Whitepaper „Maschinendaten“ – Stand Februar 2021

Rechtsrahmen, Fallstricke und Lösungsansätze

Stefan Sander, LL.M., B.Sc., Rechtsanwalt und Fachanwalt für IT-Recht, Software-Systemingenieur

„*Die Corona-Krise beschleunigt die Digitalisierung*“, darüber besteht auf breiter Front Konsens. Berichtet wird dies nicht nur aus der Industrie, die sich schon seit Längerem mit Themen wie dem Internet-of-Things (IoT), der Industrie 4.0 oder Predictive Maintenance befasst. In einer repräsentativen Umfrage im Auftrag des BITKOM vom Oktober 2020 bestätigt diese Aussage auch die öffentliche Verwaltung. Wenig überraschend, dass auch der deutsche Mittelstand zunehmend digitaler wird, in allen Bereichen der Wertschöpfung, wie auch alle Branchen und Firmengrößen. Zu diesem Ergebnis kommt die fünfte Ausgabe der im Auftrag der Telekom durchgeführten repräsentativen Studie Digitalisierungsindex Mittelstand 2020/2021.

Die digitale Unterstützung bestehender Prozesse oder der Austausch eines analogen Ablaufs durch eine digitale Alternative ist das Eine – etwas Anderes ist es jedoch, wenn mit der Digitalisierung von Maschinen neue „Produkte“ entstehen, weil durch das Erheben von Daten und deren Nutzung eine gänzlich neue Wertschöpfung betrieben wird. Beispielsweise bei der Bewirtschaftung von Gebäuden und anderen Bauwerken mithilfe von Software (Stichwort: Building Information Modeling) ist derartiges seit Längerem schon gelungen. Ist es geplant, zum Erheben der Daten erforderliche Sensoren in die zu bauenden Maschinen einzubringen, ist der gedankliche Weg nicht mehr weit, auch Aktoren einzubringen und Systeme zu vernetzen. Im Fokus soll daher hier das datengetriebene Geschäftsmodell stehen, als ein zu erschließendes Neuland für den produzierenden Mittelstand. Der nachstehende **Überblick zum Rechtsrahmen für Maschinendaten soll** insoweit **als Orientierungshilfe dienen**, für die Produzenten bzw. Maschinenhersteller einerseits sowie die häufig mit gegenläufigen Interessen agierenden Kunden andererseits, also die Rechtsträger, die die Maschinen durch ihre Beschäftigten benutzen und dabei Daten generieren. Für den eiligen Leser sei als Quintessenz vorab mitgeteilt: Ungeachtet der Frage, in welchem dieser Lager man steht, man erhält das, was man sich vertraglich ausbedingt und wenn im Vertrag nichts zu diesem Thema geregelt ist, erhält insoweit man im Zweifel nichts.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
ESF Europäischer Sozialfonds für Deutschland
EUROPÄISCHE UNION
Zusammen. Zukunft. Gestalten.

1. Der Rechtsrahmen für nicht-personenbezogene Daten

Daten, die nicht als personenbezogene Daten zu bewerten sind und deshalb nicht dem Recht des Datenschutzes unterfallen, werden schon seit geraumer Zeit als „*das neue Öl*“ oder „*das neue Gold*“ bezeichnet (ausführlich Fries/Scheufen MMR 2019, 721: Märkte für Maschinendaten – Eine rechtliche und rechtsökonomische Standortbestimmung). Dabei ist es im Vergleich zur Prominenz des Datenschutzrechts in der öffentlichen Wahrnehmung bislang Vielen verborgen geblieben, dass auch die Verordnung (EU) 2018/1807 geltendes Recht ist, die einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der EU geschaffen hat. Die EU-Kommission veröffentlichte erläuternde Leitlinien (COM/2019/250 final) zum Zusammenspiel der Verordnung (EU) 2018/1807 mit der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) und flankierte die Veröffentlichung mit dem Kommentar des damals für den digitalen Binnenmarkt zuständigen Kommissionsvizepräsidenten, Andrus Ansip: „*Bis 2025 dürfte die Datenwirtschaft 5,4 Prozent des BIP der EU-27 generieren, was 544 Mrd. Euro entspricht.*“

Diese Verordnung (EU) 2018/1807 regelt jedoch im Wesentlichen nur die (Un-)Zulässigkeit von Datenlokalisierungsauflagen und ist damit für den praktischen Umgang mit Maschinendaten nahezu nicht relevant. Vor allem ist zu betonen, dass ihre Regelungen gegenüber dem Datenschutzrecht nachrangig sind, was sich ihrem Art. 2 Abs. 2, insbesondere dem Satz 2 ergibt: „*Bei einem Datensatz, der aus personenbezogenen und nicht-personenbezogenen Daten besteht, gilt diese Verordnung für die nicht-personenbezogenen Daten des Datensatzes. Sind personenbezogene und nicht-personenbezogene Daten in einem Datensatz untrennbar miteinander verbunden, berührt diese Verordnung nicht die Anwendung der Verordnung (EU) 2016/679.*“ Was die Wendung untrennbar miteinander verbunden bedeutet, ist in keiner der beiden Verordnungen definiert und zukünftig ggf. durch die Rechtsprechung zu klären. Dieselbe Frage, also wie mit solchen gemischten Datensätzen umzugehen ist, stellt sich auch bei der Bestimmung des Anwendungsbereichs des Datenschutzrechts – also bei der Frage: Sind die Informationen als personenbezogene Daten zu bewerten? Für die Anwendungspraxis folgt daraus, dass diese Rechtsfrage im Hinblick auf die potentiell in Rede stehenden Maschinendaten klar im Vordergrund steht und bei Konzeption und Planung der neuen Wertschöpfung durch Digitalisierung besonders sorgfältig geprüft werden muss.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
ESF Europäischer Sozialfonds für Deutschland
EUROPÄISCHE UNION
Zusammen. Zukunft. Gestalten.

2. Maschinendaten als personenbezogene Daten: Anwendbarkeit des Datenschutzes

Das maßgeblich durch die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) geprägte Datenschutzrecht schützt nicht alle Daten, was einem landläufigen Irrtum entsprechen würde. Vom Gesetz geschützt werden nur „personenbezogene Daten“, mithin alle Informationen, die sich auf eine identifizierte oder identifizierbare **natürliche Person** (die im Datenschutz als "betroffene Person" bezeichnet wird) beziehen. An die Feststellung, dass die in Rede stehenden Daten unter diese Definition fallen, knüpft der Anwendungsbereich des Datenschutzrechts. Besondere Brisanz hat das Thema, weil das Datenschutzrecht von der Regelungstechnik „**Verbot mit Erlaubnisvorbehalt**“ (vgl. Art. 6 Abs. 1 DS-GVO) dominiert wird. Ist es anwendbar, würde in vielen Fällen eben dieses grundsätzliche Verbot durchgreifen und der Nutzung der Maschinendaten entgegenstehen.

Klar kennzeichnende Informationen, wie z. B. der volle Name einer Person, beziehen sich auf eine „identifizierte“ Person (etwa dann relevant, wenn sich ein Beschäftigter zwecks Betriebes der Maschine an dieser mit einem Benutzerkonto anmelden muss). Wesentlich diffiziler ist die Frage, wann Informationen in Bezug auf eine „identifizierbare“ Person vorliegen. Die Verbindung anderer Informationen mit solchen klar kennzeichnenden Informationen, wie etwa dem vollen Namen, bzw. die Möglichkeit, eine Verbindung herstellen zu können, infiziert alle anderen damit in Zusammenhang stehenden Informationen. Ob eine Information auf eine identifizierbare natürliche Person bezogen werden kann und sie deshalb als „personenbezogenes Datum“ zu bewerten ist, beurteilt sich jeweils aus Perspektive des Verantwortlichen (grundsätzlich der Rechtsträger, der mit den Daten Umgang hat) und ist im Grundsatz von seinem Kontextwissen abhängig (ein Bezug zu einer identifizierbaren Person liegt etwa vor, wenn in vorgenanntem Beispiel Informationen über den jeweiligen Zustand der Maschine (vermeintlich Informationen „nur“ in Bezug auf die Maschinen) mit dem zum Zeitpunkt der Benutzung angemeldeten Benutzerkonto in Verbindung gebracht werden). Für die Frage, ob für den Verantwortlichen in Bezug auf eine Information eine natürliche „identifizierbar“ ist, wird zwar zunächst auf das beim Verantwortlichen tatsächlich vorhandene Kontextwissen abgestellt, doch muss er sich für diese Fragestellung nach der Rechtsprechung zusätzlich jegliches Kontextwissen zurechnen lassen, welches er sich mit legalen Mitteln beschaffen könnte (EuGH, Urt. v. 19.10.2016 - C□582/14).

Für die Praxis folgt daraus z. B. die Empfehlung, dass die durch Sensoren generierten Maschinendaten so beschaffen und abgespeichert sein sollten, dass sie sich auf keine identifizierbare natürliche Person beziehen lassen. Wichtig ist insoweit darauf zu achten, dass dies für keinen der Rechtsträger, der Umgang mit diesen Daten hat, jeweils aus seiner Perspektive der Fall sein sollte (es sind also für die

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
ESF Europäischer Sozialfonds für Deutschland
EUROPÄISCHE UNION
Zusammen. Zukunft. Gestalten.

potentiell Beteiligten „Maschinenhersteller“, „Maschinenverleiher“, „Maschinenbenutzer“, etc.) separate Bewertungen dieser über den Anwendungsbereich des Datenschutzrechts entscheidenden Frage vorzunehmen). Dringend zu empfehlen ist es, den im Datenschutzrecht kodifizierten **Grundsatz der Datenminimierung** (vgl. Art. 5 Abs. 1 DS-GVO) nicht erst bei Anwendbarkeit des Datenschutzrechts, sondern schon bereits bei der Planung eines datengetriebenen Geschäftsmodells soweit es geht umzusetzen. Beispielsweise für Systeme, die im Kontext des Maschinenverleihs im B2B Bereich eine unsachgemäße Benutzung einer Maschine erkennen und dokumentieren können sollen, wird es in aller Regel nicht erforderlich sein, diese auf Verwendung von personenbezogenen Daten auszulegen. Im B2C Bereich hingegen ist schon der Kunde eine natürliche Person, so dass Informationen darüber, ob der Kunde eine Maschine unsachgemäß benutzt hat, wohl stets „personenbezogene Daten“ sein werden (auch wenn innerhalb der Maschine die Daten keinen Rückschluss auf die Identität des Benutzers ermöglichen, ist es das Kontextwissen desjenigen, der später Umgang mit diesen Daten hat, welches die Frage beantwortet, ob für ihn diese Daten „personenbezogene Daten“ darstellen).

Sollte es sich konzeptionell nicht vermeiden lassen, dass die Maschinendaten aus einer der Perspektiven als **personenbezogene Daten** zu bewerten sind, ist die geplante Wertschöpfung mit den Maschinendaten daraufhin **zu hinterfragen, ob der Plan überhaupt zulässigerweise realisiert werden darf** und falls ja, welche Anforderungen sodann einzuhalten sind. Dazu ist anzumerken, dass mit Blick auf Maschinendaten in vielen Fällen ergänzend bzw. verdrängend zu den allgemeinen Regeln der Datenschutz-Grundverordnung die spezielleren Regeln der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy)) zur Anwendung kommen. Die im Mai 2018, zum Inkrafttreten der DS-GVO, vom EDSA veröffentlichte „Erklärung des Europäischen Datenschutzausschusses zur Überarbeitung der ePrivacy-Verordnung und zu den Auswirkungen auf den Schutz der Privatsphäre“ hat bis heute nicht an Aktualität verloren, insbesondere soweit es dort heißt: „*Übermittlungsdienste, die zur Erbringung von Maschine-zu-Maschine-Diensten genutzt werden, fallen ebenfalls in den Anwendungsbereich der geltenden Richtlinie.*“ Der EDSA betont dort, wie auch schon zuvor seine Vorgängerinstitution, die sog. Art. 29 Gruppe, in ihrem Working Paper 216, „*dass Metadaten der elektronischen Kommunikation weiterhin ohne Einwilligung weiterverarbeitet werden dürfen, nachdem sie vollständig anonymisiert wurd*en“. Dazu muss man jedoch bedenken, dass Informationen, sobald und solange sie anonymisiert sind, sich gerade nicht auf eine identifizierbare natürliche Person beziehen, mithin keine personenbezogenen Daten sind und deshalb außerhalb des Anwendungsbereichs des Datenschutzrechts liegen.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
ESF Europäischer Sozialfonds für Deutschland
EUROPÄISCHE UNION
Zusammen. Zukunft. Gestalten.

Die ePrivacy-Richtlinie soll nach dem Vorschlag der EU-Kommission vom 10.01.2017 (COM/2017/010 final) zurückgenommen und durch eine Verordnung ersetzt werden – ein politisch hochgradig umstrittener Gesetzesvorschlag. Der am 20.10.2017 verabschiedete Standpunkt des Parlaments betonte die Notwendigkeit, gerade für die Kommunikation in den Bereichen Maschine-zu-Maschine (M2M) und Internet-of-Things (IoT) klarere Abgrenzung gegenüber den allgemeinen Regeln der DS-GVO einzuführen. Maschinendaten werden in diesen Bereichen als Bestandteile „elektronischer Kommunikationsdienste" der Regulierung unterfallen, so dass der weitere Verlauf dieses Gesetzgebungsverfahren für das hier betrachtete Thema von herausgehobener Bedeutung ist. Der am 10.02.2021 gefasste Standpunkt des Rates nähert sich diesem Thema so: „*Sobald elektronische Kommunikationsdaten aus einem geschlossenen Gruppennetz in ein öffentliches elektronisches Kommunikationsnetz übertragen werden, gilt diese Verordnung für diese Daten, auch wenn es sich um M2M-/IoT-Daten und Personal-/Home-Assistant-Daten handelt*."

Für einige Verwirrung sorgt derzeit die Richtlinie (EU) 2019/770 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, deren Umsetzungsfrist noch läuft und deren Inhalte deshalb in Deutschland noch nicht Gesetz wurden. Diskutiert wird der Aspekt „personenbezogene Daten als Gegenleistung". Die Richtlinie selbst hat sich insoweit eigentlich klar positioniert, indem die begrenzenden Elemente betont wurden: „*Digitale Inhalte oder digitale Dienstleistungen werden häufig auch dann bereitgestellt, wenn der Verbraucher keinen Preis zahlt, sondern dem Unternehmer personenbezogene Daten zur Verfügung stellt. Solche Geschäftsmodelle treten in verschiedenen Formen in einem erheblichen Teil des Marktes auf. Obwohl in vollem Umfang anerkannt wird, dass der Schutz personenbezogener Daten ein Grundrecht ist und daher personenbezogene Daten nicht als Ware betrachtet werden können, sollte mit dieser Richtlinie sichergestellt werden, dass die Verbraucher im Zusammenhang mit solchen Geschäftsmodellen Anspruch auf vertragliche Rechtsbehelfe haben*."

Der Praxis könnte also geraten werden, dieses deutsche Umsetzungsgesetz abzuwarten, welches ob dieses Punktes von besonderer Bedeutung für das Thema des Umgangs mit Maschinendaten ist. Sofern es erfolgsrelevant ist, das geplante Geschäftsmodell schnellst möglich auf den Markt zu bringen und daher das Umsetzungsgesetz nicht abgewartet werden kann, sollte zumindest das Gesetzgebungsverfahren beobachtet werden – und das Risiko von Änderungsbedarfen aufgrund geänderter gesetzlicher Rahmenbedingungen kalkuliert werden.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
ESF Europäischer Sozialfonds für Deutschland
EUROPÄISCHE UNION
Zusammen. Zukunft. Gestalten.

3. Neue Wertschöpfungen durch Daten und Systeme: Zuweisung von Rechten?

Für den vorzugswürdigen Fall, dass sich es sich konzeptionell sicherstellen lässt, die Maschinendaten aus der Bewertung als „personenbezogene Daten“ und damit aus dem Datenschutz herauszuhalten, stellt sich die Frage, ob diese (Maschinen-)Daten zugunsten von irgendjemandem geschützt sind? Die wichtigste Feststellung zu diesem Punkt ist die, dass es kein Eigentum an Informationen gibt und damit auch kein Eigentum an Maschinendaten. Eigentum gibt es im Grundsatz nur an Sachen und diese sind qua Definition nur körperliche Gegenstände. Daraus folgt, dass die bisweilen in der Praxis anzutreffenden, vertraglichen Absprachen wie z. B. „*Dateneigentümer der bei Betrieb der Maschine entstehenden Informationen ist der Maschinenhersteller*“ ins Leere laufen. Denn die Rechtsposition „Eigentümer“, in die jemand durch diese Klausel eingewiesen werden soll, gibt es nicht.

Betrachtet man die diversen Rechtsmaterien, die unter dem Begriff „Geistiges Eigentum“ zusammengefasst werden (d.h. das Patent- und das Markenrecht sowie die verwandten Schutzrechte), so ist festzustellen, dass sich diese Regeln – entsprechend dem Eigentum in Bezug auf Sachen – jeweils im Kern um ein ausschließliches Recht an einem immateriellen Gut drehen. Die wohl einzige Materie, die insoweit für die meisten Fälle ernsthaft in Betracht kommt, ist das Recht der Geschäftsgeheimnisse (instruktiv Hessel/Leffer MMR 2020, 647: Rechtlicher Schutz maschinengenerierter Daten). Dieses Rechtsgebiet wurde durch die Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen europaweit harmonisiert, welche in Deutschland durch das Geschäftsgeheimnisgesetz umgesetzt wurde. Mit Inkrafttreten dieses Gesetzes zum 26.04.2019 wurde dabei die hierzulande bislang geltende Rechtslage massiv verändert, insbesondere dadurch, dass Informationen jetzt nicht mehr, weil sie etwaig kraft Natur der Sache geheimhaltungsbedürftig seien, allein deshalb von Rechts wegen als Geschäftsgeheimnis geschützt werden. Der Begriff Geschäftsgeheimnis wurde in Deutschland im Zuge der Gesetzesänderung erstmals legaldefiniert. Diese Definition in § 2 Nr. 1 GeschGehG **setzt** für den Status **Geschäftsgeheimnis das Vorhandensein von angemessenen Geheimhaltungsmaßnahmen voraus**. Möchte sich der Maschinenhersteller zumindest potentiell die Tür offenhalten, Maschinendaten für sich als Geschäftsgeheimnisse reklamieren zu können, muss er jedem, dem er seine Maschinen verkauft, vermietet oder sonst überlässt, vertraglich verbieten, die Maschinendaten zur Kenntnis zu nehmen (um diese Kenntnisnahme „unbefugt“ werden zu lassen). Ferner müssen Geheimhaltungsmaßnahmen, insbesondere technischer Art, in mindestens angemessenem Umfang ergriffen werden. Zudem sollte – in den meisten Fällen müsste – auch das Beobachten, Untersuchen, Rückbauen oder Testen der

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
ESF Europäischer Sozialfonds für Deutschland
EUROPÄISCHE UNION
Zusammen. Zukunft. Gestalten.

Maschine vertraglich untersagt werden, um eine Pflicht zur Beschränkung der Erlangung des Geschäftsgeheimnisses zu konstruieren. Denn kraft Gesetzes sind diese Handlungen, bei Abwesenheit der vorgenannten Beschränkung, zur Erlangung des Geschäftsgeheimnisses erlaubt (vgl. § 3 Abs. 1 Nr. 2 lit. b) GeschGehG).

Kommt es jedoch nicht Betracht, die Maschinendaten effektiv geheim zu halten (etwa weil der Benutzer der Maschine die Daten auch verwenden können soll), bietet gegenwärtig keine der Rechtsmaterien des sog. „Geistigen Eigentums“ einen Rechtsrahmen, in dem man sich mit Maschinendaten bewegt. Der Schutz maschinengenerierter Daten beruht daher in der juristischen Praxis weit überwiegend auf dem **Grundsatz der Privatautonomie**. Es ist vertraglich ein immaterielles Gut zu konstruieren, d. h. **es sind die Rechte und Pflichten an Maschinendaten durch entsprechende Vertragsgestaltung zu erschaffen**, was separate Vertragswerke nicht voraussetzt, sondern auch in Allgemeinen Geschäftsbedingungen erfolgen kann. Weil es zur Anwendung und Auslegung sowohl der zivilrechtlichen, der strafrechtlichen und der kapitalmarktrechtlichen „Verbotsvorbehalte” kaum Rechtsprechung gibt, ist es sogar als erforderlich zu bezeichnen, der bestehenden Rechtsunsicherheit durch Verträge entgegenzutreten (ausführlich Sassenberg/Faber: Rechtshandbuch Industrie 4.0 und Internet of Things, 2. Auflage 2020, § 2 Rn.107 ff.).

Kurzfazit für die Anwendungspraxis: Sowohl zur Förderung von Rechtssicherheit, als auch zur Vermeidung von Streitigkeiten sollten insbesondere die Übermittlung und Nutzung der maschinengenerierten Daten detailliert vertraglich geregelt werden, im Verhältnis von demjenigen, in dessen Besitz sich die Maschine befindet, zu demjenigen, der Zugang zu den Daten haben und diese nutzen können sollen. Besondere Herausforderungen ergeben sich bei mehrseitigen Beziehungen oder Lieferketten, nicht nur deshalb, weil eine Vielzahl von Interessen mit einander kollidiert.

4. Grenzen für vertraglich geschaffene Rechtspositionen an Maschinendaten

Bislang selten betrachtet wurde das Thema Daten im Kontext einer Unternehmensinsolvenz. Eine der Kernaussagen in diesem Kontext ist, dass Daten in die Insolvenzmasse fallen (ausführlich Steinrötter/Bohlsen ZZP 2020, 459: Digitale Daten und Datenträger in Zwangsvollstreckung und Insolvenz). Insoweit sei nur kurz angemerkt, dass vertragliche Gestaltungen, die an die Eröffnung eines Insolvenzverfahrens anknüpfen und dann z. B. Kündigungsmöglichkeiten vorsehen, in aller Regel unwirksam sind (für das in der Praxis häufig anzutreffende Beispiel der Kündigungsmöglichkeit für diesen Fall liegt der Grund darin, dass eine solche Vertragsgestaltung das gesetzliche Wahlrecht des Insolvenzverwalters, ob laufende Verträge fortgesetzt werden oder nicht, aushöhlen würde).

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
ESF Europäischer Sozialfonds für Deutschland
EUROPÄISCHE UNION
Zusammen. Zukunft. Gestalten.

Der Vertragsgestaltung zur Konstruktion von Rechten an Maschinendaten sind zudem dort Grenzen gesetzt, wo es kraft Gesetzes Zugangsrechte zu Daten gibt. Solche ergeben sich nur höchst ausnahmsweise aus allgemeinen Gesetzen, also solchen, welche sich nicht speziell mit Daten befassen. Anzuführen ist insoweit namentlich das Kartellrecht und ein etwaiger sich daraus ergebener Kontrahierungszwang, der zur Erteilung sog. Zwangslizenzen führen kann. Die sog. „essential facilities doctrine“ könnte auf einen Datenbestand anzuwenden sein (ausführlich Louven NZKart 2018, 217: Datenmacht und Zugang zu Daten) oder die Verhinderung des Zugangs zu den Daten bzw. zum System, welches mit den Daten arbeitet, könnte im Einzelfall ein Marktmachtmissbrauch sein (wie z.B. in BGH, Urt. v. 06.10.2015 − KZR 87/13, Rn. 108 ff.). Im Wesentlichen ergeben sich gesetzliche Zugangsrechte indes aus Gesetzen, die spezielle Regelungen für den Umgang mit Daten beinhalten. Am 25.11.2020 veröffentlichte die EU-Kommission einen Vorschlag für eine neue Verordnung, der sie den Titel **„Daten-Governance-Gesetz“** gab **(COM(2020) 767 final)**. Sobald sich der Rat und das Parlament je einen Standpunkt zu diesem Vorschlag gebildet haben, wird der Trilog, mithin das ordentliche europäische Gesetzgebungsverfahren seinen Lauf nehmen. Ziel des allgemein gehaltenen, also nicht-sektorspezifischen Vorschlags ist ein Rechtsrahmen für die Nutzung von Daten, die im Rahmen bestehender Vorschriften zur Verfügung gestellt werden, ohne diese bestehenden Vorschriften zu ändern oder neue sektorale Verpflichtungen zu schaffen. Insoweit sei nur am Rande bemerkt, dass es sektorspezifische Rechtsvorschriften über den Datenzugang gibt, die bereits in Kraft sind, in Bereichen wie Automobilindustrie (Verordnung (EG) Nr. 595/2009 – u. a. Zugang zu Fahrzeugreparatur- und -wartungsinformationen), Zahlungsdienstleister (Richtlinie (EU) 2015/2366 – u. a. Zugang zu Bankkonten und Zahlungsdaten) , Daten intelligenter Verbrauchsmesssysteme (Richtlinie (EU) 2019/944), Stromnetzdaten (Verordnung (EU) 2017/1485), intelligente Verkehrssysteme (Richtlinie 2010/40/EU), Umweltinformationen (Richtlinie 2003/4/EG) und Geodaten (Richtlinie 2007/2/EG – u. a. Schaffung einer gemeinsamen Geodateninfrastruktur (INSPIRE)).

Das nunmehr vorgeschlagene Daten-Governance-Gesetz zielt insbesondere darauf ab, **die Verfügbarkeit von Daten zur Nutzung zu fördern**, indem es **Regelungen für die gemeinsame Datennutzung durch Unternehmen gegen Entgelt** in jedweder Form enthält. Auch soll die Nutzung personenbezogener Daten ermöglicht werden, mithilfe eines „Mittlers für die gemeinsame Nutzung personenbezogener Daten“, der die betroffene Person bei der Ausübung ihrer Rechte gemäß der Datenschutz-Grundverordnung unterstützen soll. Es steht jedoch zu erwarten, dass dieser Vorschlag für eine neue Verordnung hochgradig umstritten sein wird (vgl. etwa Wischmeyer/Herzog NJW 2020, 288:

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
ESF Europäischer Sozialfonds für Deutschland
EUROPÄISCHE UNION
Zusammen. Zukunft. Gestalten.

Daten für alle? Grundrechtliche Rahmenbedingungen für Datenzugangsrechte) und das Gesetzgebungsverfahren daher sehr lange dauern wird.

5. Keine Daten ohne Systeme – Anforderungen an Systeme?

Der Blick auf die Maschinendaten muss damit abgerundet werden, dass man sich bewusst macht, dass die Daten als solche nicht der einzige Anknüpfungspunkt für zukünftige und heute schon vorhandene Gesetze sind. Wird wie eingangs erwähnt, neue Wertschöpfung dadurch erreicht, dass alte Maschinen „smart“ gemacht werden, gelten für diese Maschinen rechtliche Anforderungen, die wahrscheinlich zuvor nicht einschlägig waren. Wird z. B. zur Beantwortung der Frage, wie die in der Maschine während ihrer Benutzung generierten Daten aus der Maschine heraus transportiert werden sollen, die Antwort WiFi, Bluetooth, NFC, o. ä. gegeben, bewegt man sich in der Regel in den jeweils nationalen Gesetzen zur Umsetzung z. B. der Richtlinie 2014/53/EU über die Bereitstellung von Funkanlagen auf dem Markt, der Richtlinie 2014/35/EU über die Bereitstellung elektrischer Betriebsmittel (Niederspannungsrichtlinie) oder der Richtlinie 2014/30/EU über die elektromagnetische Verträglichkeit.

Abgesehen von den somit angesprochenen **elektrotechnischen Herausforderungen**, denen man sich als produzierender Mittelständler sicherlich gut gewachsen sieht, muss man auch die **Herausforderungen der Informationstechnologie** in den Blick nehmen. Angenommen die Kühlschränke, die man bislang produzierte, sollten nunmehr als „smarte“ Kühlschränke nach dem Konzept von IoT permanent mit dem Internet verbunden sein, so darf man die Frage nach der Verantwortlichkeit stellen, wenn dieser Kühlschrank zum Zombie in einem Botnetz wird und gesteuert durch den Command & Control Server Angriffe gegen die IT eines Krankenhauses fährt, wodurch dort Steuerungssysteme ausfallen und Menschen ums Leben kommen. Wie das Handelsblatt und zahlreiche weitere Medien am 18.09.2020 zu berichten wussten, kam es nach einem Hackerangriff auf die Uni-Klinik Düsseldorf zu einem Todesfall. Am 09.02.2021 berichtete der Sicherheitsspezialist G DATA, dass sich im US-Bundesstaat Florida Unbekannte über ein schlecht gesichertes Remote-Wartungsprogramm Zugriff auf Systeme eines Wasserwerkes verschafft hatten. Dabei konnten sie die Konzentration einer zur Wasserbehandlung eingesetzten Chemikalie verändern. Aus Sicherheitskreisen wie etwa dem Cybercrime-Kompetenzzentrum beim LKA NRW ist nunmehr schon seit mindestens zwei Jahren regelmäßig wiederkehrend zu vernehmen, dass sich die Frage nicht mehr stellt, ob sich ein Unternehmen einem Cyberangriff ausgesetzt sehen wird, sondern heute nur noch zu fragen ist, wann der nächste Angriff stattfinden wird. Die Lage der IT-Sicherheit in Deutschland 2020 wurde vom

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
ESF Europäischer Sozialfonds für Deutschland
EUROPÄISCHE UNION
Zusammen. Zukunft. Gestalten.

Bundesamt für Sicherheit in der Informationstechnik im gleichnamigen Jahresbericht, den die Behörde am 20.10.2020 veröffentlichte, als „angespannt“ bezeichnet. Um zwei andere Beispiele zu nennen, die nicht Leib und Leben bedrohten, sondern nur Geld und wirtschaftliche Existenzen: Der niedersächsische MDax-Konzern Symrise, der etwa 10.000 Mitarbeiter beschäftigt, wurde Mitte Dezember 2020 Opfer einer schweren Attacke unbekannter Hacker. Die Produktion in Holzminden stand weitgehend still, berichtete das Handelsblatt am 14.12.2020. Andere Zeitungen berichteten nicht nur von IT-Sicherheitsvorfällen, sondern wurden selbst davon beeinträchtigt. Die Funke Mediengruppe wurde am 22.12.2020 nach eigenen Angaben Opfer eines Hackerangriffs. Die Tageszeitungen WAZ, Hamburger Abendblatt und Berliner Morgenpost erschienen in der Folge als erheblich dünnere Notausgaben. Diese Beispiele zeigen, dass zunehmend kriminelle Energie gezielt gegen Schwachstellen der IT-Sicherheit eingesetzt wird, etwa um Lösegeldzahlungen zu erpressen. Mit dem 2019 als Präventionsprojekt der Sicherheitspartnerschaft NRW erstmalig erstellten „Lagebild Wirtschaftsschutz“ wurden aufgrund repräsentativer Erhebungen Beschreibungen der Unternehmenssicherheit erarbeitet, mit dem Fokus auf Wirtschafts- und Cyberkriminalität gegen kleine und mittlere Unternehmen. Während althergebrachte, physische Sicherheitsaspekte durchaus von den meisten Unternehmen adäquat adressiert wurden, war die IT-Sicherheit eher unerschlossenes Brachland.

Der **Rechtsrahmen für die IT-Sicherheit** in allgemeinen Produkten bzw. Maschinen ist aktuell noch als **rudimentär** zu bezeichnen. Der zuvor erwähnte Todesfall löst reflexartig Überlegungen aus, die in Richtung Produktsicherheit und Produkthaftung gehen und die auch – ungeachtet der neuen Technik – in den alten Rechtsrahmen passen, weil dieser technikneutral formuliert ist. Dieser **Haftungsrahmen** ist ganz besonders **in den Blick** zu **nehmen**, **falls** – wie eingangs erwähnt – in die Maschinen im Zuge der Digitalisierung **auch Aktoren**, also Komponenten zur Steuerung der Maschine, **eingebracht** werden sollen (oder bereits **vorhanden** sind) **und die Systeme** dann auch noch **vernetzt** werden.

Thematisch spezielle Anforderungen brachte im Jahr 2015 das „IT-Sicherheitsgesetz“. Es fügte in § 13 TMG einen neuen Absatz 7 ein, der die entscheidenden Vorgaben macht, jedenfalls dann, wenn über die Systeme die Maschinendaten auch dem Benutzer der Maschine zugänglich gemacht werden. Zumindest in diesen Fällen dürfte von einem Anbieter-Nutzer Verhältnis im Sinne des TMG auszugehen und der Anwendungsbereich vorgenannter Norm unzweifelhaft eröffnet sein. Danach ist u. a. **durch technische und organisatorische Vorkehrungen sicherzustellen**, **dass kein unerlaubter Zugriff auf die für den Dienst genutzten technischen Einrichtungen möglich ist**. Verstöße gegen die Norm sind aktuell schon bußgeldbewehrt; allerdings ist noch kein Fall öffentlich bekannt geworden, in dem ein

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
ESF Europäischer Sozialfonds für Deutschland
EUROPÄISCHE UNION
Zusammen. Zukunft. Gestalten.

solches Bußgeld einmal verhängt worden wäre. Der Bundestag debattierte am 28.01.2021 über den Entwurf des „IT-Sicherheitsgesetz 2.0“ BT-Drs. 19/26106). Im Entwurf vorgeschlagen ist ein neuer § 7d BSI-G, der dem Bundesamt für Sicherheit in der Informationstechnik eine Kompetenz verleihen soll, Anordnungen zur Mangelbeseitigung im Bereich der Schutzmaßnahmen gem. § 13 Abs. 7 TMG treffen zu können. Am Rande bemerkt sei, dass im Bundeskabinett der Entwurf eines Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) zirkuliert (und auch schon der Öffentlichkeit „geleakt“ wurde), der jedoch vom Kabinett noch nicht beschlossen wurde. Daher hat die Bundesregierung das Gesetzgebungsverfahren dazu noch nicht förmlich eingeleitet. Der an die Öffentlichkeit gelangte Entwurf sieht eine Aufhebung u. a. von § 13 TMG vor, wobei die dort in Absatz 7 durch das IT-Sicherheitsgesetz 2015 eingeführte Regelung erhalten bleiben und nur an eine andere Stelle (§ 19 Abs. 4 TTDSG) verschoben werden soll. Mit dem im Bundestag gestellten Antrag vom 09.02.2021 (BT-Drs. 19/265339) wird derzeit versucht, die Bundesregierung dazu zu bewegen, das Gesetzgebungsverfahren zum TTDSG formell einzuleiten. Da sich dieser Entwurf auch auf die Umsetzung der ePrivacy-Richtlinie in Deutschland bezieht, ist dieses Gesetzgebungsverfahren, so es denn begonnen wird, von herausgehobener Bedeutung für den zukünftigen Umgang mit Maschinendaten.

Mit Blick auf die Praxis ist bedauerlich, dass das Thema Maschinendaten in einen sich gegenwärtig stark in Veränderungsprozessen befindlichen Rechtsrahmen fällt. Gleichzeitig ist aus diesem Blickwinkel heraus erfreulich, dass die bislang nur rudimentär vorhandenen Regeln ausgebaut und dadurch konkretisiert werden, so dass für die Zukunft eine verlässlichere Basis geschaffen wird. Hinsichtlich der Reformen im Zusammenhang mit dem IT-Sicherheitsgesetz 2.0 und dem Telekommunikations-Telemedien-Datenschutzgesetz könnte es für die beteiligten Praktiker ein Ansatz sein, zumindest die die Wahl zum 20. Deutschen Bundestag abzuwarten, die für den September des laufenden Jahres geplant ist. Sollten die beiden genannten Reformen nicht bis dahin mit Gesetzgebungsverfahren abgeschlossen worden sein, darf aufgrund des Grundsatzes der Diskontinuität davon ausgegangen werden, dass erst wieder einige Zeit vergehen wird, bis die die Themen dann – ggf. – erneut auf Tagesordnung kommen.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
ESF Europäischer Sozialfonds für Deutschland
EUROPÄISCHE UNION
Zusammen. Zukunft. Gestalten.

6. Ausblick

Das Thema ist politisch hochgradig virulent und Änderungen der Rechtslage sind zu erwarten. Am 19.02.2020 verkündete die EU-Kommission die sog. „europäischen Datenstrategie“ und sie legt u. a. am 25.11.2020 den bereits oben erwähnten Entwurf des „Daten-Governance-Gesetz“ (COM(2020) 767 final) sowie am 16.12.2020 den Entwurf für eine neue Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen IT-Sicherheitsniveaus (COM(2020) 823 final) vor. In Deutschland beschloss am 27.01.2021 das Kabinett die sog. „Datenstrategie der Bundesregierung“ – mit rund 240 Maßnahmen…

Autor: **Stefan Sander, LL.M., B.Sc.**

Rechtsanwalt und Fachanwalt für IT-Recht
Software-Systemingenieur

Das Forschungs-und Entwicklungsprojekt AnGeWaNt wird im Rahmen des Programms „Zukunft der Arbeit“ (Förderkennzeichen: 02L17B055) vom Bundesministerium für Bildung und Forschung (BMBF) und dem Europäischen Sozialfonds (ESF) gefördert und vom Projektträger Karlsruhe (PTKA) betreut. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.