Mittelstand 4.0
Kompetenzzentrum
Hamburg

DIGITAL
▶VORAUS

LEITFADEN

RECHTLICHE ASPEKTE DER DIGITALISIERUNG

NEUE TECHNOLOGIEN WIE KÜNSTLICHE INTELLIGENZ, IoT, DATA ANALYTICS ODER BLOCKCHAIN RECHTSKONFORM EINSETZEN

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

RECHTLICHE ASPEKTE DER DIGITALISIERUNG –

NEUE TECHNOLOGIEN WIE KÜNSTLICHE INTELLIGENZ, DATA ANALYTICS, IoT ODER BLOCKCHAIN RECHTSKONFORM EINSETZEN

Sehr geehrte Damen und Herren,

bei unserer Arbeit mit mittelständischen Unternehmen im Mittelstand 4.0-Kompetenzzentrum Hamburg stellen wir immer wieder fest, dass große Unsicherheit bezüglich der rechtlichen Implikationen der Digitalisierung bzw. der Industrie 4.0 besteht. Die Vielzahl der aktuellen Veränderungen sowohl auf technologischer Seite als auch im regulatorischen Umfeld wirft bei vielen Unternehmen Fragen auf.

Diese Unsicherheit droht die digitale Transformation zu verlangsamen.

Um hier mehr Klarheit zu schaffen, wurde dieser Leitfaden erarbeitet, der konkrete und aktuelle Hinweise zu rechtlichen Rahmenbedingungen gibt und hilft, rechtliche Fallstricke zu vermeiden. Auch wenn ein Leitfaden niemals die Beratung durch einen Juristen ersetzen kann, helfen Ihnen die enthaltenen Fallbeispiele, um verschiedene Technologien reflektiert einsetzen zu können und selbstbewusst mit der Digitalisierung Ihres Unternehmens voranzuschreiten.

Prof. Dr. Dr. h. c. Wolfgang Kersten

INHALTSVERZEICHNIS

EINS

EINLEITUNG

Gemäß einer Studie der KfW Bankengruppe aus April 2019 [1] haben bereits 30 % der deutschen Mittelstandsunternehmen erfolgreich Digitalisierungsprojekte abgeschlossen, Tendenz steigend. Größte Hindernisse bei diesen Projekten sind gemäß Umfragen die Themen Security, Datenschutz und Kontrollverlust über die eigenen Daten [2]. Dieser Leitfaden soll dabei helfen, die Funktionsweise und Vorteile der neuen Technologien besser zu verstehen und einen Überblick zu den rechtlichen Fallstricken bei deren Umsetzung geben.

ZWEI

RECHTLICHE GRUNDLAGEN ZUR DATENVERARBEITUNG

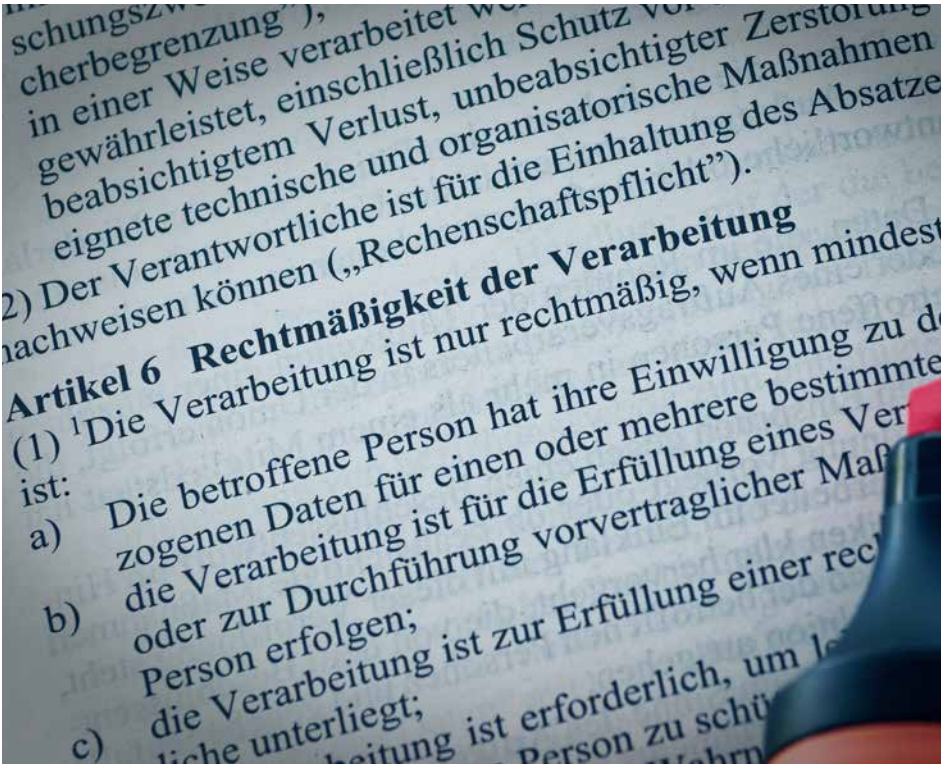
Es gibt viele Rechtsgebiete, die beim Einsatz von Informationstechnologien anwendbar und zu berücksichtigen sind, etwa das IT-Vertragsrecht, das Urheberrecht, das Markenrecht und auch das IT-Strafrecht. Die wohl in der Praxis relevantesten Anforderungen ergeben sich jedoch aus dem Datenschutzrecht. Hier greift der Grundsatz zum **Verbot mit Erlaubnisvorbehalt** [3]. Datenrelevante Maßnahmen sind hiernach grundsätzlich rechtswidrig, es sei denn, ein gesetzlich normierter Erlaubnisgrund rechtfertigt sie. Eine solche Rechtfertigung kann sich insbesondere aus Art. 6 der EU-Datenschutz-Grundverordnung („DSGVO") sowie für den Arbeitsnehmerdatenschutz aus § 26 Bundesdatenschutzgesetz [4] ergeben. Letztere Vorschrift findet nur im „Beschäftigungskontext" Anwendung, also wenn die Verarbeitung für Zwecke des Beschäftigungsverhältnisses erfolgt. Dies wäre etwa bei Neueinführung eines Systems zur Arbeitszeiterfassung der Fall, nicht jedoch bei Neueinführung eines IT-Sicherheitssystems, obwohl dort auch personenbezogene Mitarbeiterdaten verarbeitet werden. Im letzteren Fall wäre insoweit wieder der allgemeine Erlaubnisgrund des Art. 6 DSGVO eröffnet.

Wichtigste Norm als Rechtsgrundlage für die Datenverarbeitung ist damit **Art. 6 DSGVO.** Vor Einführung neuer Technologien im Unternehmen sollte daher zwingend geprüft werden, ob eine der dortigen Alternativen als Erlaubnis für die geplante Verarbeitung dienen kann. Da die dortigen Regelungen in Art. 6 Abs. 1 S.1 lit. c) bis e) [5] nur in Ausnahmefällen greifen (rechtliche Verpflichtung, lebenswichtige Interessen, öffentliches Interesse), geht es insbesondere um die Alternativen in lit. a), lit. b) und lit. f), also Einwilligung, Vertragserforderlichkeit und Interessenabwägung.

Hat der Betroffene, dessen Daten in der neuen Software verarbeitet werden sollten, zuvor nach ausreichender Belehrung ausdrücklich hierzu eingewilligt, dann liegt insoweit eine Rechtsgrundlage nach Art. 6 lit. a) DSGVO vor. Allerdings hat der Betroffene anschließend nach Art. 7 Abs. 3 DSGVO jederzeit das Recht, seine **Einwilligung** zu widerrufen, was die Verarbeitung zukünftig wieder unrechtmäßig machen würde. Anders ist dies bei der **Vertragserforderlichkeit.** Solange die Verarbeitung erforderlich ist, um einen bestehenden Vertrag mit dem Betroffenen erfüllen zu können, bleibt die Verarbeitung rechtmäßig, etwa bei Erfüllung des über einen Onlineshop zustande gekommenen Vertrages. Liegt weder eine Einwilligung des Betroffenen, noch ein Vertrag mit diesem vor, so verbleibt in

den meisten Fällen nur die **Interessenabwägung** nach Art. 6 lit. f) DSGVO. Es ist daher zu prüfen, ob die berechtigten Interessen des Unternehmens an einer Verarbeitung der personenbezogenen Daten durch die neue Technologie die schutzwürdigen Interessen der jeweils Betroffenen an einer Nicht-Verarbeitung überwiegen. Diese Interessenabwägung ist zu dokumentieren [6]. Auch hier hat der Betroffene jedoch – wie bei der Einwilligung – die Möglichkeit, eine Verarbeitung später zu verbieten und zwar in diesem Fall nach Art. 21 DSGVO durch Widerspruch, soweit nicht zwingende schutzwürdige Gründe entgegenstehen.

Im Ergebnis ist daher bei jeder der nachfolgend beschriebenen Einzeltechnologien vor Einführung zu prüfen, ob für die anstehende Verarbeitung eine Rechtsgrundlage besteht, insbesondere aus Art. 6 DSGVO sowie im Beschäftigtenbereich nach § 26 BDSG.



DREI

RECHTSKONFORMER EINSATZ NEUER TECHNOLOGIEN

3.1 Internet der Dinge

A) TECHNISCHE ERLÄUTERUNG

Ein bestimmendes Element des Internet der Dinge (engl. Internet of Things, IoT) ist die digitale Vernetzung physischer Objekte („Smart Products"). Die mit smarten Sensoren oder Auto-ID-Technik (z.B. Barcode, RFID) ausgestatteten Objekte und Maschinen verfügen über eine eindeutige Identität im Netzwerk. Die Objekte können so untereinander über das Internet kommunizieren und Daten austauschen. Zusätzlich wird die automatische Erfüllung bestimmter Aufgaben möglich. Man spricht von cyber-physischen Systemen (CPS), die die Basis für das Internet der Dinge bilden und eine Verknüpfung von physischen Objekten und virtuellen Daten realisieren. [7, p. 7]

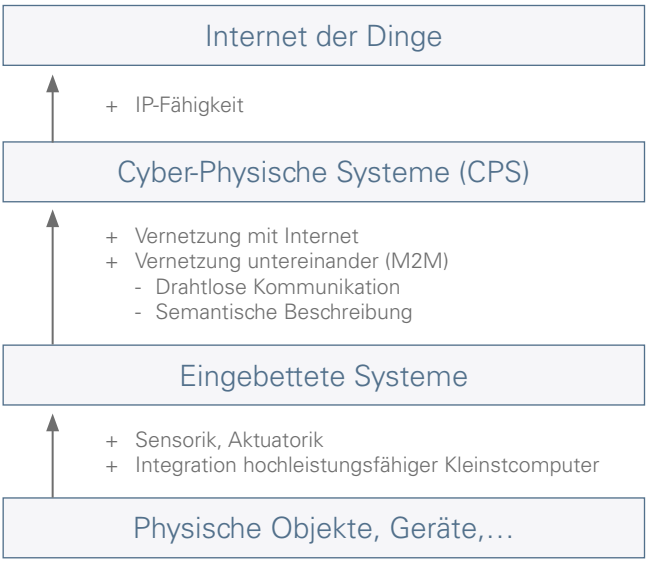


Abbildung 1: Darstellung in Anlehnung an Bauernhansl et al. (S. 604)

Cyber-physische Systeme enthalten eingebettete Systeme, so dass diese Systeme über das Internet kommunizieren können. Durch die Ausstattung mit Sensorik lässt sich die Umwelt erfassen und auswerten. Über die reale Umgebung lässt sich so eine große Menge an Daten sammeln und analysieren. [8, p. 15f.] Durch die Kombination von Sensoren und Aktoren auf der einen Seite und dezentrale Entscheidungseinheiten auf der anderen Seite werden miteinander kommunizierende, selbständige Einheiten realisiert [9, p. 177]. Ziel des Internet der Dinge ist die Verbesserung der Interaktion sowohl zwischen Mensch und Maschine als auch zwischen Maschinen [7, p. 7]. Smart Home oder Smart Factory lassen sich als beispielhafte Konzepte nennen, die auf dem Internet der Dinge basieren.

B) PRAXISBEISPIEL

Mit einer Anzahl von fast drei Millionen registrierten IoT-Geräten sind heute smarte Geräte und Alltagsgegenstände allgegenwärtig. Mit dieser steigenden Konnektivität steigt allerdings auch die Angriffsfläche für Cyberkriminelle. Von den drei Millionen registrierten Geräten weisen laut einer Studie des Softwareunternehmens Avast über 175.000 Sicherheitslücken auf [10]. Dabei reicht ein einziges, ungeschütztes Gerät aus, um eine Vielzahl von Geräten in ein Botnetz zu verwandeln und für unzulässige Zwecke einzusetzen. Einige Sicherheitsforscher deckten 2017 in diesem Zusammenhang eine Sicherheitslücke in einem Reinigungsautomaten für Laborbedarf von Miele auf [11]. Über diese konnten sich die „Angreifer" Zugriff auf beliebige Daten des Rechners ermöglichen, auf denen der Webserver lief. Miele setzte sich daraufhin mit den Anwendern der betroffenen Reinigungsautomaten in Verbindung, um über die Sicherheitslücke zu informieren und ein Software-Update zur Behebung dieser bereitzustellen.

C) RECHTLICHE BEWERTUNG MIT CHECKLISTE

Im Zusammenhang mit dem Internet der Dinge sind viele rechtliche Fragen noch offen, deshalb ist eine vertragliche Regelung fast immer empfehlenswert. Wesentlich in der **Vertragsgestaltung** mit Anbietern von Smart Products ist die Ausgestaltung der **Haftung** für vernetzte Systeme, die sowohl natürliche (z.B. Einzelunternehmer) als auch juristische Personen (z.B. Aktiengesellschaften) treffen kann. Im Regelfall haftet bei einem vom eingesetzten System verursachten Schaden dessen Betreiber gegenüber den Verletzten. Lag der Fehler jedoch in der mangelhaften Hard- oder Software des Herstellers, so kann sich der Betreiber bei diesem schadlos halten, was bestenfalls aufgrund eines gut gestalteten Vertrages erfolgen sollte, da die Gesetzeslage Anspruchsteller benachteiligt.

Im Hinblick auf das **Datenschutzrecht** ist zu beachten, dass vernetzte Objekte, etwa als „Wearables" oder über die enthaltene Sensorik, große Mengen an Informationen sammeln. Darunter sind häufig auch personenbezogene Daten der Anwender oder Arbeitnehmer, die aufgrund der digitalen Vernetzung sowohl an andere Objekte als auch in das Internet übermitteln werden. Sowohl bei der Erhebung als auch bei der Übermittlung der Daten handelt es sich um rechtfertigungsbedürftige Datenverarbeitungen im Sinne der DSGVO. Werden die durch das cyber-physische System gesammelten Daten an eine andere Stelle übermittelt, etwa zur Aufbereitung oder Auswertung, stellt dies im Regelfall eine Auftragsverarbeitung nach Art. 28 DSGVO dar, für die der Abschluss eines Auftragsverarbeitungsvertrages in schriftlicher oder elektronischer Form (PDF) erforderlich ist. Daneben müssen nicht nur im Hinblick auf die gesammelten Daten, sondern auch auf die Smart Products selbst die Anforderungen des Art. 32 DSGVO [13] eingehalten werden. Zu diesen gehört unter anderem die Absicherung der Systeme nach außen, etwa durch den Betrieb in einem separaten Netzwerk.

Achtung:
Werden Arbeitnehmerdaten im Rahmen des Internet der Dinge erhoben, ist eine datenschutzrechtliche Rechtfertigung nach § 26 BDSG (Beschäftigungskontext) bzw. Art. 6 DSGVO (sonstiger Kontext) erforderlich. Es dürfen nur solche Daten erhoben werden, die erforderlich sind, um den konkreten Zweck (bspw. Effizienzsteigerung) zu erreichen.

Im Hinblick auf die **Rechte an Daten,** die durch vernetzte Objekte generiert werden, ist umstritten, ob es ein absolutes Recht an maschinengenerierten

TIPP:

Um Haftungsrisiken zu vermeiden oder zumindest kalkulierbar zu machen, sollten mit Anbietern von Smart Products klare Risikozuweisungen vereinbart werden, die mögliche Schadensfälle definieren und Haftungsfolgen regeln. Sind mehrere Anbieter beteiligt, ist eine genaue Dokumentation der jeweils übernommenen Arbeiten unerlässlich. Ist neben den Smart Products auch der Betrieb von IT-Infrastruktur geschuldet, sollte eine hohe Verfügbarkeit der Services (mind. 99 % im Jahresdurchschnitt) vereinbart werden. Da Smart Products häufig von Hackern angegriffen und missbraucht werden [12], sollte zudem sichergestellt werden, dass eine hochwertige Sicherheitsarchitektur sowie regelmäßige Updates geschuldet sind.

TIPP:

Liegt bereits ein IT-Sicherheitskonzept vor, sollte dieses auf Smart Products ausgeweitet werden, was nebenbei positive Auswirkungen auf die Erfüllung der Anforderungen aus dem obigen GeschGehG haben dürfte.

Daten überhaupt gibt. In jedem Fall sollte jedoch geklärt werden, wer das Recht an der betreffenden Datenbank (§§ 87b UrhG) besitzt. Zudem können Daten durch das neue Geschäftsgeheimnisgesetz („GeschGehG") geschützt sein, wenn sie durch organisatorische, technische sowie vertragliche Schutzmaßnahmen besonders gesichert sind. Solche Maßnahmen sollten daher auch hinsichtlich der Smart Products selbst umgesetzt werden. Werden Analyse- und Rechenschritte von unterschiedlichen Unternehmen durchgeführt, ist zusätzlich eine vertragliche Regelung zur Klärung von Zugriff, Verwendung und Nutzungsrechten der Daten sinnvoll.

WAS IST ZU TUN?

- [ ] Verträge mit Anbietern der Smart Products schließen
  - Haftungsregelung für Schäden bei Dritten
  - Haftungsregelung für Schäden beim Anwender
  - Genaue Produktbeschreibung (insb. Verfügbarkeit der Dienste, IT-Sicherheit)
- [ ] Implementierung technischer und organisatorischer Maßnahmen, Art. 32 DSGVO
- [ ] Prüfung, an wen eine Datenübermittlung durch die Smart Products erfolgt, notfalls dann Verträge zur Auftragsverarbeitung schließen
- [ ] Implementierung von Geheimnisschutz nach dem GeschGehG

3.2 Data Analytics

A) TECHNISCHE ERLÄUTERUNG

Die umfassende Nutzung von Daten, die statistische und quantitative Analyse dieser Daten und Erstellung von erklärenden und prädiktiven Modellen lassen sich unter dem Begriff Analytics zusammenfassen. Im Analytics Prozess finden unter anderem statistische Methoden und lineare Programmierung Anwendung, um die vorliegenden Daten zu erforschen, zu visualisieren und Zusammenhänge zu entdecken. [14, p. 44]. Data Analytics beschreibt den Prozess der Untersuchung, Bereinigung, Transformation und Modellierung von Daten. Dabei wird das Ziel verfolgt nützliche Informationen zu entdecken, Schlussfolgerungen vorzuschlagen und die Entscheidungsfindung zu unterstützen. Der Fokus liegt auf der Wissensgewinnung für vorhersagende und beschreibende Zwecke, so dass neue Ideen entdeckt oder bestehende Ideen bestätigt werden. Durch Anwendungen aus dem Bereich des Internet der Dinge ist die Datenmenge stark gestiegen, so dass auch Data Analytics an Bedeutung gewonnen hat. [15, p. 47].

Abbildung 2: Eigene Darstellung der fünf Phasen des Data Analytics Prozess in Anlehnung an Sedkaoui

Der Data Analytics Prozess lässt sich in fünf Phasen einteilen. Die erste Phase beschreibt die Datenerfassung, die beispielsweise durch fortschrittliche Technologien wie Sensoren erfolgt. In dieser Phase werden die Daten sowohl hinsichtlich ihrer Herkunft und ihres Formats als auch in Bezug auf Genauigkeit und Konsistenz validiert. [16, p. 84] Anschließend folgt in der zweiten Phase die Vorbereitung der Daten, in der die Daten nach bestimmten Kriterien klassifiziert und bereinigt werden. Die Daten werden so aufbereitet und kodiert, dass sie kompatibel mit dem verwendeten Algorithmus sind. In der dritten Phase findet die Analyse der Daten statt. In diesem Schritt soll ein besseres Verständnis für die Verhaltensweisen der Daten und den zugrundeliegenden Phänomenen erlangt werden. [17, p. 85] Es folgt die Phase der Bewertung und Interpretation, in der beispielsweise die Robustheit und Genauigkeit des Models getestet wird. Abschließend folgt die

fünfte Phase mit dem Einsatz des Models, in dem die Daten in verwertbares Wissen umgewandelt werden. Ebenfalls Teil dieser Phase ist die Visualisierung der Daten bzw. des erlangten Wissens angepasst an die Anforderungen der Situation. [18, p. 86 f.]

B) PRAXISBEISPIEL

Durch Data Analytics wurden in den letzten Jahren verbesserte Methoden zur Generierung von Informationen zur Unterstützung der Entscheidungsfindung bereitgestellt, die von Unternehmen genutzt werden, um strategische Entscheidungen schneller, besser und genauer zu treffen und Ressourcen effizient und effektiv einzusetzen. Das britische Unternehmen Cambridge Analytica setzte Data Analytics bis 2018 im Bereich des Mikrotargetings ein und beeinflusste den US-Wahlkampf durch individuelle Botschaften an die Wähler. Die Grundlage für die Wahlkampfarbeit bildeten Daten aus rund 87 Millionen Facebook-Profilen, aus denen Persönlichkeitsprofile erstellt wurden [19]. Das Unternehmen hatte diese allerdings illegal erworben, was einen Skandal um Facebook und Cambridge Analytica auslöste, der in der Insolvenz von Cambridge Analytica resultierte [20].

C) RECHTLICHE BEWERTUNG MIT CHECKLISTE

Bei der Anwendung von Data Analytics liegt ein erstes Problem in der **rechtmäßigen Erlangung** der auszuwertenden Daten, da häufig Datenbestände aus öffentlich zugänglichen Quellen hinzugezogen werden. Dabei können bei der Verwendung oder Speicherung von Daten aus Datenbanken, ggf. auch aus sozialen Netzwerken, die Rechte des Datenbankerstellers nach § 87b UrhG verletzt werden. Dieser Schutz ist regelmäßig jedoch nur dann verletzt, wenn wesentliche Teile der Daten betroffen sind oder eine wiederholte und systematische Entnahme stattfindet. Die normale Auswertung dieser Daten kann in der Regel problemlos stattfinden, solange technische und organisatorische Einrichtungen des Datenbankinhabers nicht umgangen werden.

Achtung:
Öffentliche Datenquellen haben meist Lizenzbedingungen. Für alle Datenquellen ist deshalb im Vorwege zu überprüfen, ob die geplante Nutzung gestattet wird.

Werden Daten gekauft, kann die Herkunft der Daten nicht immer überprüft werden. Deshalb sollte bei der Vertragsgestaltung darauf geachtet werden, dass neben einer umfassenden Übertragung der Nutzungsrechte an den Daten auch eine Haftungsfreistellung erfolgt, etwa für den Fall, dass die Daten Rechte oder Geschäftsgeheimnisse Dritter verletzen.

Werden bei der Datenanalyse nicht nur Unternehmensdaten, sondern auch personenbezogene Daten verarbeitet, ist das **Datenschutzrecht** zu beachten. Dabei ist selbst bei der Verwendung der Daten von Bestandskunden wiederum eine gesonderte Rechtfertigung nach Art. 6 DSGVO erforderlich. Eine bereits eingeholte Einwilligung in die Datenverarbeitung **zu anderen** Zwecken ist dafür nicht ausreichend. Sofern die betroffenen Personen umfassend über die konkrete Datenanalyse informiert werden, ist eine Einwilligung nach Art. 6 lit. a) DSGVO jedoch möglich. Bei Daten aus frei zugänglichen Quellen (v.a. soziale Netzwerke) sollte bei Analyse zu Werbezwecken das Interesse der betroffenen Person am Ausschluss der Verarbeitung gegenüber dem berechtigten Interesse des Verantwortlichen regelmäßig überwiegen [21], weshalb auch hier die Einwilligung nach Art. 6 lit. a) DSGVO vorzuziehen ist. Der Betroffene ist trotz der öffentlichen Verfügbarkeit nach Art. 14 DSGVO über die Verarbeitung seiner Daten zu informieren.

Werden bei der Datenanalyse Profile einzelner Personen (Profiling) erstellt und auf deren Grundlage Entscheidungen mit Wirkung gegenüber dem Betroffenen getroffen, gelten die strengeren Anforderungen des Art. 22 DSGVO. Insbesondere die Rechtfertigung aufgrund berechtigter Interessen ist dann ausgeschlossen. Darüber hinaus muss der Betroffene über die bei der Entscheidungsfindung eingesetzte Logik informiert werden, nicht jedoch über die konkrete Berechnungsformel. Des Weiteren sind stets die allgemeinen, datenschutzrechtlichen Anforderungen einzuhalten, etwa bei Auslagerung der Datenanalyse in die Cloud (vgl. III.3.c). Der dabei verwendete **Algorithmus** darf außerdem keine diskriminierende Wirkung haben, um Verstöße gegen das AGG (Allgemeines Gleichbehandlungsgesetz) zu verhindern.

TIPP:

Der Personenbezug von Daten sollte so früh wie möglich aufgehoben werden, etwa durch die unwiderrufliche Anonymisierung und Löschung der Rohdaten. Sollte das nicht möglich sein, ist jedenfalls auf die Erhebung nur tatsächlich benötigter personenbezogener Daten und möglichst frühzeitige Pseudonymisierung zu achten.

Achtung:
Bei personenbezogenen Daten ist die Löschpflicht nach Art. 17 DSGVO bei Wegfall der Notwendigkeit einer Verarbeitung zu beachten, soweit keine Aufbewahrungspflichten bestehen.

Auch hier stellt sich die Frage nach dem **Schutz dieser Daten.** Ein „Dateneigentum" ist nicht gesetzlich geregelt. Solange sich die Analyse nicht komplett selbständig in Gang setzt, kann die Person, die den Arbeitsprozess in Gang gesetzt hat, allerdings als Urheber der neu entstandenen Werke gelten, sofern diese urheberrechtsfähig sind. Im Übrigen können die Analyseergebnisse zusätzlichen Schutz nach dem GeschGehG erfahren, wenn eine entsprechende Sicherung durch technische und organisatorische Maßnahmen implementiert wird (vgl. III. 1. c).

WAS IST ZU TUN?

- [ ] Bei Datenerlangung aus öffentlichen Datenquellen die anwendbaren Lizenzbedingungen prüfen
- [ ] Bei Erwerb von Daten stets umfassende Nutzungsvereinbarung treffen, u.a. mit Recht auf Übertragung von Nutzungsrechten an Dritte bei Verkauf des Unternehmens
- [ ] Implementierung von Geheimnisschutz nach dem GeschGehG
- [ ] Diskriminierende Algorithmen oder Lerndaten vermeiden

WAS IST BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN ZU TUN?

- [ ] Einholung von Einwilligungen in Datenanalyse, soweit keine positive Interessenabwägung nach Art. 6 lit. f) DSGVO möglich ist
- [ ] Informierung der Betroffenen bei Erhebung aus Drittquellen
- [ ] Rohdaten löschen, Anonymisierung oder Pseudonymisierung
- [ ] Bei Profiling strengere Anforderungen des Art. 22 DSGVO beachten

3.3 Cloud Computing

A) TECHNISCHE ERLÄUTERUNG

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über das Internet. Die Dienste werden in Echtzeit über das Internet als Service bereitgestellt und die Abrechnung erfolgt nach Nutzen oder Volumen. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet u.a. die Infrastruktur (z.B. Rechenleistung, Speicherplatz), Plattformen und Software. Der Zugang erfolgt über das Internet. Der Begriff „Wolke" (engl. Cloud) meint, dass der eigentliche physische Standort der Infrastruktur dieser Leistungen für den Nutzer oft nicht erkennbar rückverfolgt werden kann, sondern die Ressourcen „wie aus den Wolken", abgerufen werden können. Die IT-Dienstleistungen werden in verschiedene Organisationsformen strukturiert, welche sich grundsätzlich voneinander unterscheiden. **IaaS** (Infrastructure as a Service) ist die unterste Ebene der Cloud-Modelle. In diesem Bereich wird vom Anwender virtuelle Hardware als Infrastruktur beim Cloud-Service-Provider gemietet und in die unternehmensinterne IT-Landschaft integriert. Klassische Beispiele sind Speicherplatz, Rechenleistung oder Netzwerkbandbreite. **PaaS** (Platform as a Service) ist die mittlere Ebene der Cloud-Modelle. In diesem Bereich werden bereits Vorgaben zur Infrastruktur sowie Programmiersprachen und Schnittstellen vordefiniert. Der Anwender hat keinen oder nur eingeschränkten Zugriff auf die Administration der Hardware. Im Kern wird vom Anbieter eine Computer-Plattform zur Verfügung gestellt, welche für die Entwicklung von Webanwendungen und kompletten Entwicklungsumgebungen genutzt wird. Es können beispielsweise SaaS-Lösungen entwickelt und auf der Plattform betrieben werden. **SaaS** (Software as a Service) ist die oberste Ebene der Cloud-Modelle. In diesem Bereich werden fertige Softwarelösungen in Form von Anwendungen für den Nutzer bereitgestellt. Die Bereitstellung erfolgt üblicherweise über einen beliebigen Web-Browser, kann aber auch über spezielle Programme zur Verfügung gestellt werden. Die Verantwortung für die Wartung, Software Updates und die Verwaltung von Lizenzen obliegt vollständig dem Provider. Der Anwender mietet lediglich ein komplettes Softwarepaket. Klassische Beispiele sind Office 365, Google Apps und iCloud Apps. [22]

TIPP:

Verträge mit Cloud-Providern sollten stets im Lichte der jeweiligen Vertragsform bewertet werden. Fällt der IT-Betrieb beim Cloud-Provider aus, so liegt auch schnell der eigene Geschäftsbetrieb am Boden. Lassen Sie sich daher vertraglich eine hohe Verfügbarkeit (mind. 99 % im Jahresdurchschnitt) sowie schnelle Reaktionszeit (2,0 Std. bei kritischen Mängeln innerhalb der Supportzeiten) zusichern.

TIPP:

Unternehmen sollten bestenfalls Cloud-Verträge mit deutschen oder EU-Providern schließen, die nach ISO 27001 zertifiziert sind. Bei Wahl eines US-Providers sollte darauf geachtet werden, dass a) nur EU-Server Verwendung finden (viele Provider haben eine „EU-Cloud-Option“) und b) sich der US-Provider dem EU-US-Privacy-Shield [27] unterworfen hat.

B) RECHTLICHE BEWERTUNG MIT CHECKLISTE

Das Cloud Computing wirft insbesondere in zwei Bereichen rechtliche Probleme auf. So ist einerseits im **Vertragsrecht** zu unterscheiden zwischen den einzelnen Leistungen der Cloud-Provider. Diese gewähren Zugriff auf Ihre IT-Infrastruktur und stellen hierfür Speicherplatz zur Verfügung (Mietvertrag). Andererseits sichern sie eine bestimmte Bandbreite sowie Rechenleistung zu, pflegen sowie aktualisieren Software und überwachen den laufenden IT-Betrieb (Dienstvertrag). Soweit einzelne Anpassungsleistungen geschuldet sind (Customizing) so sind diese schließlich im Einzelfall auch erfolgsabhängig (Werkvertrag).

Andererseits ist das Cloud Computing jedoch unter **datenschutzrechtlichen Gesichtspunkten** zu betrachten. Der Cloud-Provider ist im Regelfall als Auftragsverarbeiter nach Art. 28 DSGVO zu betrachten, was den gesonderten Abschluss eines entsprechenden Vertrages zur Auftragsverarbeitung in schriftlicher oder elektronischer Form (PDF) voraussetzt, der auch zumeist von den internationalen Cloud-Providern selbständig zur Verfügung gestellt wird. Hierin sollte bestenfalls zugesichert werden, dass sich die eingesetzten Webserver ausschließlich innerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR) befinden, so dass eine Datenverarbeitung in Drittstaaten ausscheidet. Denn ansonsten sind die zusätzlichen Vorgaben der Artikel 44 ff. DSGSVO zu beachten, was im Regelfall den Abschluss eines zusätzlichen Vertrages gemäß der EU-Standarddatenschutzklauseln [23] (Art. 46 II lit. c DSGVO) voraussetzt, soweit nicht von Seiten der EU-Kommission in dem betreffenden Drittstaat [24] ein angemes-

senes Datenschutzniveau festgestellt wurde [25]. Im Hinblick auf die Einhaltung IT-sicherheitsrechtlicher Vorgaben sollten die BSI-Vorgaben zum Mindeststandard bei Nutzung externer Cloud-Dienste berücksichtigt werden [26], die sich zwar an Bundesbehörden richten und vor dem Hintergrund der alten Rechtslage vor 2018 erstellt wurden, jedoch für Unternehmen einen guten Überblick zum Stand der Technik geben.

WAS IST ZU TUN?

- [ ] Berücksichtigen, dass ein Cloud-Vertrag regelmäßig unterschiedliche Vertragsformen vereint (Mietvertrag, Dienstvertrag, Werkvertrag), die auch unterschiedliche Rechtspflichten vorsehen
- [ ] Rohdaten löschen, Anonymisierung oder Pseudonymisierung
- [ ] Vereinbarung von hoher Verfügbarkeit der Systeme und kurzer Reaktions- und Wiederherstellungszeiten, hier kann der eigene IT-Dienstleister unterstützen
- [ ] Abschluss von gesondertem Vertrag zur Auftragsverarbeitung sowie bei Serverstandort ausserhalb der EU/EWR zusätzlich einem Vertrag auf Grundlage der EU-Standarddatenschutzklauseln (Art. 46 DSGVO)
- [ ] Sicherstellung, dass Cloud-Provider über eine angemessene Zertifizierung (z.B. ISO 27001) zur IT-Sicherheit verfügt

3.4 Mobile Endgeräte

A) TECHNISCHE ERLÄUTERUNG

Mobile Endgeräte sind Endgeräte, die hinsichtlich des Transports und der Handhabbarkeit komfortabel sind. Sie lassen sich aufgrund ihrer geometrischen Maße mobil einsetzen und tragen. Sie verfügen über Standardanwendungen wie Telefonie sowie weitere Datenkommunikationsdienste, wie beispielsweise Emails. Smartphones und Tablets sind mobile Endgeräte, deren Bedeutung sowohl in der privaten Nutzung als auch in beruflichen Einsatzbereichen in den letzten Jahren zugenommen hat. Im betrieblichen Einsatz ermöglichen mobile Endgeräte den Zugriff auf Unternehmensanwendungen und -dienste aus der Ferne. [28, p. 1 f.]

Durch die stark wachsende Anzahl an mobilen Endgeräten, die mit dem Internet verbunden sind, wird die Zahl dieser Geräte in einigen Jahren die Anzahl an mit dem Internet verbundenen Personalcomputer übertreffen. Dieser Trend erfordert eine Anpassung der Infrastruktur durch die Unternehmen, so dass auf Unternehmensanwendungen drahtlos zugegriffen werden kann. Die mobilen Endgeräte ermöglichen auch die Abwicklung von Geschäftsprozessen. [29, p. 397] Zu den Basistechnologien mobiler Endgeräte zählen Netzwerk-, Service- und Lokalisierungstechnologien. Das *Global System for Mobile Communication (GSM)* und Erweiterungen wie *EDGE* oder *GPRS* gilt als Standard für Mobilfunk und ist eine heutige zukünftige Netzwerktechnologie. Servicetechnologien ermöglichen im Allgemeinen eine zur Verfügungstellung von Diensten im Web über Mobilgeräten. Die Ortsbestimmung des Nutzers eines mobilen Endgeräts wird durch lokationsbasierte Dienste ermöglicht. Beispiel für einen solchen Dienst ist der satellitengestütze Dienst GPS, der allerdings einen im Endgerät integrierten Sender voraussetzt. [30, p. 398 f.]

B) RECHTLICHE BEWERTUNG MIT CHECKLISTE

Bei der Verwendung mobiler Endgeräte zu Unternehmenszwecken sind auf rechtlicher Ebene verschiedene Aspekte zu beachten. Die **vertragliche** Regelung der betrieblichen Nutzung kann durch Arbeitsvertrag, Betriebsvereinbarungen oder interne verbindliche Richtlinien erfolgen. Dabei ist zunächst zu entscheiden, ob mobile Endgeräte betrieblich gestellt werden („Choose your own device" – CYOD) oder die betriebliche Nutzung privater Endgeräte gestattet wird („Bring your own device" – BYOD). Wird die private Nutzung dienstlicher Geräte nicht ausdrücklich untersagt, besteht das Risiko, dass diese durch betriebliche Übung zulässig wird. In diesem Fall könnte der Arbeitgeber außerdem

als Anbieter von Telekommunikationsleistungen nach § 88 TKG dem Fernmeldegeheimnis unterliegen. [31]

Im Hinblick auf das **Arbeitsrecht** stellen sich – wie bei jeder Form des mobilen Arbeitens – Probleme hinsichtlich der Arbeitszeiterfassung sowie der Einhaltung von Ruhephasen. Da gemäß § 5 ArbZG zwischen zwei Phasen der Arbeit Ruhephasen einzuhalten sind, die nicht durch die Bearbeitung betrieblicher Nachrichten unterbrochen werden dürfen, darf die permanente Erreichbarkeit auch im Einvernehmen mit dem Arbeitnehmer nicht erwartet werden.

Weitere Probleme stellen sich auf **datenschutzrechtlicher Ebene.** Bei der Verarbeitung personenbezogener Daten durch mobile Endgeräte bleibt der Arbeitgeber Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO, den die Haftung für Datenschutzverstöße trifft. Dabei kommt es nicht darauf an, ob die Geräte betrieblich gestellt oder im Rahmen von BYOD genutzt werden. Der Arbeitgeber muss (jedenfalls wenn betriebliche Daten auf dem Gerät befugt verarbeitet werden) auch für diese Geräte und die Kommunikation mit Unternehmensservern angemessene Sicherheitsmaßnahmen gemäß Art. 32 DSGVO treffen und bei Bedarf nachweisen. Zu vermeiden ist die Installation von Whatsapp oder anderen Apps, die auf das Telefonbuch zugreifen und Kontaktdaten ohne Einwilligung des Betroffenen an US-Server von Facebook senden. [32]

Auch der Zugriff des Arbeitgebers auf private, auf dem Gerät gespeicherte Daten des Arbeitnehmers stellt eine erlaubnispflichtige Verarbeitung personenbezogener Daten dar. Da eine möglicherweise rechtfertigende Einwilligung jedoch den strengen

TIPP:

Um die Einhaltung datenschutzrechtlicher Anforderungen zu überprüfen, sollte sich der Unternehmer vertraglich Kontrollrechte und die jederzeitige Zugriffsmöglichkeit auf das mobile Endgerät vom Arbeitnehmer schriftlich zusichern lassen.

TIPP:

Um die Sicherheit von Unternehmensdaten zu gewährleisten und unzulässigen Zugriff auf Mitarbeiterdaten zu verhindern, sollten Mitarbeitern mobile Endgeräte zur ausschließlich betrieblichen Nutzung zur Verfügung gestellt oder alternativ eine „Container-Lösung" (wie z.B. MobileIron oder Good) verpflichtend eingeführt werden. Bei dieser werden alle Unternehmensdaten und -Anwendungen in einem abgeschotteten Bereich (Container) des Telefons gespeichert, auf den andere Anwendungen keinen Zugriff haben. Darüber hinaus sollte es eine Nutzungsvereinbarung geben, die etwa Meldepflichten für Datenpannen oder die regelmäßige Wartung durch die Unternehmens-IT unter Verbot der Wartung durch Drittunternehmen enthält.

Anforderungen des § 26 II BDSG unterliegt, sollte ein Zugriff auf private Arbeitnehmerdaten von vornherein verhindert werden. Die Überwachung des Arbeitnehmers per GPS oder Tracking- und Analysetools ist im Regelfall ebenfalls unzulässig, denn hier überwiegen die schutzwürdigen Interessen an einem Ausschluss der Verarbeitung [33]. Eine Ausnahme stellt etwa die Ortung zur Erfüllung rechtlicher Vorschriften dar. Eine Überwachung außerhalb der Arbeitszeit ist immer unzulässig und eine wirksame Einwilligung des Arbeitnehmers nicht möglich.

Bei der betrieblichen Nutzung mobiler Endgeräte hat außerdem der **Betriebsrat** (sofern vorhanden) ein Mitbestimmungsrecht gem. § 87 I Nr. 6 BetrVG, da es sich um eine Technologie handelt, die jedenfalls theoretisch dazu dienen könnte, das Verhalten oder die Leistung von Arbeitnehmern zu überwachen.

WAS IST ZU TUN?

- [ ] Entscheidung treffen zu BYOD oder CYOD
- [ ] Technische und organisatorische Maßnahmen nach Art. 32 DSGVO zum Schutz der Geräte und Kommunikation implementieren
- [ ] Nutzungsvereinbarung mit den Mitarbeitern treffen (z.B. zur Installation von Apps, zu Meldepflichten bei Datenpannen oder zur Regelung der Arbeitszeitvorschriften)
- [ ] Bestenfalls immer eine Container-Lösung einsetzen

3.5 IT-Security

A) TECHNISCHE ERLÄUTERUNG

Im Zuge der steigenden Bedeutung von Informations- und Kommunikationstechnologien in der zunehmend digitalisierten Wirtschaft erhält die IT-Security eine Schlüsselrolle. Ihr kommt dabei die Aufgabe zu, Unternehmen und deren Werte, wie Know-How und Kundendaten, zu schützen und gleichzeitig wirtschaftliche Schäden zu verhindern. Diese Schäden können beispielsweise durch Manipulationen oder Störungen der Verfügbarkeit von Diensten des Unternehmens entstehen. Eine vollständige Verhinderung von Angriffen ist in der Praxis nicht möglich, so dass IT-Security auch Maßnahmen und Konzepte zur Risikoreduktion beim Einsatz von Informations- und Kommunikationstechnologien umfasst. [34, p. 1] Die unternehmensinternen Informationen/Daten sind schützenswerte Güter, so dass es Ziel der IT-Security ist, datensichere Systeme zu gewährleisten. Zu diesem Zweck wurden Schutzziele, wie Informationsvertraulichkeit (confidentiality), Datentegrität (integrity) und Verfügbarkeit (availability) definiert, um den Zugriff auf die Daten zu kontrollieren bzw. zu beschränken. Informationsvertraulichkeit soll eine unautorisierte Informationsgewinnung verhindern. Dabei wird festgelegt, wer Kenntnis von welchen Informationen erlangen darf. Die Datenintegrität als Schutzziel soll gewährleisten, dass eine Manipulation der zu schützenden Daten unbefugt und unbemerkt nicht möglich ist. Dafür ist es notwendig festzulegen, wer das Recht hat bestimmte Daten zu nutzen. Beispielhaft für solche Zugriffsrechte sind die Verteilung von Lese- und Schreibberechtigungen für bestimmte Dateien zu nennen. Das System gewährleistet Verfügbarkeit, wenn es einem authentifizierten und autorisierten Subjekt auch den Zugriff ermöglicht und Ausfälle des Systems verhindert. [35, p. 8 ff.]

B) PRAXISBEISPIEL

Anfang 2019 wurde Airbus Opfer eines Cyberangriffs, der sich zwar nicht auf den Geschäftsbetrieb von Airbus ausgewirkt hat, aber den Zugriff auf personenbezogene Daten einiger Airbus Mitarbeiter in Europa ermöglichte. In einer Pressemitteilung erklärte Airbus, dass unverzüglich Maßnahmen zur Verbesserung der IT-Sicherheit eingeleitet würden [36]. Gegen Ende des dritten Quartals desselben Jahres wurde Airbus allerdings erneut Ziel eines Angriffs, bei dem Hacker versuchten über den Angriff auf die Systeme von Airbus Lieferanten zuzugreifen. Die Hacker versprachen sich durch den Angriff auf Lieferanten Zugriff auf Betriebsgeheimnisse von Airbus, die weniger stark geschützt sind [37].

TIPP:

Die Maßnahmen der DSGVO sind sehr allgemein gefasst, deshalb ist bei der technischen Umsetzung momentan die Orientierung an den BSI-Grundschutzkatalogen [38] zu empfehlen. Zum Einstieg eignet sich auch die Handreichung des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT). [39]

C) RECHTLICHE BEWERTUNG MIT CHECKLISTE

Im Zusammenhang mit der IT-Security geht es einerseits um den Schutz von verarbeiteten Kundendaten oder Daten von Geschäftspartnern und andererseits um den Schutz eigener Daten vor Zugriff von außen.

Im Hinblick auf unternehmensfremde Daten ist vor allem das **Datenschutzrecht** von Bedeutung. Für deren Schutz ist Art. 32 DSGVO maßgeblich, der keine konkreten Maßnahmen vorschreibt, jedoch einzelne geeignete Maßnahmen definiert wie Pseudonymisierung und Verschlüsselung, die Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme oder die Implementierung eines Verfahrens zur regelmäßigen Evaluierung der Maßnahmen. Die Schutzmaßnahmen müssen dem Schutzniveau der jeweiligen Daten angemessen sein und dem Stand der Technik entsprechen. Darüber hinaus sollten die Schutzmaßnahmen dokumentiert und ein Meldesystem für Datenschutzverstöße implementiert werden, um den Meldepflichten nach Art. 33, 34 DSGVO fristgerecht nachzukommen.

Werden die Sicherheitsvorgaben der DSGVO nicht eingehalten, besteht das Risiko von Schadensersatzansprüchen von Kunden und Vertragspartnern nach Art. 82 DSGVO. Dazu können die Datenschutzbehörden nach Art. 83 DSGVO Bußgelder in Höhe von bis zu 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes verhängen, bei Verstößen gegen Art. 32 DSGVO bis zu 10 Mio. Euro oder 2 %.

Besonderheiten ergeben sich für **Betreiber kritischer Infrastrukturen,** die von wichtiger Bedeutung für das staatliche Gemeinwesen sind. Solche müs-

sen seit Inkrafttreten des IT-Sicherheitsgesetzes im Juli 2015 gemäß § 8a BSI-Gesetz (BSIG) u.a. besondere organisatorische und technische Vorkehrungen einrichten und strengere Registrierungs- und Meldepflichten beachten.

Auch im Hinblick auf **eigene Daten und Know-How** sollten Sicherheitsmaßnahmen umgesetzt werden. Diese können auf den Sicherheitsmaßnahmen im Zusammenhang mit dem Datenschutz aufbauen. Gemäß § 2 Nr. 1 lit. a GeschGehG sind nur solche Informationen geschützt, für die „angemessene Geheimhaltungsmaßnahmen" getroffen wurden. Auch wenn kein Umsetzungszwang besteht, haben Unternehmen bei Rechtsverletzungen nur dann Auskunfts-, Unterlassungs- oder Schadenersatzansprüche etc., wenn Informationen als Geschäftsgeheimnis erkennbar sind und durch ihrem Schutzstatus entsprechende Maßnahmen geschützt werden. Die Konkretisierung dieser Maßnahmen durch die Rechtsprechung steht jedoch noch aus.

Auch aus **Compliance-Vorgaben** ergeben sich IT-sicherheitsrechtliche Anforderungen. Gemäß § 91 AktG ist in Aktiengesellschaften und analog in großen GmbH ein Überwachungssystem zur Früherkennung von Gefahren für das Unternehmen einzurichten, das auch angemessene Maßnahmen zur IT-Sicherheit umfasst. Wird dieser Pflicht nicht nachgekommen, haften die betreffenden Vorstandsmitglieder gegenüber der Gesellschaft persönlich. Sonderregeln gibt es außerdem für Kredit- und Finanzdienstleistungsunternehmen (§ 25a KWG), im Bereich der Telekommunikation (§ 109 TKG) und für die Versicherungsbranche (§ 29 VAG).

TIPP:

Informationen sollten ihrem Schutzstatus entsprechend kategorisiert werden. Sinnvoll ist die Kategorisierung nach dem potentiellen wirtschaftlichen Schaden bei Bekanntwerden. Darüber hinaus sollten sie (1) vertraglich, etwa durch konkrete Vereinbarungen mit Arbeitnehmern oder Vertraulichkeitsvereinbarungen mit Geschäftspartnern, (2) technisch, etwa durch Zutrittskontrollen, beschränkte Zugriffsrechte und Sicherheitsupdates, sowie (3) organisatorisch, etwa durch regelmäßige Erstellung eines Gefährdungsberichts, abgesichert werden. Alle Maßnahmen sollten regelmäßig aktualisiert und dokumentiert werden.

TIPP:

Zur Überprüfung von IT-Maßnahmen eignen sich die bankaufsichtlichen Anforderungen an die IT der BaFin (BAIT) [40] auch für Unternehmen ohne Bezug zum Kreditwesen.

Haftungsrisiken aufgrund mangelnder IT-Security bestehen gemäß §§ 280 I, 241 II BGB bei Verlust bzw. Diebstahl der Daten von Vertragspartnern aufgrund unzureichender IT-Sicherheitsmaßnahmen oder gemäß §§ 280 I, II, 286 BGB, wenn sich durch Pannen Betriebsabläufe verzögern.

WAS IST ZU TUN?

- [ ] Kategorisierung von Daten anhand ihres Schutzbedürfnisses
- [ ] Umsetzung der Vorgaben des Art. 32 DSGVO, bestenfalls nach BSI Grundschutz
- [ ] Zusätzlich: Kennzeichnung und Schutz von Geschäftsgeheimnissen
- [ ] Dokumentation von Schutzmaßnahmen
- [ ] Konzept zum Umgang mit Datenpannen erstellen

3.6 Künstliche Intelligenz

A) TECHNISCHE ERLÄUTERUNG

Unter Künstlicher Intelligenz (KI oder eng. Artificial Intelligence, AI) versteht man „Systeme, die intelligentes Verhalten zeigen, indem sie ihre Umgebung analysieren und – mit einem gewissen Grad an Autonomie – Maßnahmen ergreifen, um bestimmte Ziele zu erreichen. KI-basierte Systeme können rein softwarebasiert sein, in der virtuellen Welt agieren (z.B. Sprachassistenten, Bildanalysesoftware, Suchmaschinen, Sprach- und Gesichtserkennungssysteme) oder KI kann in Hardwaregeräte eingebettet sein (z.B. fortgeschrittene Roboter, autonome Fahrzeuge, Drohnen oder Internet of Things-Anwendungen).“ [41, p. 3]. Um dies zu erreichen, werden menschliche Fähigkeiten mit Algorithmen nachempfunden. Das breite Feld der Künstlichen Intelligenz gliedert sich daher in verschiedene Bereiche, die anhand dieser Fähigkeiten strukturiert werden können.

- maschinelle Verarbeitung natürlicher Sprache (eng. Natural Language Processing NLP) zur Kommunikation mit Menschen
- Wissensrepräsentation, zur Speicherung des erworbenen Wissens

- Logisches Denken, um das Wissen zur Beweisführung und Beantwortung von Fragen zu nutzen
- Machinelles Lernen, um adaptiv zu handeln und Muster zu erkennen
- Sehvermögen um Objekte wahrzunehmen
- Robotik, um mit Objekten zu interagieren [42, p. 2 f.]

Maschinelles Lernen beinhaltet eine Vielzahl der aktuellen Anwendungsfälle im Bereich der Künstlichen Intelligenz. Hierbei wird Deep Learning (tiefes Lernen) genutzt, eine vom menschlichen Gehirn inspirierte technische Umsetzung hintereinander geschalteter, neuronaler Netze.

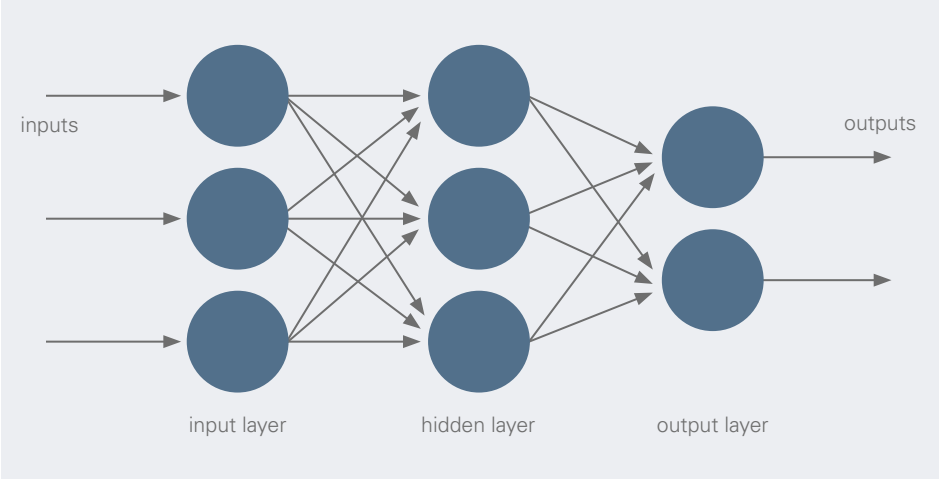


Abbildung 3: Beispielhaftes neuronales Netz mit drei Eingangswerten, einer versteckten Schicht (layer) und zwei Ausgangswerten

Diese Netze beinhalten Tausende von „Neuronen" und mehrere versteckte (hidden) Schichten dieser Neuronen. Die in das Netz eingegebenen Daten werden von den Neuronen verarbeitet und es wird am Ende ein oder mehrere Outputs generiert. Durch die Komplexität des Netzes kann hierbei nicht immer begründet werden, warum eine gewisse Entscheidung im Einzelfall getroffen wurde, was Komplikationen aus bspw. rechtlicher oder entscheidungstechnischer Sicht nach sich ziehen kann. [43, p. 411]

B) PRAXISBEISPIEL

Im Rahmen einer Digitalisierungsinitiative treibt das deutsche Chemieunternehmen Lanxess AG seit Anfang 2017 die Einführung neuer Technologien entlang der Wertschöpfungskette sowie den Aufbau und die Nutzung von Big Data voran. Laut einer Pressemitteilung des Unternehmens im Oktober 2019 setzt Lanxess im Bereich der Produktentwicklung nun auf künstliche Intelligenz, um die Entwicklung neuer und individueller Rezepturen zu beschleunigen und das Produktangebot zu erweitern. In Kooperation mit dem Big Data Plattform-Betreiber Citrine Informatics hat Lanxess nun einen Algorithmus entwickelt, der auf bestehende Messdaten zurückgreift und diese mit Expertenwissen verknüpft, um die Entwicklung optimaler Rezepturen sowie die Befriedigung kundenspezifischer Anforderungen an Produkteigenschaften zu unterstützen [44].

TIPP:

Werden bei dem Einsatz von KI personenbezogene Daten verarbeitet und findet eine automatisierte Entscheidungsfindung statt, sollte immer die informierte, ausdrückliche Einwilligung des Betroffenen eingeholt werden, wenn die Verarbeitung nicht schon zur Erreichung des Vertragszwecks erforderlich ist. Werden Daten von Mitarbeitern im Beschäftigungskontext verarbeitet, wird die wirksame Einwilligung durch § 26 II BDSG zusätzlich erschwert.

C) RECHTLICHE BEWERTUNG MIT CHECKLISTE

Im Bereich der künstlichen Intelligenz („KI") ist die Rechtslage gerade hinsichtlich immer autonomer agierender Systeme noch im Wandel. Doch bereits heute ist etwa im Hinblick auf das **Datenschutzrecht** zu beachten, dass eine Künstliche Intelligenz zunächst eine große Menge an Lerndaten verarbeiten muss. Sind dies personenbezogene Daten, kommen für eine Rechtfertigung nach Art. 6 Abs. 1 DSGVO in der Regel nur die Einwilligung der betroffenen Personen oder berechtigte Interessen des Unternehmens in Betracht.

Wird KI tatsächlich eingesetzt, handelt es sich häufig um eine automatisierte Entscheidungsfindung im Sinne von Art. 22 DSGVO, für die die Rechtfertigungs-

gründe deutlich enger gefasst sind. Die Verarbeitung muss entweder zur Vertragserfüllung mit dem Betroffenen erforderlich oder aufgrund einer Rechtsvorschrift zulässig sein oder mit Einwilligung erfolgen. Die Rechtfertigung aufgrund berechtigter Interessen fällt weg.

Daneben gelten auch beim Einsatz von KI allgemeine datenschutzrechtliche Anforderungen, etwa bei der Verwendung von Cloud Computing oder dem Einsatz von Auftragsverarbeitern [45]. Die Konferenz der deutschen Datenschutzbehörden (DSK) hat im April 2019 eine Erklärung [46] zur Künstlichen Intelligenz abgegeben. Hiernach ist der Einsatz grundsätzlich erlaubt, solange die Grundsätze der Rechtmäßigkeit, Zurechenbarkeit, Transparenz, Fairness und Datenminimierung eingehalten werden sowie die Verarbeitung nur im Rahmen der Zweckbindung erfolgt und keine Diskriminierung stattfindet. Nach Ansicht der Behörden ist im Regelfall die Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlich und die notwendigen, technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO sind zu treffen, beispielsweise Pseudonymisierung, besser noch Anonymisierung.

Wird KI in kreativen Prozessen eingesetzt und so neue Arbeitsergebnisse erreicht, ist es aus urheberrechtlicher Sicht wichtig, dass die ausschließlichen Nutzungsrechte an den Ergebnissen erworben werden, was ggf. durch Vereinbarungen zu lösen wäre. Noch wird KI zum Großteil als Werkzeug des menschlichen Geistes eingesetzt und die Person, die den Arbeitsprozess verursacht hat, gilt als Urheber am Ergebnis. Ausschließlich von einer KI geschaffene Werke sind als bloßes Ergebnis mathematischer Operationen allerdings nicht urheberrechtsfähig (vgl. III.2.c).

TIPP:

Schutz an durch KI generierten Ergebnissen bieten momentan wohl in erster Linie das GeschGehG für Geschäftsgeheimnisse und der wettbewerbliche Leistungsschutz nach § 4 Nr. 3 UWG als Auffangtatbestand. Um Schutz nach dem GeschGehG zu erhalten, müssen für die Daten besondere Schutzmaßnahmen getroffen werden, die sie als Geschäftsgeheimnisse erkennbar machen (vgl. III.5.c).

TIPP:

Da die Produzentenhaftung im Einzelfall unterschiedlich bewertet werden kann und ansonsten der Grundsatz der Betreiberhaftung gilt, sollte schon in Verträgen mit KI-Anbietern eine klare Risikozuweisung erfolgen.

TIPP:

Auch Hersteller einer durch fremdprogrammierte KI gesteuerten Sache, sollten Regressansprüche mit dem Anbieter der KI vertraglich vereinbaren.

Im Hinblick auf die **Haftung** ist für durch KI-Software verursachte Schäden im Grundsatz ihr Verwender verantwortlich. Es kann jedoch die Produzentenhaftung nach § 823 I BGB greifen, wenn der Hersteller der KI vorsätzlich oder fahrlässig gehandelt hat.

Treten auf Seiten von Verbrauchern Schäden auf, die durch KI-basierte Produkte entstanden sind, so haftet nur der Hersteller dieser Sache verschuldensunabhängig nach dem ProdHaftG.

Verwender von KI sollten außerdem beachten, dass **Vertragsschlüsse** oder rechtlich bedeutsame Handlungen künstlicher Intelligenzen entsprechend den Grundsätzen zu Computerprogrammen für sie rechtlich bindend sind, da KI nach geltendem Recht weder rechts- oder geschäftsfähig ist und es ihr an der für eine Willenserklärung erforderlichen subjektiven Komponente mangelt.

WAS IST ZU TUN?

- [ ] Einwilligung betroffener Personen nach Art. 6 Abs. 1 DSGVO einholen, soweit eine automatisierte Entscheidungsfindung stattfindet
- [ ] In Verträgen mit KI-Anbietern klare Risikozuweisungen und Haftungsregelungen regeln
- [ ] Diskriminierende Algorithmen oder Lerndaten vermeiden, da Gefahr von Verstößen gegen das AGG
- [ ] Hambacher Erklärung der deutschen Datenschutzbehörden beachten
- [ ] Geheimnisschutz implementieren

3.7 Blockchain

A) TECHNISCHE ERLÄUTERUNG

Eine Blockchain (dt. Blockkette) ist betriebswirtschaftlich vergleichbar mit einem elektronischen Kassen- oder Hauptbuch. Allerdings gibt es von diesem Buch eine Vielzahl verteilter Kopien. Technisch handelt sich also um eine dezentrale Transaktions-Datenbank (DLT – Distributed Ledger Technology), die in einem (Peer-to-Peer-)Netzwerk auf einer Vielzahl von Rechnern (Knoten) in exakt identischer, d. h. gespiegelter Form vorliegt. Der Datenbestand in Form der Blockchain besteht aus einer linearen Aneinanderreihung von Kettengliedern bzw. Blöcken, die zeitlich nacheinander und logisch konsistent aufeinander aufbauen. Jeder Block beinhaltet neben den eigentlichen Transaktionsdaten u. a. einen Zeitstempel und einen mit kryptographischen Methoden errechneten Kontroll- bzw. Hashwert dieses Blocks sowie des vorangegangenen Blocks (vergleichbar einer Quersumme). Mithilfe dieser ist jede Transaktion verifiziert bzw. unterschrieben.

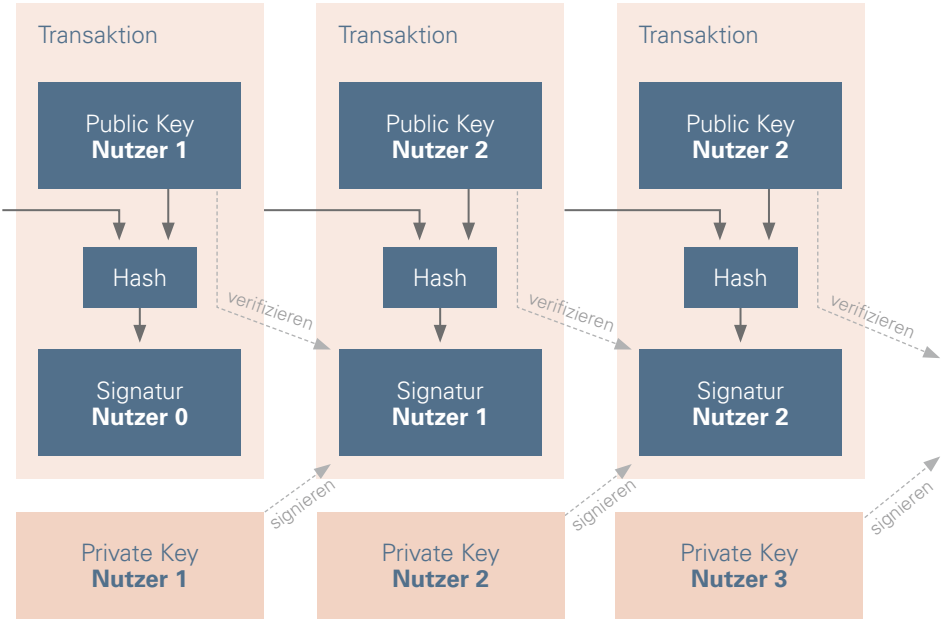


Abbildung 4: Beispielhafte Darstellung der Blockchain

Bei einer nachträglichen Löschung oder Veränderung der Informationen in einem Block passt der jeweilige Hashwert nicht mehr zu dem Block. Da die Blöcke aufeinander aufbauen, würde der nächste Block nicht mehr konsistent zu seinem Vorgänger sein. Dabei existiert keine zentrale Kontrollstelle mehr. Eine solche Manipulation würde in dem Netzwerk zwischen Rechnern, auf denen die Blockchain ja mehrfach in identischer Form vorliegt und in dem die Transaktionen „gemeinsam" verifiziert, validiert und neue Blöcke geschaffen werden, nahezu in Echtzeit auffallen. Die Daten, die sich einmal in der Blockchain befinden, können somit nicht mehr verändert oder gelöscht werden. Alle Beteiligten können die Transaktionen in der Blockchain sehen, aber niemand kann sie manipulieren.

Das Thema Blockchain ist mehr als ein Hype. Es hat Potenzial und beschäftigt immer mehr Unternehmen aus verschiedensten Branchen. Die Blockchain kann Vorteile bieten wie höhere Transparenz in den Prozessen, Manipulationssicherheit und Senkung der Transaktionskosten – ein prominentes Beispiel sind Kryptowährungen. Dem stehen aber

mögliche Nachteile und Limitationen entgegen, insbesondere die Ineffizienz der verteilten IT-Lösung mit Defiziten in der Skalierbarkeit des Systems, hohem Stromverbrauch und aufsichtsrechtlichen Hürden. [22]

B) RECHTLICHE BEWERTUNG MIT CHECKLISTE

Auch die Blockchain wirft viele, rechtlich nicht abschließend geklärte Probleme auf. So steht das Prinzip der Blockchain, insbesondere im Hinblick auf Smart Contracts, mit einigen Grundsätzen des **allgemeinen Zivilrechts** im Konflikt: Die anfängliche Nichtigkeit einer Transaktion, bspw. durch Anfechtung (§ 142 BGB), Verstoß gegen gesetzliche Verbote (§ 134 BGB) oder Sittenwidrigkeit (§ 138 BGB), etwa ist kaum darstellbar, da es zum Wesen der Blockchain gehört, nachträglich unabänderbar zu sein. Ähnliche Probleme stellen sich, wenn der **Smart Contract** nicht das von den Vertragsparteien Gewollte abbildet, etwa bei der Durchführung eines Rücktritts oder Geltendmachung von Gewährleistungsrechten. Im Übrigen ist auf die abgebildeten Verträge jedoch allgemeines Zivilrecht anwendbar.

TIPP:

Erfolgen Transaktionen über eine Blockchain bzw. Smart Contracts, sollte stets eine Methode zur Rückabwicklung nichtiger Transaktionen und darauf aufbauender, ebenfalls „falscher" Folgetransaktionen enthalten sein. Das Gleiche gilt für die Durchführung von Gewährleistungsansprüchen.

Im Hinblick auf das **Datenschutzrecht** sind bei Verwendung von Blockchains die Anforderungen der DSGVO zu beachten. Dabei ist zwischen öffentlicher (z.B. bei Kryptowährungen) und privater Blockchain zu unterscheiden. Bei letzterer, die meist bei internen Blockchain-Systemen zur Anwendung kommt, kann der für die DSGVO erforderliche Personenbezug regelmäßig schon durch Vergabe von Nutzerkennungen hergestellt werden, weshalb die entsprechende Stelle dann auch datenschutzrechtlich verantwortlich ist. Auch auf öffentliche Blockchains ist Datenschutzrecht anwendbar, da Transaktionen trotz der dort vorgenommenen Pseudonymisierung rückverfolgbar sein können. Schwieriger ist hier die Frage nach der Verantwortlichkeit: Nach heutigem Stand könnte je nach Art der konkreten Blockchain jeder Teilnehmer der Blockchain oder jeder Absender einer Transaktion, jedenfalls aber die sog. Nodes (Betreiber einzelner Netzwerkknoten) datenschutzrechtlich Verantwortlicher sein.

Die Rechtmäßigkeit der Datenverarbeitung stützt sich bei der Blockchain in der Regel auf das berechtigte Interesse der verantwortlichen Stelle nach Art. 6 lit. f) DSGVO, da eine Einwilligung nach Art. 6 lit. a) DSGVO häufig daran scheitert, dass eine Information des Betroffenen über alle Umstände der Datenverarbeitung aufgrund deren dezentraler Durchführung kaum möglich ist. Allerdings bleibt das Risiko, dass die bei der Blockchain unvermeidliche dauerhafte Speicherung der Daten einem berechtigten Interesse an der Verarbeitung entgegenstehen kann. Bei der privaten Blockchain kann die Verarbeitung auch zur Erfüllung eines Vertrages über die Nutzung der Blockchain gerechtfertigt sein. Problematisch ist

TIPP:

Betroffene müssen in der Datenschutzerklärung des Blockchain-Systems genau über die mangelhafte Umsetzung aller Betroffenenrechte informiert werden.

wegen der Unabänderlichkeit der Blockchain auch die Umsetzung von Betroffenenrechten, insbesondere auf Löschung und Vergessenwerden (Art. 17 DSGVO) und auf Berichtigung (Art. 16 DSGVO).

Nach momentaner Rechtslage ist der datenschutzkonforme Einsatz von Blockchains kaum möglich. Der Tätigkeitsbericht 2018 der Landesbeauftragten Bremen [47] enthält daher die Aussage, dass *„insbesondere Artikel 16 (Recht auf Berichtigung) und Artikel 17 (Recht auf Löschen) DSGVO sich nur schwer mit den Grundsätzen der Integrität und Vertraulichkeit der Blockchain in Einklang bringen lassen".* Auch wenn es zu Rechtsfortbildung oder Entwicklung von Zertifikaten oder *Codes of Conduct* in diesem Bereich kommen wird [48], sollte stets eine umfassende Abwägung der mit dem Einsatz von Blockchain

TIPP:

Aufgrund der Komplexität in diesem Bereich, sollte bei der Entwicklung neuer Blockchain basierter Geschäftsmodelle immer eine umfassende juristische Prüfung vorgenommen werden.

verbundenen Risiken stattfinden und möglichst wenige personenbezogene Daten in der Blockchain gespeichert werden. Der Einsatz privater Blockchains, in denen nur berechtigte Personen Zugriff auf die im System vorhandenen Informationen erhalten, ist vorzuziehen.

Daneben gibt es im Einzelfall weitere **rechtliche Risiken:** Bitcoin etwa werden von der BaFin und vom Bundesfinanzministerium als „Rechnungseinheit", also als Finanzinstrument nach § 1 XI Nr. 7 KWG qualifiziert. [49] Deshalb ist für gewerbliches Mining, Kaufen und Verkaufen von Bitcoin regelmäßig die Erlaubnis der BaFin erforderlich. Werden Blockchain-Technologien bspw. von Banken, Versicherungen oder Energieversorgern verwendet, können diese als kritische Infrastrukturen im Sinne von § 2 X BSIG besonderen Sicherungspflichten unterliegen.

WAS IST ZU TUN?

- [ ] Bei Smart Contracts nur solche Blockchains einsetzen, die Mittel zur Rückabwicklung nichtiger Transaktionen vorsehen
- [ ] Bestenfalls nur anonymisierte Daten einsetzen, hilfsweise pseudonymisierte.
- [ ] Bei Einsatz personenbezogener Daten innerhalb der Datenschutzerklärung über die unvollständige Durchsetzung von Betroffenenrechten informieren (Risiko der Beanstandung durch Behörden)
- [ ] Risikoabwägung zum Datenschutz vornehmen und dokumentieren
- [ ] Entwicklung der Rechtslage beobachten, insbesondere zu den Veröffentlichungen des EPRS (European Parliamentary Research Service)

VIER

HANDLUNGSEMPFEHLUNGEN UND FAZIT

Betrachtet man die hier vorgestellten Technologien, zeigt sich, dass der rechtskonforme Einsatz in fast allen Fällen auch heute schon möglich ist. Schwierigkeiten zeigen sich dabei meistens im Bereich des Datenschutzes. Dabei muss dieser Thematik keinesfalls skeptisch begegnet werden. Ein Großteil der momentan vorhandenen Unsicherheiten beruht nämlich nicht darauf, dass der Einsatz innovativer Technologien grundsätzlich unzulässig ist. Das Problem liegt vielmehr darin, dass vieles im Datenschutz bewusst offen gelassen wurde. Grund dafür ist das Bewusstsein des Gesetzgebers, dass Entwicklungen wie die wachsende Relevanz von Blockchains oder im Bereich der Künstlichen Intelligenz vor wenigen Jahren noch nicht in vollem Umfang abzusehen waren und Gesetze wie die DSGVO sollen in der Lage sein, darauf zu reagieren. Selbst im Hinblick auf das Thema Blockchain, das rechtlich momentan die größten Schwierigkeiten zu verursachen scheint, hat das Europäische Parlament in einer erst im Juli 2019 erschienen Studie klargestellt, dass die Verwendung von Blockchains trotz allem nicht per se unzulässig sein soll. Stattdessen seien der Gesetzgeber, die Wissenschaft und nationale sowie internationale Institutionen und Behörden in der Pflicht, neue Handlungsanweisungen, Zertifikate oder *Codes of Conduct* zu entwickeln. Ein grundsätzliches Verbot des Einsatzes solcher Technologien ist demnach gerade nicht bezweckt.

Man sollte also nicht davor zurückschrecken, den Einsatz von Internet of Things, Data Analytics etc. zu erproben und so den eigenen Handlungsspielraum zu erweitern. Andere Themen, wie die Verwendung mobiler Endgeräte oder der Einsatz von Cloud Computing, sind schon heute in vielen Unternehmen kaum mehr wegzudenken. Wer sich früh mit den Anforderungen auseinandersetzt, die diese Innovationen mit sich bringen, ist in der Lage, auch langfristig mit dem Fortschritt mitzuhalten.

Trotzdem ist zu beachten, dass fast alle hier vorgestellten Technologien in der Regel sehr datenintensiv sind. Das führt nicht nur zu Problemen im Bereich des Datenschutzes – auch sensible Unternehmensdaten sollten vor unberechtigtem und externem Zugriff geschützt werden. Deshalb sollte Basis für die Implementierung neuer datenbasierter Technologien zunächst die sorgfältige Organisation und Anpassung auf Ebene der IT-Security sein. Teilweise – etwa bei der KI – kommt dazu, dass deren technische Entwicklung immer noch am Anfang steht und es ist nicht klar, ob unser Recht auch in Zukunft „mithalten" kann.

Die wichtigsten Maßnahmen dürften neben der ganz allgemein datenschutzkonformen Organisation des Unternehmens die Überprüfung der datenschutzrechtlichen Rechtmäßigkeit aller Verarbeitungen personenbezogener Daten, die Überprüfung der internen IT-Security und die Erstellung eines Sicherungskonzeptes für die eigenen Daten sein. Letzteres sollte sowohl den Anforderungen von DSGVO und BDSG als auch denen des GeschGehG genügen. Da außerdem immer mehr Leistungen außerhalb der internen (digitalen) Infrastruktur ausgeführt werden, sollten Verträge mit externen Betreibern und Dienstleistern regelmäßig sorgfältig geprüft und gegebenenfalls ergänzt werden.

Letztendlich wird es in allen Bereichen der Digitalisierung erforderlich sein, die aktuellen Entwicklungen der Rechtsetzung und Rechtsprechung zu beobachten, die auch in Zukunft hoffentlich mit Fortschritt und Innovation Schritt hält. Daneben gilt es, sich stets eine gewisse Flexibilität zu bewahren und vor Einführung jeder neuen Technologie abzuwägen, ob diese umsetzbar ist und sich für das Unternehmen lohnt.

FÜNF

LITERATUR

[1] KfW-Digitalisierungsbericht Mittelstand 2018, https://t1p.de/grsp

[2] Umfrage der Funkschau aus 2017, zusammen mit dem Bundesverband mittelständische Wirtschaft, https://t1p.de/yacv.

[3] Zum Begriff siehe Roßnagel, Kein „Verbotsprinzip“ und kein „Verbot mit Erlaubnisvorbehalt“ im Datenschutzrecht, NJW 2019, 1.

[4] Das Bundesdatenschutzgesetz ergänzt auf nationaler Ebene die DSGVO.

[5] Die Alternativen stehen in Artikel 6 Absatz 1 Satz 1 lit. a) bis f) DSGVO. Nachfolgend werden jedoch Verweise dieser Vorschrift abgekürzt, etwa durch Art. 6 lit. f) DSGVO.

[6] Siehe hierzu Art. 5 Abs. 2 DSGVO.

[7] Jakob, Sabine, Dr. Axel T. Schulte, Dominik Sparer, Roman Koller, and Prof. Dr. Michael Henke. Blockchain und Smart Contracts: Effiziente und sichere Wertschöpfungsnetzwerke, 7.

[8] Bauernhansl, Thomas, Michael ten Hompel, and Birgit Vogel-Heuser. Industrie 4.0 in Produktion, Automatisierung und Logistik. Wiesbaden: Springer Fachmedien Wiesbaden, 2014, 15f.

[9] ten Hompel, Michael, and Sören Kerner. Logistik 4.0: Die Vision vom Internet der autonomen Dinge. In: Informatik-Spektrum, vol. 38, no. 3, pp. 176–182,

[10] https://doi.org/10.1007/s00287-015-0876-y, 2015, 177.

https://www.golem.de/news/internet-of-things-fehler-in-geschirrspueler-ermoeglicht-zugriff-auf-webserver-1703-126953.html

[11] https://press.avast.com/de-de/studie-von-avast-enth%C3%BCllt-hunderttausende-von-iot-ger%C3%A4ten-in-deutschland-%C3%B6sterreich-und-der-schweiz-sind-unsicher

[12] Heise.de: Massiver DDOS-Angriff auf Wikipedia, https://t1p.de/htdq.

[13] Siehe hierzu unten: Kapitel III Ziffer 5.

[14] Sedkaoui, Soraya. Data Analytics and Big Data: Understand Data and Take to Analytics Applications and Methods. Newark: John Wiley & Sons, Incorporated, 2018, 44

[15] Sedkaoui, Soraya. Data Analytics and Big Data: Understand Data and Take to Analytics Applications and Methods. Newark: John Wiley & Sons, Incorporated, 2018, 47

[16] Sedkaoui, Soraya. Data Analytics and Big Data: Understand Data and Take to Analytics Applications and Methods. Newark: John Wiley & Sons, Incorporated, 2018, 84

[17] Sedkaoui, Soraya. Data Analytics and Big Data: Understand Data and Take to Analytics Applications and Methods. Newark: John Wiley & Sons, Incorporated, 2018, 85

[18] Sedkaoui, Soraya. Data Analytics and Big Data: Understand Data and Take to Analytics Applications and Methods. Newark: John Wiley & Sons, Incorporated, 2018, 86 f.

[19] https://www.dw.com/de/facebook-datenskandal-was-bisher-geschah/a-43322775

[20] https://www.sueddeutsche.de/digital/eil-cambridge-analytica-reicht-insolvenz-ein-1.3965523

[21] DSK – Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung S. 5, November 2018, https://t1p.de/0caz.

[22] Handelskammer Hamburg – Digitalisierungsportal

[23] Die EU-Standardvertragsklauseln werden derzeit vom Europäischen Gerichtshof überprüft, https://t1p.de/p160.

[24] Ein solches wurde bereits für die Länder Andorra, Argentinen, Kanada, Faröer Inseln, Guernsey, Israel, Isle of Man, Japan, Jersey, Neuseeland, Schweiz, Uruguay festgestellt (Stand Juli 2019), siehe https://t1p.de/5t4v.

[25] Im Hinblick auf Unternehmen mit Sitz in den USA ist hier das sog. EU-US-Privacy-Shield zu beachten, welches als Vereinbarung zwischen der EU-Kommission und dem US-Handelsministerium für US-Unternehmen die Möglichkeit bietet, sich den EU-Datenschutzregeln zu unterwerfen und damit ein angemessenes Datenschutzniveau herzustellen; siehe hierzu Molnar-Gabor/Kaffenberger: EU-US-Privacy-Shield – Bedeutung des Angemessenheitsbeschlusses der EU-Kommission, ZD 2018, 162.

[26] https://t1p.de/fewv.

[27] Auch dieses Abkommen steht derzeit unter gerichtlicher Prüfung durch den Europäischen Gerichtshof, https://t1p.de/8yuh.

[28] Herzig, Markus. Basistechnologien und Standards des Mobile Business. In: Wirtschaftsinformatik, vol. 43, no. 4, pp. 397–406, 2001, 1 f.

[29] Disterer, George, and Carsten Kleiner. Mobile Endgeräte im Unternehmen: Technische Ansätze, Compliance-Anforderungen, Management. Wiesbaden: Springer Vieweg, 2014, 397

[30] Disterer, George, and Carsten Kleiner. Mobile Endgeräte im Unternehmen: Technische Ansätze, Compliance-Anforderungen, Management. Wiesbaden: Springer Vieweg, 2014, 398 f.

[31] Dies wurde in einigen Urteilen bejaht, die Frage wurde jedoch noch nicht höchstrichterlich beantwortet.

[32] So etwa der Landesdatenschutzbeauftragte Niedersachsen, https://t1p.de/72b4.

[33] Was sich auch in Art. 88 II DSGVO wiederspiegelt („Überwachungssysteme am Arbeitsplatz“).

[34] Eckert, Claudia. IT-Sicherheit. Berlin, Boston: De Gruyter, 2018, 1

[35] Eckert, Claudia. IT-Sicherheit. Berlin, Boston: De Gruyter, 2018, 8 ff.

[36] https://www.airbus.com/newsroom/press-releases/en/2019/01/airbus-statement-on-cyber-incident.html

[37] https://www.infosecurity-magazine.com/news/airbus-suppliers-hit-in/

[38] Im Februar 2019 überarbeitet, https://t1p.de/4a7r.

[39] Handreichung des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT), https://t1p.de/9tv1.

[40] Rundschreiben 10/2017 (BA) – BAIT, https://t1p.de/9x9t.

[41] Plattform Industrie 4.0 Ergebnispapier „Künstliche Intelligenz und Recht im Kontext von Industrie 4.0", 3

[42] Russell, Stuart J., and Peter Norvig. Artificial intelligence: a modern approach. Malaysia; Pearson Education Limited, 2016, 2 f.

[43] Witten, Ian H., Eibe Frank, Mark A. Hall, and Christopher J. Pal. Data Mining: Practical machine learning tools and techniques. Morgan Kaufmann, 2017, 411.

[44] https://lanxess.de/fileadmin/user_upload/2019-00086.pdf

[45] Siehe hierzu Kapitel III 3.

[46] Hambacher Erklärung, https://t1p.de/o2gy.

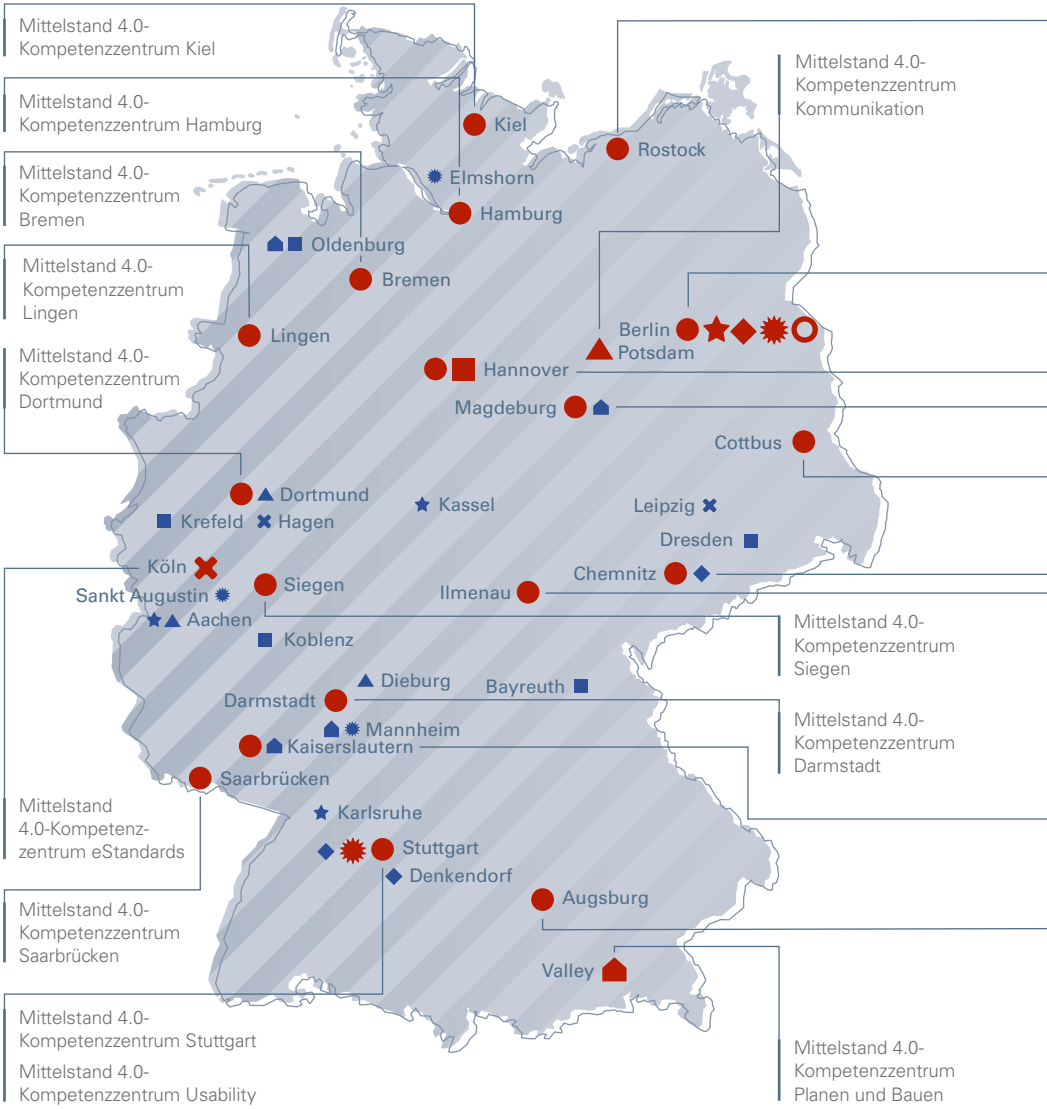
[47] 1. Jahresbericht der Landesbeauftragten für Datenschutz der Freien und Hansestadt Bremen nach der Europäischen Datenschutzgrundverordnung, 22, https://t1p.de/fn6e.

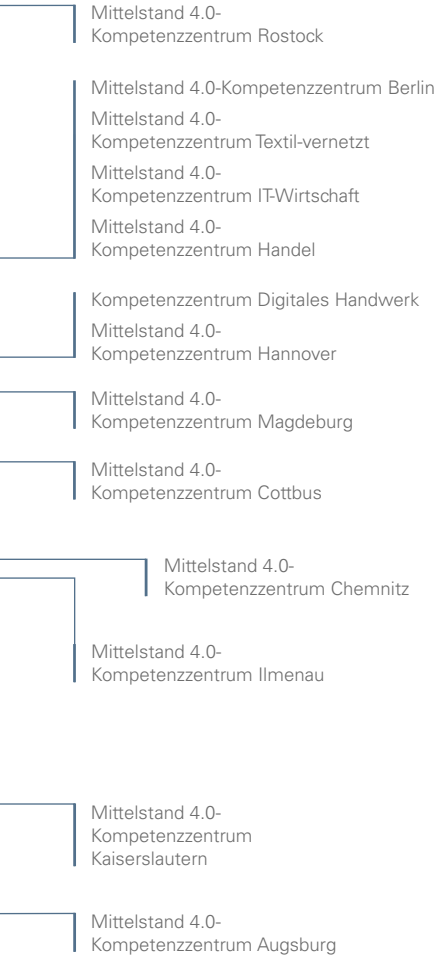
[48] EPRS | European Parliamentary Research Service – Blockchain and the General Data Protection Regulation, Juli 2019, https://t1p.de/w3dh.

[49] So auch die Bundesregierung in Drs. 19/6034,https://t1p.de/01wv.

SECHS

ÜBER MITTELSTAND-DIGITAL





Stand: Juli 2019

Das Mittelstand 4.0-Kompetenzzentrum Hamburg ist eines von aktuell 26 Mittelstand 4.0-Kompetenzzentren bundesweit. Diese sind Teil der Förderinitiative „Mittelstand 4.0 – Digitale Produktions- und Arbeitsprozesse“, die im Rahmen des Förderschwerpunkts „Mittelstand-Digital – Strategien zur digitalen Transformation der Unternehmensprozesse“ vom Bundesministerium für Wirtschaft und Energie (BMWi) gefördert wird.

Das Mittelstand 4.0-Kompetenzzentrum Hamburg richtet sich insbesondere an Unternehmen kleinerer und mittlerer Größe in der Metropolregion Hamburg und unterstützt diese auf ihrem Weg zur Digitalisierung von Prozessen und Produkten.
Ein besonderer Fokus liegt dabei auf dem Bereich Logistik.

Weitere Informationen finden Sie unter:
https://www.kompetenzzentrum-hamburg.digital/

SIEBEN

MITTELSTAND 4.0-KOMPETENZZENTRUM

Für kleine und mittlere Unternehmen bei Fragen und Herausforderungen der digitalen Transformation.

KONTAKT:

Mittelstand 4.0-
Kompetenzzentrum Hamburg
Rudolf Neumüller (Leiter)
c/o HKS Handelskammer Hamburg
Service GmbH

Adolphsplatz 1
20457 Hamburg
Tel.: +49 40 36138-263
kompetenzzentrum@hk24.de

WEITERES INFOMATERIAL FINDEN SIE HIER:

Online finden Sie unseren aktuellen Flyer und weitere Informationen.

QR-Code mit dem Smartphone abscannen

www.kompetenzzentrum-hamburg.digital
www.facebook.com/digitalvoraushamburg

PROJEKTPARTNER:

Konsortialführer des Mittelstand 4.0-Kompetenzzentrums Hamburg und zentraler Ansprechpartner für Unternehmen ist die HKS Handelskammer Hamburg Service GmbH.

Handelskammer Hamburg
HKS Service

Weitere Projektpartner im Mittelstand 4.0-Kompetenzzentrum Hamburg sind:

- Technische Universität Hamburg
- Helmut-Schmidt-Universität
- Hochschule für Angewandte Wissenschaften
- Handwerkskammer Hamburg

TUHH
Technische Universität Hamburg

Helmut Schmidt Universität
Universität der Bundeswehr Hamburg

HAW Hamburg

Handwerkskammer Hamburg

Mit Unterstützung von:

HEUKING KÜHN LÜER WOJTEK

ACHT

IMPRESSUM

HERAUSGEBER:

Prof. Dr. Dr. h. c. Wolfgang Kersten
Technische Universität Hamburg
Für das Mittelstand 4.0-Kompetenzzentrum Hamburg

AUTOREN:

Dr. Hans Markus Wulf, Partner
Theresa Bardenhewer, wiss. Mit.
HEUKING KÜHN LÜER WOJTEK

Sebastian Lodemann, M.Sc.
Technische Universität Hamburg
Für das Mittelstand 4.0-Kompetenzzentrum Hamburg

GESTALTUNG:

LOCKVOGEL – Werbenest Hamburg, www.lockvogel-hamburg.de

DRUCK:

Beisner Druck GmbH & Co. KG

BILDNACHWEIS:

Sikov/stock.adobe.com (1), Feodora/stock.adobe.com (4)
DatenschutzStockfoto/stock.adobe.com (6), sdecoret/stock.adobe.com (17),
greenbutterfly/stock.adobe.com (28), Siarhei/stock.adobe.com (31),
yingyaipumi/stock.adobe.com (33)

AUFLAGE:

1. Auflage, 02/2020

Was ist Mittelstand-Digital?

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Regionale Kompetenzzentren helfen vor Ort dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenlose Nutzung aller Angebote von Mittelstand-Digital. Weitere Informationen finden Sie unter www.mittelstand-digital.de

www.kompetenzzentrum-hamburg.digital

MITTELSTAND 4.0-KOMPETENZZENTRUM HAMBURG

Adolphsplatz 1, 20457 Hamburg
Tel.: +49 40 36138-263, kompetenzzentrum@hk24.de