Prozesses oder einer Vorrichtung und ist oft Voraussetzung für den Zugriff auf Ressourcen in einem Informationssystem. Hierunter fallen beispielsweise die Überprüfung der Herkunft oder des Inhalts einer Nachricht oder anderer Informationen sowie alle anderen Aspekte der Zugangskontrolle, bei denen Dateien und Texte – mit Ausnahme von Passwörtern, persönlichen Identifikationsnummern oder ähnlichen Daten, die vor unbefugtem Zugriff geschützt werden sollen – nicht verschlüsselt werden.

- Verschlüsselung von digitalen Signaturen, Datenintegrität und Unbedenklichkeitsnachweisen: Diese Art der Verschlüsselung bietet die Möglichkeit, die Integrität und Herkunft der Daten nachzuweisen, verschlüsselt die Daten selbst aber nicht.

- Verschlüsselung bei der digitalen Lizenzverwaltung: Diese Art der Verschlüsselung schützt Urheberrechte, indem sie überprüft, ob jemand das Recht hat, Inhalte herunterzuladen, anzuzeigen oder zu nutzen.

## 6. Handelssanktionen und protektionistische Handelspolitik

Die protektionistische Handelspolitik der gegenwärtigen US Administration wird begleitet von Neubewertungen und Nachverhandlungen internationaler Handelsabkommen[200] und verhängter Handelssanktionen gegen Handelspartner der USA.[201] Ging man zunächst davon aus, dass die USA sich mit dieser Strategie nur selbst schaden würden,[202] so scheinen die Handelspartner inzwischen mehr unter dem Handelskonflikt zu leiden als die USA.[203] Zwar scheinen sich diese protektionistische Handelspolitik und der Handelsstreits mit z. B. China noch nicht unmittelbar auf die digitalen Dienste der Maschinen- und Anlagenbauer auswirken. Soweit sich allerdings die Konjunktur in China aufgrund der Handelssanktionen abschwächt, wird dies auch auf die Nachfrage nach Maschinen aus Deutschland in China durchschlagen.

Auswirkungen der von der vorigen US Administration initiierten und der EU mitgetragenen Handelssanktionen können Maschinen- und Anlagenbauer, die digitale Dienste anbieten, in Einzelfällen bereits jetzt spüren. Dies ist z. B. dann der Fall, wenn in Russland (etwa im Wege des Condition Monitoring) generierte Maschinendaten nicht auf in den USA betriebenen Maschinen genutzt werden dürften. Ein anderes denkbares Szenario ist, dass Maschinen- und Anlagenbauer aufgrund der Handelssanktionen daran gehindert werden, mit russischen Kunden zu kontrahieren, wenn sie zugleich in den USA aktiv sind und eine Datenaustauschplattform für eine Vielzahl von Teilnehmern aus unterschiedlichen Ländern betreiben möchten. Eine multilaterale Datenaustauschplattform scheitert dann ggf. bereits daran, dass sich auch russische Kunden einloggen können.

# XI. Handlungsempfehlungen und Ausblick

## 1. Handlungsempfehlungen an Unternehmen

### Klare Digitalstrategie

**Wenn Unternehmen von Anfang an potenzielle Digitalisierungsbarrieren auch beim Auf- und Ausbau neuer und innovativer Geschäftsmodelle in den Blick nehmen, lassen sich hierdurch oft erhebliche Kosten vermeiden.**

Potenzielle regulative Digitalisierungsbarrieren müssen in Unternehmen oft hinter dem Momentum der Innovationen zurückstehen, insbesondere, wenn sich die digitalisierte/n Produktion und Produkte noch in der Auf- und Ausbauphase befinden. Unternehmen sollten sich jedenfalls mit den unterschiedlichen regulatorischen Anforderungen und Marktbedingungen vertraut machen und eine klare Strategie zum Umgang mit (potenziellen) Digitalisierungsbarrieren entwickeln. Hierdurch können ggf. anfallende zusätzliche Kosten (z. B. Partnerunternehmen in Russland) oder lokale Anforderungen (z. B. Datenspeicherung in China) bereits von Anfang an einbezogen und gewichtet werden.

Richtet ein Unternehmen beispielsweise von Anfang an sein Geschäftsmodell (zumindest in den Grundzügen) datenschutzkonform aus, erspart es sich nachträglich, das Geschäftsmodell ggf. kostenintensiv zu überprüfen und anzupassen, um die regulatorischen Vorgaben einzuhalten. Dabei zeigt sich, dass mit der DS-GVO das europäische Datenschutzrecht immer mehr Staaten als Vorbild für eigene Datenschutzgesetze dient. Unternehmen, die ihre Geschäftsmodelle auf das europäische Datenschutzniveau ausrichten, werden damit voraussichtlich in Zukunft auch in einer Vielzahl anderer Länder die dortigen Vorgaben erfüllen.

Insbesondere Unternehmen, deren Strukturen sich noch im Aufbau befinden, können hier von Anfang an flexible Ansätze wählen, die später die Einhaltung der anwendbaren Vorschriften erleichtern. Beispielsweise können Betreiber von Datenaustauschplattformen Dienstleistungen unterschiedlicher Anbieter in Anspruch nehmen (z. B. ein lokaler Cloud-Anbieter (IaaS) und ein europäischer Plattformtechnologieanbieter (PaaS)), um sich nicht einseitig der Einflussnahme eines bestimmten Marktes auszusetzen. Denkbar ist auch, zunächst eine Plattform in einem regional begrenzten Markt zu entwickeln (z. B. in Europa) und mit dieser dann in andere Märkte zu expandieren und sie dabei den weiteren örtlichen Begebenheiten anzupassen.

### Stärkung von Vertrauen in digitalisierte Produkte

**Unternehmen können sich durch sichere und vertrauenswürdige digitale Produkte einen Marktvorteil gegenüber weniger gut aufgestellten Mitbewerbern verschaffen.**

Unternehmen sollten überlegen, wie sie das Vertrauen von Lieferanten und Kunden in ihre digitalisierten Produkte stärken können. Insbesondere mit Blick auf die Unsicherheiten, die sich durch potenzielle Zugriffe nationaler Regierungen ergeben, bedürfen Kunden eines vertrauensvollen Verhältnisses zu Maschinen- und Anlagenbauern. Beispielsweise kann die Verwendung standardisierter Schnittstellen durch Betreiber von Datenaustauschplattformen ein vertrauensbildendes Element zu Kunden und Lieferanten sein. Auch die Verwendung von anerkannten Verschlüsselungstechnologien für die Datenübermittlung kann ein vertrauensbildendes Moment darstellen. Beispielhaft lässt sich der technische Standard IEC 62443 (und die entsprechenden lokalen Adaptionen) als zentraler und anerkannter Standard für die Sicherheit von Automatisierungstechnik, Maschinen und Anlagen („*Industrial Control System Security*“) anführen.

Unternehmen können sich auch an diversen nationalen und globalen Initiativen beteiligen. Bereits sehr etabliert ist die „*International Data Spaces Association*“ (IDSA), durch welche sich Wirtschaft und Forschung aktiv an der Gestaltung einer vertrauenswürdigen Architektur für die Datenwirtschaft beteiligen.[204] Ziel der IDSA ist es, die Datenhoheit durch eine offene, herstellerunabhängige Architektur für ein Peer-to-Peer-Netzwerk zu gewährleisten, das die Nutzungskontrolle von Daten aus allen Bereichen ermöglicht.[205]

Weiterhin ist „Security by Design“[206] für ein System, das frei von angreifbaren Schwachstellen sein soll, unerlässlich. Darum wird das System von Anfang an so sicher und unangreifbar wie möglich konzipiert. Dies geschieht z. B. durch kontinuierliche Tests, sichere Authentifizierung, aber auch durch Schulungen der Mitarbeiter und Sicherstellung der Systemintegrität in den Betrieben der Kunden.

### Einstellen auf lokale Divergenzen

**Global agierende Unternehmen dürfen im digitalen Umfeld nicht nur auf eine einzige international anwendbare Lösung setzen; sie müssen ihre Lösungen spezifisch auf die jeweiligen Märkte und deren regulatorische Anforderungen ausrichten.**

Unternehmen müssen sich auf heterogene Regulierung in den verschiedenen Märkten einstellen und lernen, lokal vorzugehen. Hierzu bieten sich mehrere Ansätze an: Unternehmen können Systeme oder Plattformen in einem begrenzten Markt entwickeln (z. B. in Europa) und diese dann in andere Märkte migrieren und ggf. dort entsprechend der Kundennachfrage lokalisieren.

Alternativ können Unternehmen einen pragmatischen Ansatz verfolgen und digitale Verarbeitungsprozesse im jeweiligen Land belassen, z. B. durch den Aufbau von Betriebsstätten vor Ort. Soweit dies insbesondere für KMUs zu aufwändig ist, bietet sich der Weg zur Kooperation mit lokalen oder internationalen Partnern an. Diese agieren bereits unter den bestehenden Rahmenbedingungen und ermöglichen den Maschinen- und Anlagenbauern, ihre digitalen Dienste auf die regulatorischen Anforderungen auszurichten.

Über das Erfordernis der Anpassung an lokale Anforderungen sollte nicht vergessen werden, dass der Erfolg der Use Cases in der Verarbeitung und Auswertung großer Datenmengen sowie unterschiedlicher Datenquellen liegt. In dem Zusammenhang kommt Datenaustauschplattformen eine entscheidende Funktion zu. Unternehmen müssen ihre Maschinendaten aus unterschiedlichen Maschinen, Standorten und Ländern zusammenführen, um diese Synergien, etwa im Bereich Predictive Maintenance, gewinnbringend und zukunftsorientiert auszunutzen. Selbst wenn man den Fokus auf große Märkte, z. B. China, legt, lassen sich die gewünschten Effekte nicht erzeugen, wenn Unternehmen kleinteilig nur auf lokaler Ebene bzw. auf vielen lokalen Ebenen agieren. Eine Lösungsmöglichkeit für KMUs wäre eine Zusammenführung von Daten über eine neutrale Datenaustauschplattform.[207] Über eine solche Plattform können für die einzelnen Unternehmen die Transaktionskosten für individuelles Compliance-Monitoring reduziert werden. Eine Auswertung von Datenströmen könnte dann auf eine dezentrale Datenauswertung hinauslaufen. Datenübermittlungen werden ggf. reduziert oder nur noch auf die Auswertung selbst beschränkt und aus diesen Erkenntnissen können Unternehmen dann Datenmodellierung betreiben.

### Einbringung in Gesetzgebungsverfahren

**Soweit sich behördliche Regelungen und Gesetze noch in der Entstehungsphase befinden, sollten Unternehmen die Möglichkeiten nutzen, sich in geeigneter Form – auch ggf. mit Blick auf ausländische Gesetzgebung – an der Diskussion zu anstehenden Gesetzgebungsverfahren zu beteiligen.**

Interessierte Unternehmen können sich zu diesem Zweck je nach Zielmarkt an unterschiedliche Organisationen wenden. In China sind die richtigen Anlaufstellen die European Union Chamber of Commerce, die AHK und der VDMA. In der EU können hierfür ORGALIM und der VDMA angesprochen werden.

In Russland können sich auch nicht-russische Unternehmen in das derzeitige Gesetzgebungsverfahren zum russischen Digital-Programm einbringen.[208] Dies soll sicherstellen, dass auch Unternehmensinteressen und Branchenfachwissen in die Umsetzung des Digital-Programms über die Digitalwirtschaft einfließen. Aus diesem Grund wurden unter der Leitung der autonomen, nicht kommerziellen Organisation „Digitale Wirtschaft“[209] eine Reihe von Arbeitsgruppen und Kompetenzteams eingerichtet. Über diese Arbeitsgruppen können russische und nicht-russische Unternehmen ihre Interessen bei der Umsetzung des Digital-Programms einbringen.

Zudem können russische und nicht-russische Unternehmen Bedenken und Anliegen an den zuständigen Ombudsmann[210] richten. Dieser, vom Präsidenten ernannte, Staatsbeamte setzt sich für den Schutz der Rechte und Interessen russischer und ausländischer Unternehmen in Russland ein.

## 2. Handlungsempfehlungen an den VDMA

### Unterstützung durch Handreichungen und Veranstaltungen

**Der VDMA sollte auf Grund der hohen Komplexität der Themen Unterstützung in geeignetem Umfang zur Verfügung stellen.**

Empfehlenswert ist dabei die Fokussierung des Themas „Internationale Digitalisierungspolitik" auf einen Ansprechpartner. Dieser könnte das Thema zentral handhaben und den spezifischen Input aus den unterschiedlichen Abteilungen und Arbeitskreisen bündeln.

Die deutlichen Unterschiede zwischen dem Digitalisierungsstand der Unternehmen des Maschinen- und Anlagenbaus stellen den VDMA vor die Aufgabe, die Unternehmen mit den richtigen Informationen zu adressieren und in den jeweils relevanten Fragestellungen zu unterstützen. Unternehmen, die mit der Digitalisierung ihrer Produktion und Produkte bereits weit fortgeschritten sind, machen sich vermehrt Gedanken um Digitalisierungshindernisse und den globalen (digitalen) Protektionismus. Andere Unternehmen wollen zunächst den Fokus auf ihre eigene Digitalisierung legen und sehen Digitalisierungsbarrieren für sich selbst eher als Zukunftsthema. Seitens des VDMA könnten z. B. Handreichungen und Veranstaltungen zu den unterschiedlichen Digitalisierungsbarrieren und Zielmärkten hilfreich sein.

**Ausarbeitung von Verhaltensregeln unter der DS-GVO**

Der VDMA sollte überlegen, inwieweit die Entwicklung von Verhaltensregeln zur Anonymisierung und Pseudonymisierung personenbezogener Daten im Bereich des Maschinen- und Anlagenbaus im Rahmen der Digitalisierungspolitik sinnvoll sein könnte und sich unter Umständen entsprechenden Initiativen auf europäischer Verbandsebene anschließen.

Mit Blick auf die kritische Frage der erfolgreichen Anonymisierung und Pseudonymisierung personenbezogener Daten bietet es sich möglicherweise an, dass der VDMA Verhaltensregeln (Art. 40 DS-GVO) für die Use Cases Remote Access und Condition Monitoring entwickelt und durch den Genehmigungsprozess nach Art. 40, 41 DS-GVO bringt. Damit könnte unter Umständen eine erhebliche Hilfestellung und Arbeitserleichterung, insbesondere für die kleineren und mittleren Unternehmen, für all diejenigen Fälle geschaffen werden, in denen die Verarbeitung personenbezogener Daten eher einen „Beifang" der Verarbeitung von Maschinendaten darstellt.

**Dialog mit Regierungen und Organisationen**

Da sich viele behördliche Regelungen und Gesetze zur Ausformung und Ergänzung des chinesischen Cyber-Security-Gesetzes noch in einem frühen Vorbereitungsstadium befinden und die Gesetzgebung und Vorgabe behördlicher Leitlinien stark von der Politik beeinflusst ist, ist zu empfehlen, dass internationale Unternehmen (über Handelsorganisationen, die ihre Interessen in China vertreten) in den Dialog mit der Bundesregierung als Intermediär zwischen den Unternehmen und der chinesischen Regierung treten. Ein solches Vorgehen könnte z. B. durch das VDMA-China-Büro koordiniert werden. Da in China der direkte Zugang zur Regierung auch für internationale Handelsorganisationen (z. B. Handelskammern, Verbände) relativ beschränkt sein dürfte, ist insbesondere der Dialog auf Regierungsebene bzw. EU-China Ebene von entscheidender Bedeutung. Des Weiteren ist eine Beteiligung an öffentlichen Diskussionen des Technischen Komitees über Änderungsentwürfe möglich.[211]

Auf EU Ebene ist zu empfehlen, in den Dialog mit der Deutschen Gesellschaft für Internationale Zusammenarbeit (GIZ) zu treten, die zunehmend globale Digitalisierungsprojekte initiiert und weltweite Kooperationen anstrengt.

## 3. Handlungsempfehlungen an die Politik

Die Politik muss Unternehmen in der Umsetzung digitaler Geschäftsmodelle insoweit unterstützen, dass sie protektionistisch-regulatorischen Strömungen entgegen wirkt und den freien Datenverkehr fördert. Dazu gehören sowohl Maßnahmen mit Vorbildfunktion, die auf der Ebene des nationalen und EU-Rechts greifen (DS-GVO, international technische Standards für den Datenaustausch und Cybersicherheit, Referenzarchitektur der IDSA), wie auch die vertiefte Ansprache und Regelung digitaler Fragen und dabei insbesondere des freien Datenverkehrs im Rahmen internationaler Handelsabkommen mit den wichtigen Zielmärkten China, Russland und USA.

### Mehr Transparenz

**Regierungen und internationale Organisationen können Unternehmen im Umgang mit (lokalen) Digitalisierungsbarrieren durch verstärkte Transparenz der relevanten Regelungen unterstützen.**

Das Bundesministerium für Wirtschaft und Energie und internationale Organisationen sollten eine bessere weltweite Transparenz für Regelungen des digitalen Protektionismus gewährleisten, um Unternehmen einen besseren Überblick über Digitalisierungsbarrieren zu verschaffen und diese langfristig mittels Handelsabkommen abzubauen.[212] Beispielhaft ist hier der „*Digital Trade Restrictiveness Index*" von ECIPE anzuführen, der in transparenter Weise darlegt, wie und mit welchen Mitteln 64 untersuchte Länder den digitalen Handel beschränken.[213] Wünschenswert ist, eine ähnliche Aufstellung auch branchenspezifisch zu erstellen, damit z. B. Maschinen- und Anlagenbauer besser einschätzen können, welche Digitalisierungsbarrieren für sie in den einzelnen Ländern relevant sind.

### Handelsabkommen

**Die Bundesregierung sollte aktiv darauf hinwirken, die Rahmenbedingungen für den freien Datenverkehr und globale Digitalisierung in weltweiten bi- und multi-lateralen Abkommen festzulegen.**

"The future of trade is the future of data."[214] Mit Handelsabkommen, insbesondere im Bereich Digitalwirtschaft ist es möglich, rechtliche Fragmentierungen und Barrieren global abzubauen und den Zugang zu wichtigen Ressourcen, einschließlich IKT-Systeme, zu regeln.[215] Das Risiko eines Datenzugriffs durch nationale Sicherheitsbehörden und womöglich einer damit einhergehende Ausspähung von Geschäftsgeheimnissen bzw. Maßnahmen aktiver Wirtschaftsspionage lässt sich unternehmensseitig allenfalls eingrenzen, aber nicht vollständig verhindern. Regierungen sollten jedoch aktiv darauf hinwirken, die Rahmenbedingungen für den freien Datenverkehr und globale Digitalisierung in weltweiten bi- und multilateralen Abkommen festzulegen und ggf. Lokalisierungsvorschriften abzubauen. Hierdurch kann der Fragmentierung, die durch nationale protektionistische Regelungen entsteht, entgegengewirkt und Unternehmen die Unsicherheit im Umgang mit grenzüberschreitenden Datenströmen genommen werden.

Die EU Kommission hat angekündigt, die Möglichkeiten der Neuverhandlung und Ergänzung von EU-Handelsabkommen zu nutzen, um Regeln für den elektronischen Geschäftsverkehr und den grenzüberschreitenden Datenverkehr festzulegen und gegen neue Formen des digitalen Protektionismus vorzugehen.[216]

Den globalen Datenschutz sieht die EU dabei als gesonderte Materie an, der nicht zur Handelsware werden soll.[217] Vielmehr sieht sich die EU als Vorreiter eines modernen Datenschutzes, der Drittländern als Bezugsrahmen dienen soll, eigene Rechtsvorschriften in diesem Bereich zu entwickeln. Entsprechend setzt die EU Kommission auf Gespräche mit ihren internationalen Partnern, um die Konvergenz durch die Entwicklung hoher und interoperabler Standards für den Schutz personenbezogener Daten weltweit zu fördern.[218] Ferner möchte sie die Zusammenarbeit mit den Datenschutz- und Aufsichtsbehörden in Drittländern verstärken, um die wirksame

Durchsetzung der Datenschutzvorschriften zu erleichtern, auch durch gegenseitige Vereinbarungen über die Amtshilfe.[219] Im Januar 2019 hat die EU Kommission mit ihrer Angemessenheitsentscheidung zu Japan ein klares Zeichen gesetzt und zusammen mit den japanischen Behörden den weltweit größten Raum für die Übermittlung personenbezogener Daten nach den Anforderungen des EU-Rechts geschaffen.[220] Die Schaffung ähnlicher Freiräume für den freien Datenverkehr nicht-personenbezogener Daten sollte nun das nächste große Ziel der EU sein.

## 4. Ausblick

Der Maschinen- und Anlagenbau hat ein vitales Interesse an freiem Datenverkehr, sei es zum Aufbau neuer datenbasierter Geschäftsmodelle, sei es zur beständigen Weiterentwicklung der eigenen Produkte und etablierter Dienste, die auf die Auswertung von Maschinendaten angewiesen sind, um auch in Zukunft ihren internationalen Stellenwert und Marktführerschaft beizubehalten bzw. auszubauen. Für Maschinen- und Anlagenbauunternehmen führen Digitalisierungsbarrieren in der Regel nicht unmittelbar und zwangsläufig zur Abschottung des Zugangs zu einzelnen Märkten. Vielmehr gibt es eine Vielzahl regulatorischer Stellschrauben, die sich im Ergebnis als Digitalisierungsbarrieren bei der Umsetzung der in Rede stehenden Use Cases auswirken können. Die Themen der Datenlokalisierung (Beispiel Russland für personenbezogene Daten), technischer und de facto Standards für Datenübertragung nach und aus China (Beispiel VPN-Dienste) sowie die Regulierung bzw. Beschränkung von Verschlüsselungsanforderungen sind dafür nennenswerte Beispiele. Unternehmen müssen den Umgang mit den einzelnen lokalen Regelungen im weltweiten Zusammenspiel beständig verfolgen, um sich frühzeitig auf die sich daraus für Unternehmen resultierenden Folgen, einschließlich eventueller Bußgelder, vorzubereiten und ggf. präventive Maßnahmen, z. B. die Rückstellung finanzieller Mittel, zu treffen. Zusätzlich sollten Unternehmen bestehende Spielräume ausnutzen und sich aktiv in die voranschreitende Gesetzgebung zu den Themen Digitalisierung und freier Datenverkehr einbringen.

Von der Politik ist zu fordern, Unternehmen darin zu unterstützen, den latent-protektionistischen Strömungen bzw. der Eingrenzung des freien Datenaustauschs im industriellen Umfeld entgegen zu wirken bzw. nach Mitteln zu suchen, dem positive Gegenbeispiele entgegen zu halten, wie sie sich z. B. für Datenaustauschplattformen in der Referenzarchitektur der IDSA wiederspiegeln. Dabei sollte einem Weg zur „Gegen-Abschottung“ eine Absage erteilt werden. Unternehmen sollten dazu angehalten werden, die besten verfügbaren Technologien zu nutzen, ohne hierbei durch zu strenge Regularien oder Regelwerke in ihrem industriellen Forstschritt gehindert zu werden. Soweit protektionistische Tendenzen in ausländischen Zielmärkten unmittelbare oder mittelbare Auswirkungen auf die Use Cases Remote Access, Condition Monitoring und Datenaustauschplattformen haben, ist die Unterstützung der Bundesregierung und der europäischen Kommission erforderlich, im Rahmen entsprechender Initiativen aktiv dafür zu sorgen, dass ein freier Datenverkehr und -handel mit möglichst geringen Digitalisierungsbarrieren auch in Zukunft möglich ist. Maschinen- und Anlagenbauer sollten die Themen freier Datenverkehr und Digitalisierung aktiv verfolgen und sich in die rechtliche Gestaltung einbringen, um zu gewährleisten, dass für den Maschinenbau relevante Regelungen erreicht werden können.

Mit besonderer Aufmerksamkeit sollten dabei insbesondere die Themen IT-SiG 2.0 in Deutschland, die Ausgestaltung der Cyber-Security-Zertifizierungsmodelle nach dem EU Cyber-Security-Act, die weitere konkrete Ausformung durch Rechtsverordnungen und (behördliche) Maßnahmen des Cyber-Security-Gesetz in China und des Digitalprogramms in Russland, weitere Handelssanktionen der USA und der Abschluss etwaiger Handelsabkommen („TTIP 3.0“) zwischen Europa und den USA verfolgt werden.

# Abkürzungsverzeichnis

| | |
|---|---|
| **Abs.** | Absatz |
| **APEC** | Asia-Pacific Economic Cooperation |
| **Art.** | Artikel |
| **AWG** | Außenwirtschaftsgesetz |
| **AWV** | Außenwirtschaftsverordnung |
| **BAFA** | Bundesamt für Wirtschaft und Ausfuhrkontrolle (Deutschland) |
| **B2B2C** | Business-to-Business-to-Consumer |
| **BIS** | Bureau of Industry and Security (USA) |
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik (Deutschland) |
| **bzw.** | Beziehungsweise |
| **CAC** | Cyberspace Administration of China |
| **CAD** | Computer-Aided-Design |
| **CNC** | Computerised numerical controlled |
| **CNCA** | Certification and Accreditation Administration of the People's Republic of China |
| **CSF** | Cybersecurity Framework |
| **d. h.** | Das heißt |
| **DS-GVO** | Europäische Datenschutz-Grundverordnung |
| **DPI** | Deep Packet Inspection |
| **EAR** | Export Administration Regulation (USA) |
| **EAWU** | Eurasische Wirtschaftsunion |
| **ECIPE** | European Centre for International Political Economy |
| **EDSA** | Europäischer Datenschutzausschuss |
| **EG** | Europäische Gemeinschaft |
| **ERP** | Enterprise Resource Planning |
| **EU** | Europäische Union |
| **EWR** | Europäischer Wirtschaftsraum |
| **ff.** | Folgende |
| **FIE** | Foreign Invested Enterprises |
| **FSTEK** | Föderaler Dienst für technische und Exportkontrolle (Russland) |
| **GB** | Gigabyte |
| **ggf.** | Gegebenenfalls |
| **HMI** | Human Machine Interface |
| **IaaS** | Infrastructure as a Service |
| **IDSA** | International Data Spaces Association (Deutschland) |
| **IEC** | International Electrotechnical Commission |
| **IKT** | Informations- und Kommunikations-technik |
| **IoT** | Internet of Things |
| **IP** | Intellectual Property |
| **IT** | Informationstechnologie |
| **ITIF** | Information Technology & Innovation Foundation |
| **IT-SiG 2.0** | Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme |
| **KI** | Künstliche Intelligenz |
| **KMU** | Kleine und mittlere Unternehmen |
| **LLP** | Limited Liability Partnership |
| **MPS** | Ministerium für Öffentliche Sicherheit (China) |

| | |
|---|---|
| **NAFTA** | Nordamerikanisches Freihandelsabkommen |
| **NIST** | National Institute of Standards and Technology (USA) |
| **Nr.** | Nummer |
| **NTIA** | National Telecommunications and Information Association (USA) |
| **NutzerID** | Nutzeridentifikator |
| **OECD** | Organisation for Economic Cooperation and Development |
| **PaaS** | Platform as a Service |
| **RMB** | Renminbi |
| **Rn.** | Randnummer |
| **S.** | Seite |
| **SaaS** | Software as a Service |
| **SCA** | State Cryptography Administration (China) |
| **TKG** | Telekommunikationsgesetz |
| **US/USA** | United States/United States of America |
| **USD** | US Dollar |
| **VDMA** | Verband Deutscher Maschinen- und Anlagenbau e. V. |
| **VPN** | Virtual Private Network |
| **WTO** | World Trade Organization |
| **z. B.** | Zum Beispiel |

# Abbildungsverzeichnis

Abbildung 1: Datenströme 8

Abbildung 2: Beispiele für Maschinendaten in der Automatisierungstechnik 9

Abbildung 3: Übersicht Regelungen zum Schutz Kritischer Infrastrukturen 17

Abbildung 4: Regulatorische Hemmnisse für den freien Datenfluss 18

# Quellenverzeichnis


- *Abele*, Corinne et al., Das Chinageschäft der Zukunft – Herausforderungen und Strategien für den deutschen Maschinenbau, Studie des VDMA, Oktober 2018.

- BeckOK DatenschutzR/*-Schild*, C.H.Beck München 27. Edition 2019, DS-GVO Art. 4.

- *Brand*, Thomas: Was müssen smarte Sensoren für Condition Monitoring können?, 09.04.2018, Fachzeitschrift ELEKTRONIKPRAXIS Ausgabe 7/2018 (abrufbar unter: **http://files.vogel.de/vogelonline/vogelonline/issues/ep/2018/007.pdf**, S. 26, zuletzt abgerufen am 25.07.2019).

- *Brodkin*, Joe, arstechnica, Tim Cook calls for strong US privacy law, rips "data-industrial complex", (abrufbar unter: **https://arstechnica.com/tech-policy/2018/10/tim-cook-calls-for-strong-us-privacy-law-rips-data-industrial-complex/**; zuletzt abgerufen am 25.07.2019).

- Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA), Informationsblatt, (abrufbar unter: **http://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_exportkontrolle_bafa.html**; zuletzt abgerufen am 25.07.2019).

- Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA), Übersicht über die länderbezogenen Embargos (Stand 24.01.2019, abrufbar unter **https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_embargo_uebersicht_laenderbezogene_embargos.pdf?__blob=publicationFile&v=4**; zuletzt abgerufen am 25.07.2019).

- Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA), Technologietransfer und Non-Proliferation – Leitfaden für Industrie und Wirtschaft, S. 16.

- Bundesministerium für Wirtschaft und Energie, Weissbuch – Digitale Plattformen: Digitale Ordnungspolitik für Wachstum, Innovation, Wettbewerb und Teilhabe (abrufbar unter: **https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/weissbuch-digitale-plattformen.pdf?__blob=publicationFile&v**; zuletzt abgerufen am 25.07.2019).

- Bundesverband der Deutschen Industrie, Grundsatzpapier/China, Partner und systematischer Wettbewerber – Wie gehen wir mit Chinas staatlich gelenkter Volkswirtschaft um? (6. Januar 2019) (abrufbar unter: **https://www.politico.eu/wp-content/uploads/2019/01/BDI-Grundsatzpapier_China.pdf**; zuletzt abgerufen am 25.07.2019).

- *Castor*, Daniel / McQuinn, Alan, Cross-Border Data Flows Enable Growth in All Industries, 2015, Information Technology & Innovation Foundation (ITIF), (abrufbar unter: **http://www2.itif.org/2015-cross-border-data-flows.pdf**; zuletzt abgerufen am 25.07.2019).

- CNCA (Certification and Accreditation Administration of the People's Republic of China): Netzwerkschlüsselausrüstung und Netzwerksicherheitsprodukte – Durchführungsbestimmungen zur Sicherheitszertifizierung (nur auf Chinesisch abrufbar unter: **http://www.cnca.gov.cn/xxgk/ggxx/2018/201807/t20180702_56737.shtml**; zuletzt abgerufen am 25.07.2019).

- Congressional Research Service: "Data Flows, Online Privacy, and Trade Policy", 11.03.2019 (abrufbar unter: **https://fas.org/sgp/crs/row/R45584.pdf**; zuletzt abgerufen am 25.07.2019).

- Comments of the U.S. Chamber of Commerce to the National Telecommunications and Information Administration, U.S. Department of Commerce, "International Internet Policy Priorities" (July 2018) (abrufbar unter: **https://www.ntia.doc.gov/files/ntia/publications/180717_comments_uscc_ntia_internationalinternetpolicypriorities.pdf;** zuletzt abgerufen am 25.07.2019).

- Deloitte Bericht „Industry 4.0 and Cybersecurity" (abrufbar unter: **https://www2.deloitte.com/content/dam/insights/us/articles/3749_Industry4-0_cybersecurity/DUP_Industry4-0_cybersecurity.pdf**; zuletzt abgerufen am 25.07.2019).

- Draft NISTIR 8183A Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide (abrufbar unter: **https://csrc.nist.gov/News/2019/nist-releases-draft-nistir-8183a-for-comment**, zuletzt abgerufen am 25.07.2019).

- EU Handelskammer in China, Positionspapier der Cyber-Security Arbeitsgruppe 2018/2019 (abrufbar unter: **https://static.europeanchamber.com.cn/upload/documents/documents/Cybersecurity_EN2018[625].pdf**; zuletzt abgerufen am 25.07.2019).

- EU Kommission: Pressemitteilung, "State of the Union 2017: A framework for the free flow of non-personal data in the EU" (abrufbar unter: **http://europa.eu/rapid/press-release_IP-17-3190_en.htm**; zuletzt abgerufen am 03.06.2019).

- EU Kommission: Pressemitteilung, „Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers", 10.01.2017 (abrufbar unter: **http://europa.eu/rapid/press-release_MEMO-17-15_en.htm**; zuletzt abgerufen am 25.07.2019).

- EU Kommission: Pressemitteilung, Online-Plattformen: Kommission legt neue Standards für Transparenz und Fairness fest, 26.04.2018 (abrufbar unter: **http://europa.eu/rapid/press-release_IP-18-3372_de.htm**; zuletzt abgerufen am 25.07.2019).

- EU Kommission: Mitteilung der Kommission über Aufbau einer europäischen Datenwirtschaft, SWD (2017) 2 final (abrufbar unter: **https://ec.europa.eu/transparency/regdoc/rep/1/2017/DE/COM-2017-9-F1-DE-MAIN-PART-1.PDF**; zuletzt abgerufen am 25.07.2019).

- EU Kommission: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über die Halbzeitüberprüfung der Strategie für einen digitalen Binnenmarkt, COM (2017) 228 final (abrufbar unter: **https://ec.europa.eu/transparency/regdoc/rep/1/2017/DE/COM-2017-228-F1-DE-MAIN-PART-1.PDF**; zuletzt abgerufen am 25.07.2019).

- EU Kommission: "Commission Staff Working Document – Impact Assessment", SWD(2017) 304 final (abrufbar unter: **https://eur-lex.europa.eu/resource.html?uri=cellar:51c9c47e-985c-11e7-b92d-01aa75ed71a1.0001.02/DOC_1&format=PDF** (Teil 1) und **https://eur-lex.europa.eu/resource.html?uri=cellar:51c9c47e-985c-11e7-b92d-01aa75ed71a1.0001.02/DOC_2&format=PDF** (Teil 2); beide zuletzt abgerufen am 25.07.2019).

- EU Kommission: Schwerpunkte der IKT-Normung für den digitalen Binnenmarkt, COM (2016) 176 final (abrufbar unter: **https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016DC0176&from=DE**; zuletzt abgerufen am 25.07.2019).

- EU Kommission: Mitteilung der Kommission über Strategie für einen digitalen Binnenmarkt für Europa, COM (2015) 192 final (abrufbar unter: **https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52015DC0192&from=EN**; zuletzt abgerufen am 25.07.2019).

- EU Kommission: Cross-border data flow in the Digital Single Market: data localisation restrictions (SMART 2015/0054 (abrufbar unter: **https://ec.europa.eu/digital-single-market/en/news/cross-border-data-flow-digital-single-market-data-location-restrictions**; zuletzt abgerufen am 25.07.2019).

- EU Kommission: Mitteilung der Kommission an das Europäische Parlament und den Rat, Leitlinien zur Verordnung über einen Rahmen für den Verkehr nicht-personenbezogener Daten in der Europäischen Union, COM(2019) 250 final (abrufbar unter: **https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=COM:2019:250:FIN&from=EN**; zuletzt abgerufen am 25.07.2019).

- EU Kommission:"Facilitating cross border data flow in the Digital Single Market" (abrufbar unter: **https://ec.europa.eu/newsroom/document.cfm?doc_id=41185**, zuletzt abgerufen am 25.07.2019).

- *Felbermayr*, Gabriel: "„Trump sitzt am längeren Hebel" – Künftiger IfW-Chef sieht USA im Streit mit China im Vorteil", Handelsblatt, 17.01.2019 (abrufbar unter: h**ttps://www.handelsblatt.com/politik/international/gabriel-felbermayr-im-interview-trump-sitzt-am-laengeren-hebel-kuenftiger-ifw-chef-sieht-usa-im-streit-mit-china-im-vorteil/23874994.html?ticket=ST-12527-0LjkNSdOhqGqK9cbG-6BI-ap5**; zuletzt abgerufen am 25.07.2019).

- *Felbermayr/Steiniger/Yalcin*: „Quantifying Trump: The Costs of a Protectionist US", CESifo Forum 4/2017 December Volume 18.

- *Ferracane,* Martina Francescaet al., ECIPE, Digital Trade Restrictiveness Index (abrufbar unter: **https://ecipe.org/wp-content/uploads/2018/05/DTRI_FINAL.pdf**; zuletzt abgerufen am 25.07.2019).

- *Godel,* Moritz et al., Facilitating cross border data flow in the Digital Single Market (SMART 2015/0016) (abrufbar unter: **https://ec.europa.eu/digital-single-market/en/news/cross-border-data-flow-digital-single-market-data-location-restrictions**; zuletzt abgerufen am 25.07.2019).

- Gemeinsame Vision, gemeinsames Handeln: Ein stärkeres Europa – Eine Globale Strategie für die Außen- und Sicherheitspolitik der Europäischen Union, 2016 (abrufbar unter: **https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_de_0.pdf**; zuletzt abgerufen am 25.07.2019).

- Handelsblatt Maschinenbau-Export verzeichnet deutliches Plus im US-Geschäft, 20.06.2018 (abrufbar unter: **https://www.handelsblatt.com/unternehmen/industrie/vdma-maschinenbau-export-verzeichnet-deutliches-plus-im-us-geschaeft/22714218.html?ticket=ST-939459-kCnDusdFIkfLytVO25I0-ap4**; zuletzt abgerufen am 25.07.2019).

- *Haellmigk, Philip:* (Cloud-)Datentransfer und Exportkontrolle – Neue Compliance-Herausforderungen für Unternehmen, CCZ 2016, 28-34.

- *Hoeren,* Thomas / *Sieber,* Ulrich / *Holznagel,* Bernd, Handbuch Multimedia-Recht, C.H. Beck, München, Oktober 2018.

- *Kinkel,* Steffen et al., Digital-vernetztes Denken in der Produktion, Studie im Auftrag der IMPULS-Stiftung, Hochschule Karlsruhe – Technik und Wirtschaft, ILN Institut für Lernen und Innovation in Netzwerken, Karlsruhe, November 2016.

- *Kleinhans,* Jan-Peter, Stiftung Neue Verantwortung, 5G vs. National Security (abrufbar unter: **https://www.stiftung-nv.de/sites/default/files/5 g_vs._national_security.pdf**; zuletzt abgerufen am 25.07.2019).

- *Lagarde,* Christine, "Creating a Better Global Trade System", 29. Mai 2018 (abrufbar unter: **https://blogs.imf.org/2018/05/29/creating-a-better-global-trade-system/**; zuletzt abgerufen am 25.07.2019).

- National Conference of State Legislatures, Security Breach Notification Laws (abrufbar unter: **http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx**; zuletzt abgerufen am 25.07.2019).

- National Institute of Standards and Technology, Cybersecurity Framework (abrufbar unter: **https://www.nist.gov/cyberframework/framework**; zuletzt abgerufen am 25.07.2019).

- NIST Interner Bericht (NISTIR) 8228: Considerations for Managing Internet of Things (IoT), Cybersecurity and Privacy Risks (abrufbar unter: **https://csrc.nist.gov/publications/detail/nistir/8228/draft**; zuletzt abgerufen am 25.07.2019).

- NYTimes, Their Soybeans Piling Up, Farmers Hope Trade War Ends Before Beans Rot (abrufbar unter: **https://www.nytimes.com/2018/11/05/business/soybeans-farmers-trade-war.html**; zuletzt abgerufen am 25.07.2019).

- Plattform Industrie 4.0: Forschungsprojekt IUNO: Glossar (abrufbar unter: **https://iuno-projekt.de/glossar**); Grundlagen (abrufbar unter: **https://iuno.axoom.cloud/en/landingpage/start**); Technologiedatenmarktplatz (abrufbar unter: **https://iuno-projekt.de/anwendungen/technologiedatenmarktplatz)** (alle zuletzt abgerufen am 25.07.2019).

- Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat, Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, 27.03.2019 („RefE") (abrufbar unter: **http://intrapol.org/wp-content/uploads/2019/04/IT-Sicherheitsgesetz-2.0-_-IT-SiG-2.0.pdf**; zuletzt abgerufen am 25.07.2019).

- Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (abrufbar unter: **https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L0943&from=DE**; zuletzt abgerufen am 25.07.2019).

- Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie) (abrufbar unter: **https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L1148**; zuletzt abgerufen am 25.07.2019).

- *Rose,* Sören: Industrie 4.0 lebt vom Datenaustausch – zeitnah und zielgerichtet, 14.01.2019 (abrufbar unter: **https://www.industry-of-things.de/industrie-40-lebt-vom-datenaustausch-zeitnah-und-zielgerichtet-a-789386/**, zuletzt abgerufen am 25.07.2019).

- Security Week: Top Russian Internet Firm Reportedly Under Pressure on Data (abrufbar unter: **https://www.securityweek.com/top-russian-internet-firm-reportedly-under-pressure-data**, zuletzt abgerufen am 25.07.2019).

- Symantec Whitepaper "Smarter Security for Manufacturing in the Industry 4.0 Era" (abrufbar unter: **https://www.symantec.com/content/dam/symantec/docs/solution-briefs/industry-4.0-en.pdf**; zuletzt abgerufen am 25.07.2019).

- *Thakkar,* Danny, Bayometric, Biometric Regulations in the U.S. States: The State of Play (abrufbar unter: **https://www.bayometric.com/biometric-regulations-us-states/**; zuletzt abgerufen am 03.07.2019).

- *Townsend, T.:* „Are You an Exporter? You Might Be: The Often Overlooked Controls on Software with En-cryption Capacity", The National Law Review, 02.05.2018 (abrufbar unter: **https://www.natlawreview.com/article/are-you-exporter-you-might-be-often-overlooked-controls-software-encryption-capacity**; zuletzt abgerufen am 25.07.2019).

- U.S. International Trade Commission, "Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions", Investigation Number: 332-561, August 2017 (abrufbar unter: **https://www.usitc.gov/publications/332/pub4716_0.pdf**; zuletzt abgerufen am 25.07.2019).

- *Van et al.,* Lu: National Institute of Standards and Technology, Current Standards Landscape for Smart Manufacturing Systems (abrufbar unter: **https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8107.pdf**; zuletzt abgerufen am 25.07.2019).

- VDMA-Infoblatt, Status Quo VPN & Datenaustausch in China.

- VDMA, Chinageschäft der Zukunft, 2018.

- Verordnung (EG) Nr. 428/2009 des Rates vom 5. Mai 2009 über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, Verbringung, der Vermittlung und der Durchfuhr von Gütern mit doppeltem Verwendungszweck (abrufbar unter: **https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02009R0428-20140702&from=DE**; zuletzt abgerufen am 25.07.2019).

- Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union, 2017/0228 (COD) (abrufbar unter: **https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017PC0495&from=EN**; zuletzt abgerufen am 25.07.2019).

- Weltwirtschaftsforum, The Global Risks Report 2018, 13. Edition (abrufbar unter: **http://www3.weforum.org/docs/WEF_GRR18_Report.pdf**; zuletzt abgerufen am 25.07.2019).

- *Wiechers,* Ralph: Maschinenbau macht weiter Tempo im Export, 19.11.2018 (abrufbar unter: **https://www.vdma.org/v2viewer/-/v2article/render/27115762**; zuletzt abgerufen am 25.07.2019).

# Endnoten

**1** „Today, data is the greatest asset. Both opportunities as well as the biggest challenges are being created by the global flow of data." Premierminister von Indien Narendra Modi, Weltwirtschaftsgipfel, 24.01.2019, (abrufbar unter: **https://www.narendramodi.in/pm-modi-addresses-world-economic-forum-plenary-session-davos-538623**; zuletzt abgerufen am 25.07.2019).

**2** Siehe **https://www.bbk.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html** (zuletzt abgerufen am 25.07.2019).

**3** Einzelheiten finden sich in Ziffer VII.3 „Schutz Kritischer Infrastrukturen".

**4** Einzelheiten finden sich in Ziffer VIII.3 „Schutz Kritischer Infrastrukturen".

**5** Wiechers, Ralph: Maschinenbau macht weiter Tempo im Export, 19.11.2018 (abrufbar unter: **https://www.vdma.org/v2viewer/-/v2article/render/27115762**, zuletzt abgerufen am 25.07.2019).

**6** „Maschinenbau-Export verzeichnet deutliches Plus im US-Geschäft", Handelsblatt, 20.06.2018.

**7** Rose, Sören: Industrie 4.0 lebt vom Datenaustausch – zeitnah und zielgerichtet, 14.01.2019 (abrufbar unter: **https://www.industry-of-things.de/industrie-40-lebt-vom-datenaustausch-zeitnah-und-zielgerichtet-a-789386/**, zuletzt abgerufen am 25.07.2019).

**8** Einzelheiten finden sich in Ziffer VI. „Überblick Prüffelder"

**9** Im Rahmen dieser Studie wird der Begriff Maschinendaten als Oberbegriff verstanden und nicht nach den einzelnen hierunter zu verstehenden Datenkategorien differenziert. Sofern einzelne Digitalisierungsbarrieren nur für bestimmte Datenkategorien, aber nicht Maschinendaten in ihrer Gesamtheit relevant sind, weist diese Studie hierauf an entsprechender Stelle hin.

**10** VDMA-Leitfaden Datennutzung, Orientierungshilfe zur Vertragsgestaltung für den Mittelstand, S. 13.

**11** EU Kommission: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über die Halbzeitüberprüfung der Strategie für einen digitalen Binnenmarkt, COM (2017) 228 final (abrufbar unter: **https://ec.europa.eu/transparency/regdoc/rep/1/2017/DE/COM-2017-228-F1-DE-MAIN-PART-1.PDF**; zuletzt abgerufen am 25.07.2019), S. 13.

**12** Siehe Abbildung 2.

**13** Alternativ kann auch von „Technologiedaten" gesprochen werden. So etwa im Rahmen des Forschungsprojekts IUNO. Im Forschungsvorhaben IUNO, dem Nationalen Referenzprojekt zur IT-Sicherheit in Industrie 4.0, werden Bedrohungen und Risiken für die intelligente Fabrik identifiziert, Schutzmaßnahmen entwickelt und exemplarisch in vier Anwendungsfällen umgesetzt. Das Projekt ist seit September 2018 abgeschlossen und wurde vom Bundesministerium für Bildung und Forschung gefördert (abrufbar unter: **https://iuno-projekt.de/**; zuletzt abgerufen am 25.07.2019).

**14** Siehe hierzu Forschungsprojekt IUNO Glossar zu Technologiedaten.

**15** Beispielsweise im Gesetz des US Bundesstaats Kalifornien („California Consumer Privacy Act“) in Titel 1.81.5, Ziffer 1798.140 (o) (1) in Unterkapitel 4 von Kapitel 3 des Bürgerlichen Gesetzbuchs („Civil Code“): „Personenbezogenen Informationen bezeichnet Informationen, die einen bestimmten Verbraucher oder Haushalt direkt oder indirekt identifizieren, sich auf diesen beziehen, ihn beschreiben oder mit diesem in Verbindung gebracht werden können.“

**16** Einzelheiten zu den Möglichkeiten der Pseudonymisierung personenbezogener Daten finden sich in Ziffer VII.5 „Datenschutzgrundverordnung“.

**17** Kinkel, Steffen et al., Digital-vernetztes Denken in der Produktion, Studie im Auftrag der IMPULS-Stiftung, Hochschule Karlsruhe – Technik und Wirtschaft, ILN Institut für Lernen und Innovation in Netzwerken, Karlsruhe, November 2016, S. 60: Größere Betriebe (mit 250 oder mehr Beschäftigten) setzen digitale Technologien in der eigenen Produktion deutlich häufiger als KMU ein. Dabei nimmt der Grad der Digitalisierung der Produktion mit steigender Produktkomplexität und höherer Seriengröße zu. Betriebe mit Einzel- oder Kleinserienfertigung setzen hingegen seltener digitale Technologien in der eigenen Produktion ein.

**18** Brand, Thomas: „Was müssen smarte Sensoren für Condition Monitoring können?“, 09.04.2018, Fachzeitschrift ELEKTRONIKPRAXIS Ausgabe 7/2018 (abrufbar unter: **http://files.vogel.de/vogelonline/vogelonline/issues/ep/2018/007.pdf**, S. 26, zuletzt abgerufen am 25.07.2019).

**19** Alternativ kann auch von „Datenmarktplatz“ oder „Data Space“ gesprochen werden.

**20** Siehe hierzu beispielhaft Forschungsprojekt IUNO Grundlagen.

**21** Bundesministerium für Wirtschaft und Energie, Weissbuch – Digitale Plattformen: Digitale Ordnungspolitik für Wachstum, Innovation, Wettbewerb und Teilhabe, S. 14 (abrufbar unter: **https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/weissbuch-digitale-plattformen.pdf?__blob=publicationFile&v**; zuletzt abgerufen am 25.07.2019).

**22** Förderprogramm der EU Kommission in Höhe von 300 Millionen Euro bis 2020; weitere Investitionen in Schlüsseltechnologien wie Nanoelektronik, Fotonik, Robotik, 5G-Dienste, Hochleistungsrechne, Big Data, Cloud-Computing und künstliche Intelligenz und in deren Integration entlang der Wertschöpfungskette mit Pilotfertigungsbändern und Prüfständen sind ebenfalls geplant; siehe Mitteilung der Kommission über die Halbzeitüberprüfung der Strategie für einen digitalen Binnenmarkt, S. 19.

**23** Siehe Einzelheiten zum Forschungsprojekt IUNO Technologiedatenmarktplatz.

**24** Siehe hierzu beispielhaft die Forderungen der Referenzarchitektur der International Data Spaces Association (**https://www.internationaldataspaces.org/**) (zuletzt abgerufen am 25.07.2019).

**25** Siehe hierzu beispielhaft die Forderungen der Referenzarchitektur der International Data Spaces Association (**https://www.internationaldataspaces.org/**) (zuletzt abgerufen am 25.07.2019).

**26** Siehe VDMA-Leitfaden mit Datennutzung, Orientierungshilfe zur Vertragsgestaltung für den Mittelstand, S. 14; siehe zudem die Forderungen der Referenzarchitektur der International Data Spaces Association (**https://www.internationaldataspaces.org/**) (zuletzt abgerufen am 25.07.2019).

**27** Bestimmte Prüffelder waren zum Zeitpunkt der Ausarbeitung der Studie für einzelne Zielmärkte mit Blick auf den Fokus der Studie, d. h. Digitalisierungsbarrieren, nur von geringer Relevanz und werden entsprechend nicht thematisiert, z. B. weil hierzu (noch) keine Gesetzgebung vorliegt oder diese ihren Fokus (noch) nicht auf digitale Sachverhalte legt.

**28** Siehe Art. 2 Nr. 1 Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung.

**29** Siehe Erwägungsgrund 16 des „Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union".

**30** Begründung des „Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union", S. 7.

**31** Godel, Moritz et al., Facilitating cross border data flow in the Digital Single Market (SMART 2015/0016) (abrufbar unter: **https://ec.europa.eu/digital-single-market/en/news/cross-border-data-flow-digital-single-market-data-location-restrictions**; zuletzt abgerufen am 03.07.2019), S. 7; Siehe Studie der EU Kommission: Cross-border data flow in the Digital Single Market: data localisation restrictions (SMART 2015/0054 (abrufbar unter: **https://ec.europa.eu/digital-single-market/en/news/cross-border-data-flow-digital-single-market-data-location-restrictions**; zuletzt abgerufen am 25.07.2019), S. 1.

**32** Innerhalb der EU wurden mehr als 60 Beschränkungen für 25 Mitgliedsstaaten festgestellt, siehe EU Kommission: „Commission Staff Working Document – Impact Assessment", SWD (2017) 304 final (abrufbar unter: **https://eur-lex.europa.eu/resource.html?uri=cellar:51c-9c47e-985c-11e7-b92d-01aa75ed71a1.0001.02/DOC_2&format=PDF**; zuletzt abgerufen am 25.07.2019), Annex 5, S. 37.

**33** EU Kommission: Mitteilung der Kommission an das Europäische Parlament und den Rat, Leitlinien zur Verordnung über einen Rahmen für den Verkehr nicht-personenbezogener Daten in der Europäischen Union, COM(2019) 250 final, S. 9 (abrufbar unter: **https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=COM:2019:250:FIN&from=EN**; zuletzt abgerufen am 25.07.2019).

**34** EU Kommission: Mitteilung der Kommission an das Europäische Parlament und den Rat, Leitlinien zur Verordnung über einen Rahmen für den Verkehr nicht-personenbezogener Daten in der Europäischen Union, COM(2019) 250 final, S. 8.

**35** Siehe Erwägungsgrund 12 des „Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union".

**36** Auszüge aus der Studie „Cross-border data flow in the Digital Single Market: data localisation restrictions", S. 2.

**37** Siehe Pressemitteilung der EU Kommission, "State of the Union 2017: A framework for the free flow of non-personal data in the EU" (abrufbar unter: **http://europa.eu/rapid/press-release_IP-17-3190_en.htm**; zuletzt abgerufen 25.07.2019).

**38** Beispielsweise gestattet es das französische Gesetz Nr.80.538 vom 16. Juli 1980, dass Daten, die die „Souveränität, die Sicherheit, die öffentliche Ordnung oder wesentliche wirtschaftliche Interessen Frankreichs beeinträchtigen könnten", nicht übermittelt werden dürfen. Die Daten können allerdings aus anderen Ländern abgerufen werden, wenn bestimmte Bedingungen erfüllt sind (z. B. das Bestehen internationaler Verträge oder internationaler Vereinbarungen).

**39** Zwei Studien (SMART 2015/0016 und SMART 0054/2016) identifizierten innerhalb der EU mehr als 60 Beschränkungen für 25 Mitgliedsstaaten. Beide Studien waren im Umfang nicht erschöpfend. Daher ist die Anzahl der Einschränkungen und Anforderungen als Auszug zu verstehen, der nur die „Spitze des Eisbergs" widerspiegelt, siehe EU Kommission – „Commission Staff Working Document – Impact Assessment", SWD (2017) 304 final, Annex 5, S. 37.

**40** EU Kommission:„Facilitating cross border data flow in the Digital Single Market“, S. 37 (abrufbar unter: **https://ec.europa.eu/newsroom/document.cfm?doc_id=41185**, zuletzt abgerufen am 25.07.2019).

**41** Einzelheiten finden sich in Ziffer VI.3 „Vorschriften zur Datenlokalisierung“.

**42** Einzelheiten finden sich in Ziffer VI.1 „Schutz von Geschäftsgeheimnissen“.

**43** Siehe beispielhaft die Verordnung (EG) Nr. 428/2009 des Rates vom 5. Mai 2009 über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchfuhr von Gütern mit doppeltem Verwendungszweck.

**44** Informationsblatt des Bundesamtes für Wirtschaft und Ausfuhrkontrolle (abrufbar unter: **http://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_exportkontrolle_bafa.html**; zuletzt abgerufen am 25.07.2019).

**45** Verordnung (EG) Nr. 428/2009 des Rates vom 5. Mai 2009 über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchfuhr von Gütern mit doppeltem Verwendungszweck.

**46** Einzelheiten zum Thema Einfuhr- / Ausfuhrkontrollbestimmungen finden sich in den Kapiteln der jeweiligen Zielmärkte, d. h. für die EU Ziffer VII.6 „Ausfuhrbestimmungen (Exportkontrolle)“, für China Ziffer VIII.6 „Einfuhr-/Ausfuhrkontrollbestimmungen“, für Russland IX.6 „Einfuhrkontrollbestimmungen“ und für die USA Ziffer X.5 „Ausfuhrkontrollbestimmungen (Exportkontrolle)“.

**47** Beispielsweise hat die US-Administration Anfang 2019 den Einsatz von ausländischen Telekommunikationskomponenten in föderalen Netzen untersagt.

**48** Beispielsweise sind seit Jahren Sanktionen gegen den Iran in Kraft, die den Handel zwischen dem Iran und Unternehmen beeinträchtigen.

**49** EU Kommission: Schwerpunkte der IKT-Normung für den digitalen Binnenmarkt, COM (2016) 176 final (abrufbar unter: **https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016DC0176&from=DE**; zuletzt abgerufen am 25.07.2019), S. 1.

**50** EU Kommssion: Mitteilung der Kommission über Strategie für einen digitalen Binnenmarkt für Europa, COM (2015) 192 final (abrufbar unter: **https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52015DC0192&from=EN**; zuletzt abgerufen am 25.07.2019);
EU Kommission: Mitteilung der Kommission über Aufbau einer europäischen Datenwirtschaft, SWD (2017) 2 final (abrufbar unter: **https://ec.europa.eu/transparency/regdoc/rep/1/2017/DE/COM-2017-9-F1-DE-MAIN-PART-1.PDF**; zuletzt abgerufen am 25.07.2019).

**51** EU Kommission: Mitteilung der Kommission an das Europäische Parlament und den Rat, Leitlinien zur Verordnung über einen Rahmen für den Verkehr nicht-personenbezogener Daten in der Europäischen Union, COM(2019) 250 final, S. 2.

**52** EU Kommission: Mitteilung der Kommission an das Europäische Parlament und den Rat, Leitlinien zur Verordnung über einen Rahmen für den Verkehr nicht-personenbezogener Daten in der Europäischen Union, COM(2019) 250 final, S. 2.

**53** Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung.

**54** In Deutschland wurde das Umsetzungsgesetz („Geschäftsgeheimnisgesetz“) am 21.03.2019 vom Bundestag verabschiedet.

**55** Art. 2 Nr. 1 Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung: „Informationen, die alle nachstehenden Kriterien erfüllen: a) Sie sind in dem Sinne geheim, dass sie weder in ihrer Gesamtheit noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne weiteres zugänglich sind; b) sie sind von kommerziellem Wert, weil sie geheim sind; c) sie sind Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen durch die Person, die die rechtmäßige Kontrolle über die Informationen besitzt."

**56** § 2 Abs. 10 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BISG).

**57** Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie) (abrufbar unter: **https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L1148**; zuletzt abgerufen am 25.07.2019).

**58** Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat, Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, 27.03.2019 **(„RefE")** (abrufbar unter: **http://intrapol.org/wp-content/uploads/2019/04/IT-Sicherheitsgesetz-2.0-_-IT-SiG-2.0.pdf**; zuletzt abgerufen am 25.07.2019).

**59** Art. 1 Nr. 1 lit. d RefE.

**60** Art. 1 Nr. 1 lit. e, Abs. 14 RefE, einschließlich der dortigen Bezugnahme auf § 48 Börsenordnung der Frankfurter Wertpapierbörse.

**61** Art. 1 Nr. 16, § 8 g RefE.

**62** Begründung des „Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union", S. 2 (2017/0228 (COD)).

**63** Einzelheiten zu den relevanten Datenkategorien finden sich in Ziffer VI.3 „Vorschriften zur Datenlokalisierung".

**64** Pressemitteilung der EU Kommission, Online-Plattformen: Kommission legt neue Standards für Transparenz und Fairness fest, 26.04.2018 (abrufbar unter: **http://europa.eu/rapid/press-release_IP-18-3372_de.htm**; zuletzt abgerufen am 25.07.2019).

**65** Pressemitteilung der EU Kommission, Online-Plattformen: Kommission legt neue Standards für Transparenz und Fairness fest, 26.04.2018.

**66** Die Art.-29-Datenschutzgruppe war ein unabhängiges Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes unter der europäischen Datenschutzrichtlinie (95/46/EG). Mit dem Inkrafttreten der DS-GVO wurde die Art.-29-Datenschutzgruppe durch den Europäischen Datenschutzausschuss (EDSA) abgelöst. Der EDSA hat in seiner ersten Plenarsitzung die bisherigen Stellungnahmen und Hilfestellungen der Art.-29-Datenschutzgruppe zur DS-GVO bestätigt; damit haben diese auch weiterhin Gültigkeit.

**67** Art.-29-Datenschutzgruppe, Working Paper 216, „Anonymisation Techniques“, S. 11. Diese Stellungnahme wurde vom EDSA nicht bestätigt, da sie nicht zur DS-GVO ergangen ist, kann aber als Indiz und Hilfestellung weiterhin herangezogen werden, solange der EDSA keine neuere Stellungnahme erlässt.

**68** Art.-29-Datenschutzgruppe, Working Paper 216, S. 11.

**69** Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden (Art. 4 Nr. 5 DS-GVO).

**70** BeckOK DatenschutzR/-Schild, DS-GVO Art. 4 Rn. 69.

**71** BeckOK DatenschutzR/-Schild, DS-GVO Art. 4 Rn. 72.

**72** Vgl. Erwägungsgrund 29 zur DS-GVO.

**73** Wie in Artikel 4 Nr. 7 DS-GVO definiert, d. h. die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

**74** Übersicht über die länderbezogenen Embargos (Stand 24.01.2019, abrufbar unter **https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_embargo_uebersicht_laenderbezogene_embargos.pdf?__blob=publicationFile&v=4**; zuletzt abgerufen am 03.07.2019).

**75** Haellmigk, Philip: (Cloud-)Datentransfer und Exportkontrolle – Neue Compliance-Herausforderungen für Unternehmen, CCZ 2016, 30.

**76** Art. 4 und 8 EG-Dual-Use-Verordnung.

**77** Beispielsweise gilt in Deutschland zusätzlich die nationale Ausfuhrliste Anlage 1 zur AWV.

**78** Art. 4 Abs. 1 EG-Dual-Use-Verordnung und § 4 AWG.

**79** Vgl. Anhang I zur EG-Dual-Use-Verordnung, dort in den Buchstaben D und E des jeweiligen Dual-Use-Guts.

**80** Hoeren/Sieber/Holznagel/-Kuner/Hladjk, Multimedia-Recht-HdB, Teil 17 Rn. 46.

**81** Artikel 2 Nr. 2 iii) der Dual-Use-Verordnung.

**82** Sog. Kriterium der Zweckgerichtetheit, siehe BAFA – Technologietransfer und Non-Proliferation – Leitfaden für Industrie und Wirtschaft, S. 15.

**83** Art. 2 Nr. 2 EG-Dual-Use-Verordnung.

**84** BAFA – Technologietransfer und Non-Proliferation – Leitfaden für Industrie und Wirtschaft, S. 18.

**85** Art. 2 Nr. 2 iii) Alt. 2 EG-Dual-Use-Verordnung.

**86** Siehe hierzu §§ 49 ff. AWV sowie BAFA – Technologietransfer und Non-Proliferation – Leitfaden für Industrie und Wirtschaft, S. 18.

**87** BAFA – Technologietransfer und Non-Proliferation – Leitfaden für Industrie und Wirtschaft, S. 16.

**88** So ausdrücklich: BAFA – Technologietransfer und Non-Proliferation – Leitfaden für Industrie und Wirtschaft, S. 19.

**89** Vgl. ähnlich gelagertes Beispiel für Software zur Auslegung und Optimierung eines Triebwerkes in: BAFA – Technologietransfer und Non-Proliferation – Leitfaden für Industrie und Wirtschaft, S. 19.

**90** Weiterführende Informationen in: Merkblatt „Exportkontrolle und das BAFA – Grundlagen der Exportkontrolle, Antragstellung, Informationsquellen und Ansprechpartner", 5. Auflage 2018, S. 12 ff.

**91** Übersicht über die länderbezogenen Embargos (Stand 24.01.2019, abrufbar unter **https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_embargo_uebersicht_laenderbezogene_embargos.pdf?__blob=publicationFile&v=4**; zuletzt abgerufen am 25.07.2019).

**92** Beispielsweise eine Anpassung der Sicherheitsanforderungen des § 109 TKG.

**93** Abele, Corinne et al., Das Chinageschäft der Zukunft – Herausforderungen und Strategien für den deutschen Maschinenbau, Studie des VDMA, Oktober 2018, S. 81.

**94** Leitende Stellungnahme des Staatsrates zur Vertiefung der Entwicklung des industriellen Internets „Internet+Advanced Manufacturing Industry", veröffentlicht vom Staatsrat am 27. November 2017.

**95** Chinageschäft der Zukunft, Studie des VDMA, S. 81.

**96** Chinageschäft der Zukunft, Studie des VDMA, S. 27.

**97** Chinageschäft der Zukunft, Studie des VDMA, S. 40.

**98** Chinageschäft der Zukunft, Studie des VDMA, S. 42.

**99** Chinageschäft der Zukunft, Studie des VDMA, S. 7.

**100** Einzelheiten zum Risiko des Abflusses von Know-how finden sich in Ziffer VIII.2 „Schutz von Geschäftsgeheimnissen"; siehe auch Chinageschäft der Zukunft, Studie des VDMA, S. 70.

**101** Einzelheiten finden sich in Ziffer V.1 „Einführung".

**102** Chinageschäft der Zukunft, Studie des VDMA, S. 41.

**103** Chinageschäft der Zukunft, Studie des VDMA, S. 41.

**104** Siehe **http://german.china.org.cn/txt/2018-01/28/content_50332602.htm** (zuletzt abgerufen am 25.07.2019).

**105** Chinageschäft der Zukunft, Studie des VDMA, S. 84.

**106** Chinageschäft der Zukunft, Studie des VDMA, S. 84.

**107** BDI, Grundsatzpapier/China, Partner und systematischer Wettbewerber – Wie gehen wir mit Chinas staatlich gelenkter Volkswirtschaft um?, Januar 2019 (abrufbar unter: **https://www.politico.eu/wp-content/uploads/2019/01/BDI-Grundsatzpapier_China.pdf**; zuletzt abgerufen am 25.07.2019), S. 8.

**108** Siehe vertiefend Kleinhans, Jan-Peter, Stiftung Neue Verantwortung, 5G vs. National Security (aufrufbar unter: **https://www.stiftung-nv.de/sites/default/files/5 g_vs._national_security.pdf**; zuletzt abgerufen am 25.07.2019).

**109** Chinageschäft der Zukunft, Studie des VDMA, S. 84.

**110** Chinageschäft der Zukunft, Studie des VDMA, S. 50.

**111** Untersucht wurden insgesamt 64 Staaten zu unterschiedlichen Aspekten von Handelsbarrieren. Siehe Ferracane, Martina Francesca et al., ECIPE, "DTRI Trade Restrictiveness Index", April 2018, S. 52 (abrufbar unter: **https://ecipe.org/wp-content/uploads/2018/05/DTRI_FINAL.pdf**; zuletzt abgerufen am 25.07.2019).

**112** Art. 30 Cyber-Security-Gesetz.

**113** 5G vs. National Security, S. 7.

**114** Chinageschäft der Zukunft, Studie des VDMA, S. 38.

**115** Einzelheiten finden sich auch im VDMA-Infoblatt, Status Quo VPN & Datenaustausch in China, S. 7.

**116** Einzelheiten finden sich auch im VDMA-Infoblatt, Status Quo VPN & Datenaustausch in China, S. 7.

**117** Art. 31 Cyber-Security-Gesetz.

**118** Art. 76 Abs. 3 Cyber-Security-Gesetz.

**119** Art. 76 Abs. 1 Cyber-Security-Gesetz.

**120** Maßnahmenentwürfe zur Sicherheitsbewertung beim Export personenbezogener Daten und wichtiger Daten („Maßnahmenentwürfe").

**121** Positionspapier der Cyber-Security Arbeitsgruppe der EU Handelskammer in China, 2018/2019, S. 3 (abrufbar unter: **https://static.europeanchamber.com.cn/upload/documents/documents/Cybersecurity_EN2018[625].pdf**; zuletzt abgerufen am 25.07.2019).

**122** Art. 37 Cyber-Security-Gesetz.

**123** „Critical Information Infrastructure Verification Guide (Trial)" von der CAC veröffentlicht.

**124** Beispielsweise ab der Übertragung eines Datenvolumens von 1.000 GB.

**125** Einzelheiten finden sich in Ziffer IX.4 „Vorschriften zur Datenlokalisierung".

**126** „National Information Security Standardisation Technical Committee" (TC260).

**127** Siehe Appendix A und Appendix B der Spezifikationen, GB/T 35273-2017.

**128** „Cybersecurity Protection Bureau of the Ministry of Public Security" (MPS).

**129** „Third Research Institute".

**130** Entwurf des neuen Positionspapiers der EU Handelskammer in China zu Cyber-Security, S. 2.

**131** Art. 16 Maßnahmenentwürfe.

**132** Art. 38 Maßnahmenentwürfe.

**133** Ein Beispiel für der Einfuhrkontrolle unterliegende Produkte sind abhörsichere Telefone.

**134** „Critical Network Equipment“ und „Specialised Network Security Products“.

**135** CNCA (Certification and Accreditation Administration of the People’s Republic of China): Netzwerkschlüsselausrüstung und Netzwerksicherheitsprodukte – Durchführungsbestimmungen zur Sicherheitszertifizierung (nur auf Chinesisch abrufbar unter: **http://www.cnca.gov.cn/xxgk/ggxx/2018/201807/t20180702_56737.shtml**; zuletzt abgerufen am 25.07.2019).

**136** Regierungserlass Nr. 1632-r vom 28. Juli 2017 zur Genehmigung des Programms für die Digitalwirtschaft der Russischen Föderation.

**137** Regierungserlass Nr. 1632-r vom 28. Juli 2017 zur Genehmigung des Programms für die Digitalwirtschaft der Russischen Föderation.

**138** Siehe **http://council.gov.ru/activity/activities/parliamentary/92113/** (zuletzt abgerufen am 25.07.2019).

**139** Siehe **https://data-economy.ru/organization** (zuletzt abgerufen am 25.07.2019).

**140** Verordnung des Föderalen Dienstes für technische und Exportkontrolle (FSTEK) über die Genehmigung der Anforderungen an die Gewährleistung der Sicherheit wichtiger Objekte Kritischer Infrastrukturen der Russischen Föderation Nr. 239 vom 25 Dezember 2017 („Verordnung des FSTEK”); Einzelheiten finden sich in Ziffer IX.3 „Schutz Kritischer Infrastrukturen“.

**141** Verordnung des FSTEK.

**142** Verordnung des FSTEK.

**143** Einzelheiten zum Begriff finden sich in Ziffer III „Vorgehensweise“.

**144** Siehe Ferracane, Martina Francesca et al., ECIPE, “DTRI Trade Restrictiveness Index”, April 2018, S. 52.

**145** Föderales Gesetz zu personenbezogenen Daten Nr. 152-FZ vom 27. Juli 2006.

**146** Siehe unverbindlicher Kommentar des Ministeriums der Russischen Föderation für Digitale Entwicklung, Telekommunikation und Massenmedien (nur auf Russisch erhältlich (abrufbar unter: **http://minsvyaz.ru/ru/personaldata/**; zuletzt abgerufen am 25.07.2019)).

**147** Föderales Gesetz zu personenbezogenen Daten Nr. 152-FZ vom 27 Juli 2006.

**148** Einzelheiten finden sich in Ziffer IX.3 „Schutz Kritischer Infrastrukturen“.

**149** Rendezvous-System bezeichnet dabei eine Variante der synchronen Interprozesskommunikation. Ein Rendezvous ist ein Kontaktpunkt zwischen zwei nebenläufigen Prozessen zur Übergabe von Daten, wobei der sendende Prozess an einer bestimmten Stelle seines Programms wartet, bis der empfangende Prozess die Daten abgeholt hat. Umgekehrt wartet der Empfänger, wenn er die Daten benötigt, so lange, bis der Sender die Daten bereitstellt.

**150** Federal Law No 5485 dated 21 July 1993 On State Secrecy.

**151** Beispielsweise kommerzielle Kosten für die Anmietung von Datenspeicherplatz oder Serverkapazität.

**152** Beispielsweise hat die russische Datenaufsichtsbehörde das Recht, vor Gericht ein Verfahren einzuleiten, um die Nichteinhaltung des russischen Datenschutzgesetzes geltend zu machen. Die russische Datenschutzaufsichtsbehörde kann in diesem Zuge auch den Internetzugang sperren, über den die personenbezogene Daten unter Verletzung des russischen Datenschutzgesetzes verarbeitet werden (Artikel 15.5 Föderales Gesetz Nr. 149-FZ vom 27. Juli 2006 über Information, Informationstechnologien und Informationsschutz).

**153** Bundesgesetz über die Telekommunikation vom 7. Juli 2003 Nr. 126-FZ und Regierungsverordnung über die Genehmigung von Bestimmungen zur Speicherung von Textnachrichten, Sprachdaten, Bildern, Tönen, Videos und weiteren Nachrichten der Nutzer von Telekommunikationsdiensten Nr. 445 vom 12. April 2018 durch die Telekommunikationsanbieter.

**154** Art. 12 Abs. 1 Föderales Gesetz Nr. 149-FZ vom 27. Juli 2006 über Information, Informationstechnologien und Informationsschutz.

**155** Föderales Gesetz Nr. 44-FZ zum Beschaffungssystem für den Einkauf von Waren, Arbeiten und Dienstleistungen für den staatlichen und kommunalen Bedarf vom 5. April 2013.

**156** Regierungserlass Nr. 1236 vom 16 November 2015 über das Verbot des Zugangs von Software aus dem Ausland zum Zwecke der Beschaffung für staatliche und kommunale Zwecke.

**157** Da dieser Abschnitt nur eine geringe Anzahl von Unternehmen des Maschinen- und Anlagenbaus betrifft, hat Bird & Bird LLP von einer Aufzählung der umfassenden Voraussetzungen für die Aufnahme in das eurasische Sonderregister abgesehen.

**158** Siehe am Beispiel des Messengerdienstes Telegram", der nach Verweigerung der Offenlegung abgeschaltet wurde (abzurufen unter: **https://www.securityweek.com/top-russian-internet-firm-reportedly-under-pressure-data**; zuletzt abgerufen am 25.07.2019).

**159** Der Gesetzesentwurf wurde Mitte April 2019 im russischen Parlament mit großer Mehrheit (307 Ja-Stimmen, 68 Nein-Stimmen) beschlossen und anschließend im Bundesrat verabschiedet. In Kraft tritt das Gesetz voraussichtlich am 1. November 2019.

**160** DPI steht für ein Verfahren in der Netzwerktechnik, mit dem Datenpakete überwacht und gefiltert werden. Dabei werden die Datenpakete auf bestimmte Merkmale wie Protokollverletzungen, Computerviren, Spam und weitere unerwünschte Inhalte untersucht. DPI ermöglicht auch eine Regulierung von Datenströmen.

**161** Beispielsweise wird DPI in chinesischen Firewalls eingesetzt.

**162** RBC, Roskomnadsors Vorschlag zum Testen der Souveränität von RuNet (nur auf Russisch erhältlich, abrufbar unter: **https://www.rbc.ru/technology_and_media/28/03/2019/5c9cdfa09a79473d7d241980?from=from_main**; zuletzt abgerufen am 25.07.2019).

**163** Chinageschäft der Zukunft, Studie des VDMA, S. 22.

**164** Chinageschäft der Zukunft, Studie des VDMA, S. 22.

**165** Chinageschäft der Zukunft, Studie des VDMA, S. 22.

**166** Bericht des Congressional Research Service: Data Flows, Online Privacy, and Trade Policy, S. 19 (abrufbar unter: **https://fas.org/sgp/crs/row/R45584.pdf**; zuletzt abgerufen am 25.07.2019).

**167** "Bipartisan Congressional Trade Priorities and Accountability Act" von 2015.

**168** Das Wirtschaftsspionage-Gesetz von 1996 („Economic Espionage Act 1996", 18 U.S.C. § 1831) kriminalisiert Wirtschaftsspionage und Diebstahl von Geschäftsgeheimnissen. Das Gesetz bestraft diejenigen, die sich wissentlich Geschäftsgeheimnisse unberechtigt aneignen oder dies versuchen bzw. sich verabreden, sich Geschäftsgeheimnisse mit der Absicht oder dem Wissen unberechtigt anzueignen, dass ein solcher Diebstahl einem ausländischen Regierungsvertreter zugutekommen wird.

**169** In Hinblick auf § 1637 ist Cyberspace definiert als „das unabhängige Netzwerk von informationstechnischen Infrastrukturen" und umfasst „das Internet, Telekommunikationsnetze, Computersysteme sowie eingebettete Prozessoren und Steuerungen". U.S. Congress, Carl Levin and Howard P. „Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, 113th Cong., Public Law 113-291 (Washington, D.C., December 19, 2014).

**170** Division 5 CLOUD Act (abrufbar unter: **https://www.govtrack.us/congress/bills/115/hr1625/text**; zuletzt abgerufen am 25.07.2019).

**171** Nach dem „Defend Trade Secrets Act 2016".

**172** U.S. International Trade Commission, "Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions", Investigation Number: 332-561, August 2017 (abrufbar unter: **https://www.usitc.gov/publications/332/pub4716_0.pdf**, S. 40, zuletzt abgerufen am 25.07.2019).

**173** Bericht des Congressional Research Service: Data Flows, Online Privacy, and Trade Policy, S. 14.

**174** Bericht des Congressional Research Service: Data Flows, Online Privacy, and Trade Policy, S. 1.

**175** Kommentare der US Handelskammer an die „National Telecommunications and Information Administration, U.S. Department of Commerce", „International Internet Policy Priorities" (Juli 2018) (abrufbar unter: **https://www.ntia.doc.gov/files/ntia/publications/180717_comments_uscc_ntia_internationalinternetpolicypriorities.pdf; zuletzt abgerufen am** 25.07.2019**)**.

**176** Bericht des Congressional Research Service: Data Flows, Online Privacy, and Trade Policy, S. 19.

**177** Siehe etwa gemeinsamer Brief von Leitern des Handelsausschusses des Senats (abrufbar unter: **https://www.moran.senate.gov/public/index.cfm/2018/9/commerce-subcommittee-leaders-to-secretary-ross-online-privacy-protections-require-congressional-action**; zuletzt abgerufen am 25.07.2019).

**178** Apple und andere Unternehmen fordern ein umfassendes Datenschutzgesetz auf Bundesebene, um dem entstehenden Flickenteppich der Landesgesetze zuvorzukommen („Tim Cook calls for strong US privacy law, rips 'data-industrial complex'", (abrufbar unter: **https://arstechnica.com/tech-policy/2018/10/tim-cook-calls-for-strong-us-privacy-law-rips-data-industrial-complex/; zuletzt abgerufen am** 25.07.2019).

**179** Siehe „Security Breach Notification Laws" (abrufbar unter: **http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx**; zuletzt abgerufen am 03.07.2019).

**180** Bericht des Congressional Research Service: Data Flows, Online Privacy, and Trade Policy, S. 16.

**181** Texas, Illinois und der Bundesstaat Washington haben Datenschutzgesetze mit Schwerpunkt biometrische Daten erlassen. Mehrere andere Staaten erwägen, solche Gesetze zu erlassen (siehe „U.S. States Enact BIPA: Legal Framework for Biometric Information Privacy", abrufbar unter: **https://www.bayometric.com/biometric-regulations-us-states/**; zuletzt abgerufen am 25.07.2019).

**182** California Consumer Privacy Act (abrufbar unter: **https://www.oag.ca.gov/privacy/ccpa**; zuletzt abgerufen am 25.07.2019); Mehrere andere Staaten (darunter Hawaii, Maryland, Massachusetts, New Mexico, Rhode Island, Illinois, New Jersey, New York, Oregon, Virginia und Washington) haben zuletzt ähnliche Gesetzgebungsvorschläge eingebracht, die die Rechte von Verbrauchern mit Blick auf den Schutz personenbezogener Daten stärken.

**183** Ende 2018 haben die Senatoren von Oregon und Hawaii auf Bundesebene Gesetzesentwürfe für Datenschutzgesetze eingebracht. Auch diese Entwürfe betreffen unmittelbar nur die Verarbeitung personenbezogener Daten, allerdings in einem solchen Ausmaß mit Blick auf Mitarbeiter, Lieferanten, Handelspartner und Kunden, dass sich hieraus im Gegensatz zu den gegenwärtigen gesetzlichen Regelungen ein zumindest mittelbares Hemmnis für Maschinen- und Anlagenbauer (etwa im Bereich der Mensch-Maschine-Kommunikation) ergeben könnte. Für Einzelheiten siehe für Oregon: Gesetzesentwurf des Senators Wyden (abrufbar unter: **https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20one%20pager%20Nov%201.pdf) und für Hawaii:** Gesetzesentwurf des Senators Schatz (abrufbar unter: **https://www.congress.gov/115/bills/s3744/BILLS-115s3744is.pdf**) (beide zuletzt abgerufen am 25.07.2019).

**184** Mass. Ann. Laws ch. 93H, § 2 (LexisNexis, Lexis Advance through Act 321 of the 2018 Legislative Session); 2018 Colo. HB. 1128.

**185** Im Jahr 2018 haben mindestens 22 Staaten Gesetze zur Cyber Security verabschiedet; siehe „Cybersecurity Legislation 2018" (abrufbar unter: **http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx**; zuletzt abgerufen am 25.07.2019

**186** 201 CMR 17.03 (abrufbar unter: **https://www.mass.gov/regulations/201-CMR-1700-standards-for-the-protection-of-personal-information-of-ma-residents#17-03-duty-to-protect-and-standards-for-protecting-personal-information-**; zuletzt abgerufen am 25.07.2019).

**187** 2018 Cal ALS 860, 2018 Cal AB 1906, 2018 Cal Stats. (abrufbar unter: **http://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=201720180AB1906**; zuletzt abgerufen am 25.07.2019).

**188** NIST Cybersecurity Framework (abrufbar unter: **https://www.nist.gov/cyberframework/framework**; zuletzt abgerufen am 25.07.2019).

**189** Einzelheiten finden sich unter **https://www.nist.gov/cyberframework** (zuletzt abgerufen am 25.07.2019).

**190** Die USA haben Apple daraufhin verklagt, die US-Regierung bei der Entschlüsselung des Telefons eines Verbrauchers zu unterstützen. Siehe „Apple v. the FBI: A complete timeline of the war over tech encryption" (abrufbar unter: **https://www.digitaltrends.com/mobile/apple-encryption-court-order-news/**; zuletzt abgerufen am 25.07.2019).

**191** Current Standards Landscape for Smart Manufacturing Systems (abrufbar unter: **https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8107.pdf**; zuletzt abgerufen am 25.07.2019); Towards a Platform for Smart Manufacturing Improvement Planning (abrufbar unter: **https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=925915**; zuletzt abgerufen am 25.07.2019).

**192** NIST Interner Bericht (NISTIR) 8228: Considerations for Managing Internet of Things (IoT), Cybersecurity and Privacy Risks (abrufbar unter: **https://csrc.nist.gov/publications/detail/nistir/8228/draft**; zuletzt abgerufen am 25.07.2019).

**193** Siehe Dokument zur Referenzarchitektur des Industrial Internet Consortium (abrufbar unter: **https://www.iiconsortium.org/IIRA.htm**; zuletzt abgerufen am 25.07.2019).

**194** Symantec Whitepaper „Smarter Security for Manufacturing in the Industry 4.0 Era" (abrufbar unter: **https://www.symantec.com/content/dam/symantec/docs/solution-briefs/industry-4.0-en.pdf**; zuletzt abgerufen am 25.07.2019); Deloitte Bericht „Industry 4.0 and Cybersecurity" (abrufbar unter: **https://www2.deloitte.com/content/dam/insights/us/articles/3749_Industry4-0_cybersecurity/DUP_Industry4-0_cybersecurity.pdf**; zuletzt abgerufen am 25.07.2019

**195** Draft NISTIR 8183A Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide (abrufbar unter: **https://csrc.nist.gov/News/2019/nist-releases-draft-nistir-8183a-for-comment**, zuletzt abgerufen am 25.07.2019).

**196** Das „Department of the Treasury's Office of Foreign Asset Control" verfügt über ein Sanktionsprogramm, das Wirtschafts- und Handelssanktionen auf der Grundlage der US-Außenpolitik gegen bestimmte Länder und Personen verwaltet und durchsetzt, z. B. bestimmte Regime und Länder, Terroristen, Personen, die an Aktivitäten im Zusammenhang mit der Verbreitung von Massenvernichtungswaffen beteiligt oder ähnlichen Mitteln beteiligt sind (abrufbar unter:: **https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx**; zuletzt abgerufen am 25.07.2019); beispielsweise Exportkontrollvorschriften, die den Export bestimmter Informationen oder Technologien verbieten oder Einzelpersonen oder nicht-amerikanische Länder einschränken, in die die Unternehmen exportieren dürfen (BIS, Lists of Parties of Concern; abrufbar unter: **https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern**; zuletzt abgerufen am 25.07.2019).

**197** Siehe **https://2016.export.gov/ecr/index.asp** (zuletzt abgerufen am 25.07.2019).

**198** BIS, Encryption and Export Administration Regulations (EAR) (abrufbar unter **https://protect-eu.mimecast.com/s/jnZ2CyPW1IjrVZgtMbSu7** zuletzt abgerufen am 25.07.2019).

**199** T. Townsend „Are You an Exporter? You Might Be: The Often Overlooked Controls on Software with Encryption Capacity", The National Law Review, 02.05.2018 (abrufbar unter: **https://www.natlawreview.com/article/are-you-exporter-you-might-be-often-overlooked-controls-software-encryption-capacity**; zuletzt abgerufen am 25.07.2019)

**200** Beispielsweise dem nordamerikanische Freihandelsabkommen (NAFTA) und dem Austritt aus der Transpazifischen Partnerschaft (siehe The Global Risks Report 2018, Weltwirtschaftsforum, 13. Edition, S. 29.).

**201** Zudem verhängten die USA im ersten Halbjahr 2017 26 % mehr Handelssanktionen gegen G20 Partner als im Vorjahr (The Global Risks Report 2018, Weltwirtschaftsforum, 13. Edition, S. 29). Einen großen Teil hiervon machen die gegen China verhängten Schutzzölle auf Importe aus China aus. Die chinesische Regierung führte als Reaktion auf die Zölle selbst Zölle auf amerikanische Produkte ein (siehe **https://www.nytimes.com/2018/11/05/business/soybeans-farmers-trade-war.html;** zuletzt abgerufen am 25.07.2019).

**202** Siehe Felbermayr/Steiniger/Yalcin: „Quantifying Trump: The Costs of a Protectionist US", CESifo Forum 4/2017 December Volume 18.

**203** Gabriel Felbermayr, „„Trump sitzt am längeren Hebel" – Künftiger IfW-Chef sieht USA im Streit mit China im Vorteil", Handelsblatt, 17.01.2019 (abrufbar unter: **https://www.handelsblatt.com/politik/international/gabriel-felbermayr-im-interview-trump-sitzt-am-laengeren-hebel-kuenftiger-ifw-chef-sieht-usa-im-streit-mit-china-im-vorteil/23874994.html?ticket=ST-12527-0LjkNSdOhqGqK9cbG6BI-ap5**; zuletzt abgerufen am 25.07.2019).

**204** Mehr als 90 Unternehmen und Institutionen unterschiedlicher Branchen und Größen aus 18 Ländern, darunter mehrere Fortune-500-Unternehmen, global agierende mittelständische Unternehmen und Software- und Systemhäuser, sind Mitglieder des Verbandes.

**205** Siehe **https://www.internationaldataspaces.org/our-approach/#about-us** (zuletzt abgerufen am 25.07.2019).

**206** „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen" gemäß Art. 25 DS-GVO.

**207** Siehe hierzu beispielhaft die Forderungen der Referenzarchitektur der International Data Spaces Association (https://www.internationaldataspaces.org/) (beide zuletzt abgerufen am 03.06.2019)

**208** Einzelheiten wie sich Unternehmen einbringen können finden sich unter **http://aebrus.ru/ (zuletzt abgerufen am** 25.07.2019**)**.

**209** Siehe **https://data-economy.ru/organization (zuletzt abgerufen am** 25.07.2019**)**.

**210** Siehe **http://ombudsmanbiz.ru/#1 (zuletzt abgerufen am** 25.07.2019**)**.

**211** Einzelheiten hierzu finden sich unter Ziffer VIII.4 „Datenschutzrecht und Schutz wichtiger nicht-personenbezogener Daten".

**212** Information Technology & Innovation Foundation (ITIF), Daniel Castor, Alan McQuinn, 2015, "Cross-Border Data Flows Enable Growth in All Industries", S. 12.

**213** Ferracane, Martina Francesca et al., ECIPE Digital Trade Restrictiveness Index.

**214** Christine Lagarde, "Creating a Better Global Trade System", 29. Mai 2018 (abrufbar unter: **https://blogs.imf.org/2018/05/29/creating-a-better-global-trade-system/**; zuletzt abgerufen am 25.07.2019).

**215** Gemeinsame Vision, gemeinsames Handeln: Ein stärkeres Europa – Eine Globale Strategie für die Außen- und Sicherheitspolitik der Europäischen Union, 2016, S. 35 (abrufbar unter: **https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_de_0.pdf**; zuletzt abgerufen am 25.07.2019).

**216** Mitteilung der Kommission über die Halbzeitüberprüfung der Strategie für einen digitalen Binnenmarkt, S. 29.

**217** Pressemitteilung der EU Kommission, „Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers", 10.01.2017.

**218** Pressemitteilung der EU Kommission, „Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers", 10.01.2017.

**219** Pressemitteilung der EU Kommission, „Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers", 10.01.2017.

**220** Pressemitteilung der EU Kommission, 23.01.2019 (abrufbar unter: **http://europa.eu/rapid/press-release_IP-19-421_en.htm**; zuletzt abgerufen am 25.07.2019).

IMPULS-
STIFTUNG

Dr. Johannes Gernandt
Geschäftsführender Vorstand

Stefan Röger
Geschäftsführender Vorstand

IMPULS-Stiftung
für den Maschinenbau,
den Anlagenbau und
die Informationstechnik

Lyoner Straße 18
60528 Frankfurt

Telefon +49 69 6603 1462
Fax +49 69 6603 2462
Internet www.impuls-stiftung.de
E-Mail info@impuls-stiftung.de