2.3.2 Datenschutz in 4.0-Prozessen

Stichwörter: Arbeitnehmerdatenschutz, Kundendatenschutz, Identitätsschutz, Anonymisierung, Pseudonymisierung, Verschlüsselung, personenbezogene Daten

› Warum ist das Thema wichtig?

Die intelligente Software[1] mit ihren Modellen der künstlichen Intelligenz (KI) kann Arbeitsvorgänge protokollieren, im Voraus strukturieren und 4.0-Prozesse[2] ganz oder teilweise steuern. Dabei erfassen cyber-physische Systeme (CPS)[3] nicht nur Sach-, Material-, Prozess- und Auftragsdaten. Sie sammeln ebenfalls Daten über Ort, Zeit und Ergebnis der Tätigkeit des arbeitenden Menschen. Deswegen ist das Thema Datenschutz in fast allen 4.0-Prozessen zu beachten.

› Worum geht es bei dem Thema?

Begriff: Datenschutz
Der Datenschutz betrifft personenbezogene Daten und den Schutz vor deren Missbrauch während der Erhebung, Verarbeitung und Nutzung. Dabei gilt das Recht auf informationelle Selbstbestimmung. Demnach ist jeder Mensch nach dem Grundgesetz (GG) der Bundesrepublik Deutschland frei und kann selbst darüber entscheiden, wie mit seinen personenbezogenen Daten umgegangen wird, sofern kein Gesetz eine andere Regelung vorsieht. Grundlage für den Datenschutz in Deutschland bilden, neben dem GG, die EU-Datenschutz-Grundverordnung (EU-DSGVO)[4] und das Bundesdatenschutzgesetz (BDSG n.F.). Zusätzlich gibt es spezielle Regelungen in den Bundesländern.[5] Wer die darin aufgeführten Anforderungen nicht erfüllt, muss mit drastischen Bußgeldern rechnen. Der Wandel hin zu „Arbeit 4.0“ und die Datenschutzregelungen erfordern von Betrieben und allen Beteiligten, aber auch von Selbstständigen eine deutlich höhere Sensibilität und ein Bewusstsein für Belange des Datenschutzes.[6]

Autonome und selbstlernende Software-Systeme (CPS) und 4.0-Technologien[7] generieren und sammeln bei ihrem Einsatz innerhalb des Betriebes und in betriebsübergreifenden Wertschöpfungsketten ständig neue Daten, die durch Sensoren und miniaturisierte Verwaltungsprogramme erfasst und zum Beispiel von intelligenter Software (inkl. KI) weiterverarbeitet werden können. Dinge wie Maschinen, Gebäude, Fahrzeuge, aber auch Personen und Prozesse produzieren Daten, wenn diese mit dem System verknüpft beziehungsweise daran angeschlossen sind. Zu diesen Daten gehören in der Regel auch personenbezogene oder personenbeziehbare Daten von Beschäftigten, Kunden und externen Selbstständigen. Dadurch entsteht ein Datengeflecht, das als Big Data bezeichnet wird. So kann beispielsweise ein neu gekaufter Handbohrer Daten produzieren und mit dem Hersteller oder weiteren Akteuren kommunizieren, zum Beispiel über Einsatzort und -dauer, Arbeitsgeschwindigkeit oder Verschleiß. In Zeiten der digitalen Transformation können Daten umfassend erfasst und Personen sowie „digitalgesteuerten“ Maschinen zugeordnet werden und mit den Daten können beispielsweise Personenprofile erstellt werden.

Dies bedeutet, dass der Betreiber wissen sollte, welche Daten wie erzeugt werden, wie der Zugriff darauf geregelt ist und wie die Beschäftigten hier einbezogen werden müssen. So rücken die 4.0-Prozesse den Datenschutz in den Fokus. Es geht darum, dies im Betrieb proaktiv voranzutreiben. Dazu gehört zum Beispiel zu wissen, welche personenbezogenen Daten erhoben und verarbeitet werden, und die Überlegung, ob betriebsspezifische Regelungen zum Umgang mit diesen Daten erforderlich sind (wie Zustimmungserklärung, Vereinbarung). Dies gilt insbesondere dann, wenn die Daten, die über CPS erfasst und ausgetauscht werden, den rechtlich verfassten Ort Betrieb via horizontale Wertschöpfungskette verlassen, das heißt zu Herstellern, Kunden oder Lieferanten gelangen. Der erfolgreiche, rechtssichere und präventive Einsatz von intelligenter Software (inkl. KI) gelingt nur mit Datenschutz.

Diese Umsetzungshilfe gibt Experten und Interessierten Anregungen, wie Arbeit 4.0 zu gestalten ist. Die Empfehlungen sollten an die jeweilige konkrete betriebliche Situation angepasst werden.

[1] Intelligente Software steuert cyber-physische Systeme (CPS) und andere autonome technische Systeme (wie Messenger-Programme). Intelligente Software nutzt Modelle künstlicher Intelligenz zusammen mit anderen Basistechnologien wie zum Beispiel Algorithmen, semantischen Technologien, Data-Mining. Intelligente Software ist autonom und selbstlernend.

[2] Unter 4.0-Prozessen werden hier alle Arbeitsprozesse verstanden, in denen cyber-physische Systeme (CPS) oder andere autonome technische Systeme (wie Plattformen, Messenger-Programme) beteiligt sind. 4.0-Prozesse sind in den Arbeitsprozessen bisher selten vollständig, aber in Ansätzen in allen Betrieben umgesetzt.

[3] Cyber-physische Systeme (CPS) verbinden und steuern als autonome technische Systeme Arbeitsmittel, Produkte, Räume, Prozesse und Menschen beinahe in Echtzeit. Die komplette oder teilweise Steuerung übernimmt intelligente Software auf Grundlage von Modellen der künstlichen Intelligenz. Genutzt werden dazu unter anderem auch Sensoren/Aktoren, Verwaltungsschalen, Plattformen/Clouds.

[4] EU-DSGVO – Die Verordnung soll zu einer weitgehenden Vereinheitlichung europäischen Datenschutzrechtes führen.

[5] Während die EU-DSGVO die Grundsätze regelt, gehen in einzelnen Regelungsbereichen spezielle Datenschutzregelungen vor, zum Beispiel hat der Gesetzgeber bei der Behandlung personenbezogener Beschäftigtendaten spezielle Regelungen in § 26 BSDG n. F. beziehungsweise in den Landesdatenschutzgesetzen festgelegt.
Für den Betrieb kann statt des BDSG n. F. alternativ das Datenschutzgesetz des jeweiligen Bundeslandes gelten, in dem sich der Unternehmenssitz befindet. Es ist sinnvoll, sich intensiv mit den für den Betrieb maßgeblichen Gesetzen auseinanderzusetzen. Hilfestellungen bieten in der Regel Industrie- und Handelskammern, Handwerkskammern oder branchenspezifische Verbände.

[6] Schröter 2015

[7] 4.0-Technologie bezeichnet hier Hardware und technologische Produkte (wie Assistenzmittel/Smartphones, Sensoren/Aktoren in smarten Arbeitsmitteln, Fahrzeugen, Produkten, Räumen usw., smarte Dienstleistungen, Apps), die von intelligenter Software (inkl. KI) ganz oder teilweise gesteuert werden.

Die Datensammlung ist in keinem Betrieb unbekannt. So werden in Buchhaltungsprogrammen, Personal- und Kundendateien oder Materialdatenbanken Daten erfasst, verarbeitet und gespeichert. In der digitalen Transformation gewinnt dies zunehmend an Bedeutung, da durch die gestiegene Leistungsfähigkeit und weitergehende Miniaturisierung von Sensoren, verbunden mit zunehmend billiger und breiter verfügbar werdenden Technologien, eine Vielzahl von Informationen erfasst werden kann – in allen Bereichen der Leistungserbringung: Daten werden unaufhörlich produziert, beispielsweise von Fahrzeugen, Produkten und Dienstleistungen, Arbeitsmitteln, Führungskräften und Beschäftigten sowie von Kunden.[8] Dazu gehören auch Taktfrequenzen der Arbeit und das Leistungsprofil der Person. So kann beispielsweise erhoben werden, wie schnell ein Beschäftigter einen Arbeitsschritt ausführt oder ob Fehler gemacht werden. Ermöglicht werden die Erstellung umfassender Profile und die Verknüpfung mit anderen über die jeweilige Person verfügbaren Daten. Intelligente Software (inkl. KI), kann programmiert werden, um mit den erhobenen Daten Anwendungen zu erzeugen (wie die ganze oder teilweise Steuerung von Maschinen und Fahrzeugen, Organisationsprozesse im Betrieb oder Persönlichkeitsprofile). Datenverarbeitung ist allgegenwärtig geworden und wird fast unbemerkt im Hintergrund vollzogen. Die Daten können unter Umständen Bestandteil des Internets werden, was die neue Qualität der Verknüpfung, Kommunikation und Steuerung von Daten erzeugenden Dingen und Personen über intelligente Software (inkl. KI) im Internet beschreibt.

Neben Daten-Akquisen in vertikal vernetzten CPS (auch Wertschöpfungsprozessen) kommen Datensammlungen aus betriebsübergreifenden Wertschöpfungsprozessen hinzu, wie Informationen zu Angeboten, Beschwerden, Profile von Kunden. Damit lassen sich einerseits beispielsweise betriebsübergreifende Montageabläufe ganz oder teilweise steuern wie auch aus Qualitätssicherungsgründen dokumentieren. Andererseits können CPS somit Daten aus einem Betrieb in einen anderen transportieren. Gegebenenfalls kann das Datenvolumen um Daten von Crowd-Plattform-Beteiligten erweitert werden, wenn im Umsetzungsprozess eines Arbeitsganges Daten von Crowdworkern, wie zur Arbeitsleistung, Arbeitszeit, Produktivität und Einhaltung der Sicherheitsstandards, Datenschutz oder Datensicherheit integriert werden. Dies alles bringt effektive und effiziente Möglichkeiten für die Gestaltung der Arbeit mit sich und eröffnet auch der betrieblichen Prävention neue Potenziale, wenn der Datenschutz beachtet wird.

Aus technischer Perspektive werden die personenbezogenen und personenbeziehbaren Daten zumeist nicht primär aus Kontrollgesichtspunkten zur Überprüfung der Beschäftigten zusammengeführt. Vielmehr sollen sie dazu dienen, über direkte, indirekte und Metadaten den beabsichtigten Abläufen überhaupt eine Art „Schmiermittel“ (bildlich gesprochen wie eine Art Motoröl) mitzugeben. Die Aggregation dieser Daten kann dazu führen, dass betriebliche Abläufe optimiert werden und reibungsloser funktionieren. So kann die Herausforderung sowohl aus betrieblicher als auch aus datenschutzrechtlicher Perspektive weniger in Einschränkung der Erhebung der Daten liegen, sondern eher in der Art und Weise, wie die Daten erfasst, verarbeitet und ausgewertet werden.

Diese („Schmiermittel“-)Daten dienen zugleich als Fundament für vorausschauende betriebliche Anwendungen von Big-Data-Systemen. Sie können angereichert werden durch Daten aus Scannern, Sensoren, intelligenten Brillen und Kleidungsstücken, durch Daten aus eingebetteten Systemen, Crowd-Plattformen et cetera. So können personen- und prozessbezogene Daten gesammelt, zusammengeführt, analysiert und für eine wirkungsvolle Prozessgestaltung genutzt werden. Die Möglichkeit der automatisierten Bewertung der Daten eröffnet zugleich ungeplante Potenziale, die Prozesse verändern können, gegebenenfalls ohne dass die Beteiligten dies merken. Dies gelingt mit kleinen und großen Datenmengen. Beispielsweise können Daten über Auslastung, Anwendungen (etwa ergonomische Parameter, Nutzung der Schutzeinrichtungen), Leerzeiten, Störungen und Wartungsintervalle Informationen sein, die verarbeitet werden.

Die Personen in Betrieben können sich dieser durch CPS-Prozesse stattfindenden Sammlung und Verarbeitung von Daten vom Ansatz her nicht entziehen. Es kommt also darauf an, die Prozesse so zu gestalten, dass alle etwas davon haben. Ein Bestandteil dieses Gestaltungsprozesses ist das Thema Datenschutz. In vielen kleinen und mittleren Unternehmen hat es aber keine ausreichende Priorität.

Daher ist es hilfreich für die Führungskräfte, folgende Fragen zu reflektieren:[9]

- Welche Daten werden im Betrieb generiert und für was verwendet (Produktdaten, Lager- und Bestandsdaten, Maschinenauslastung, Kunden- und Beschäftigtendaten (personenbezogene Daten), Umgebungsdaten (Position, Temperatur, Beleuchtung)?
- Welcher Risikoklasse gehören diese Daten an? Ist gegebenenfalls eine Datenschutzfolgeabschätzung vorzunehmen?[10]
- Welche digitalen und mobilen Kommunikationswege und Möglichkeiten der Datenvermittlung werden genutzt und welche Daten werden warum übermittelt (Messenger-Apps)?
- Wie und durch was werden die Daten erfasst (systematische/automatisierte Datenerfassung)?
- Welche Daten stehen zur Verfügung und sind im Betrieb von Relevanz (Daten zu Produkten, Prozessen, Beschäftigten, Know-how)?
- Welche Daten stellt die intelligente Software (inkl. KI) wem und wofür zur Verfügung/welche werden generiert?
- Wo sind die Daten verortet (Cloud oder intern? Bei Ablage der Daten in einer Cloud: Welche Informationen zum Schutz der Daten liegen vor? [Zertifizierung, deutsche Gesetzgebung])?
- Welche Schnittstellen der CPS zu anderen Programmen (zum Beispiel Assistenzsysteme, Verwaltungssoftware von CPS) gibt es?

[8] Büttner & Brück 2015, S. 131
[9] Cernavin & Lemme 2018
[10] Art. 35 der DSGVO verpflichtet die Verantwortlichen, eine Datenschutzfolgeabschätzung (DSFA) vorzunehmen, wenn ein „voraussichtlich hohes Risiko“ mit der Verarbeitung von Daten verbunden ist. Ein solches Risiko liegt in der Regel vor, wenn die unsachgemäße Handhabung der Daten einen betroffenen Menschen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte (Ansehen der Person oder existenz- oder lebensbedrohende Schädigungen). Das Ansehen betreffende Daten sind zum Beispiel Daten zu Einkommen, Beitragszahlungen oder Sozialleistungen, Zeugnisse oder Gesundheitsdaten. Existenzbedrohend wären dagegen zum Beispiel Daten zu Straffälligkeit, aber auch betriebliche Beurteilungen oder Daten zu Schulden, Pfändungsverfahren und so weiter. Die „Artikel 29 Datenschutzgruppe“ hat in diesem Zusammenhang Beispiele genannt, die gegebenenfalls zu Datenschutzfolgeabschätzungen zwingen. Dazu gehören Scoring, Profiling, automatisierte Einzelfallentscheidungen bei Behörden, aber auch systematische Überwachung oder eine weite geografische Ausdehnung der Verarbeitung.

- Wem gehören die Daten und wie/durch wen/wofür dürfen sie genutzt werden?
- Welche gesetzlichen Vorschriften sind zu beachten (zum Beispiel BDSG, Datenschutzgesetze der Länder, Telemediengesetz, EU-DSGVO, § 87, Abs. 1, Nr. 6 BetrVG) und welche Pflichten gehen damit einher?

Hilfreich könnte es sein, wenn Tarifpartner Rahmenvereinbarungen erarbeiten, die Betriebe als Orientierung nutzen können.

Begriff: Datenschutzbeauftragte
Ein Datenschutzbeauftragter[11] ist im Unternehmen zu benennen, wenn mindestens zehn Personen ständig mit personenbezogenen Daten beschäftigt sind. Datenschutzbeauftragte haben unter anderem die Aufgabe, Unternehmer über Aufgaben und Pflichten im Datenschutz zu informieren, die Umsetzung der Anforderungen zu begleiten und zu überwachen, die Sensibilisierung und Qualifizierung der Beschäftigten im Umgang mit den Daten zu begleiten und mit den Aufsichtsbehörden zusammenzuarbeiten (spezielle Regelungen der Bundesländer beachten).

Welche Chancen und Gefahren gibt es?

Die Anwendung und Nutzung von intelligenter Software (inkl. KI) eröffnet im Hinblick auf den Datenschutz mindestens drei Schlüsselgefahren in der betrieblichen und über- wie außerbetrieblichen Praxis. In einer partizipativ gestalteten und einvernehmlich ausgehandelten 4.0-Arbeits- und Geschäftsumgebung können hohe Datenschutzstandards jedoch auch *neue* Potenziale eröffnen:
Mögliche **Chancen** sind zum Beispiel:

- Ein modernisiertes Datenschutzverständnis auf der Basis von CPS-Anwendungsumgebungen kann im Wettbewerb um Kunden ein wesentlicher Vertrauens- und Marketingvorteil sein. Der Schutz von Kundendaten schafft Kundenbindung.
- Ein modernisiertes Datenschutzverständnis auf der Basis von CPS-Anwendungsumgebungen kann im Wettbewerb um Fachkräfte ein wesentlicher Vertrauensvorteil sein. Der Schutz von Beschäftigtendaten schafft Mitarbeiterbindung.
- Ein Datenschutzverständnis, das die Möglichkeiten von CPS-Anwendungen reflektiert, kann verhindern, dass sich Wettbewerber oder Kriminelle durch Identitätsdiebstahl und Entwendung von sensiblen Firmendaten Wettbewerbsvorteile verschaffen.

Mögliche **Gefahren** sind zum Beispiel:

- Intelligente Software (inkl. KI) und 4.0-Technologien können beinahe in Echtzeit Profile der Person hervorbringen, von denen Daten erfasst wurden. Geschieht dies ohne Kenntnis des Betriebes und der beteiligten Personen im Betrieb, verletzt das den Datenschutz und führt gegebenenfalls zu Verunsicherung und Misstrauen bei den beteiligten Personen.
- Intelligente Software (inkl. KI) und 4.0-Technologien können ungeschützte personenbezogene und personenbeziehbare Daten in horizontale Wertschöpfungsketten einfließen lassen und somit unberechtigten betriebsinternen und betriebsexternen Personen Zugang zu betrieblichen Daten ermöglichen.
- Intelligente Software (inkl. KI) und 4.0-Technologien können ungeschützte Auftrags- und Kundendaten in horizontale Wertschöpfungsketten einfließen lassen und somit unberechtigten betriebsinternen und betriebsexternen Personen Zugang zu betrieblichen Daten ermöglichen.

Welche Maßnahmen sind zu empfehlen?

Die Erfahrungen aus der digitalen Wirtschaft in den letzten Jahren zeigen, dass die größten Herausforderungen für die Betriebe in puncto Datenschutz (Kundendaten, Beschäftigtendaten usw.) in drei Bereichen liegen:

- Fehlende Kenntnis, welche Daten die 4.0-Technologien erfassen, wo diese Daten liegen, was mit ihnen geschieht und wer Zugriff auf diese Daten hat
- Ungenügende Anwender- und Nutzungskultur sowie das Anwenderverhalten (fehlerhafter, lässiger oder unzulässiger Umgang mit personenbezogenen Daten)
- Deutlich ansteigende Zahl äußerer technischer ungezielter Angriffe mithilfe gefährlicher intelligenter Software (wie Viren, Malware, Bots) oder bewusst gezielter Angriffe (etwa Datendiebstahl, Lahmlegung der Systeme, Wissensdiebstahl, Sabotage)

Um der geänderten Situation in Bezug auf den Umgang mit personenbezogenen Daten Rechnung zu tragen, bedarf es eines neuen Umgangs mit dem Thema im Betrieb. Erreicht werden kann dies durch die Schaffung eines neuen Bewusstseins im Unternehmen. Für Betriebe, die in der digital-virtuellen Geschäfts- und Arbeitswelt unterwegs sind, stellt die aktive Kultur eines bewusst gelebten Datenschutzes und einer solide gebauten Datensicherheit ein wesentliches zukunftsträchtiges Qualitäts- und Unterscheidungsmerkmal dar. Diese Qualität bildet einen positiven Wettbewerbsfaktor.

Im Zentrum der Maßnahmen stehen fünf Handlungsebenen:

- Der Betrieb sollte wissen, welche Daten die 4.0-Technologie erfasst, speichert, verarbeitet und wer Zugriff auf sie hat. Vor der Anschaffung der 4.0-Technologie sollten deshalb die Allgemeinen Geschäftsbedingungen beziehungsweise die Lizenzverträge sorgfältig durchgelesen werden. Vom Hersteller sollte eine kurze und verständliche Information eingefordert werden, welche Daten das technische Assistenzsystem erfasst, wie und wo sie gespeichert und verarbeitet wer-

[11] Abschnitt 4 DSGVO

den und wer Zugriff auf die Daten hat, um diese an die Führungskräfte und Beschäftigten weitergeben zu können. *› Siehe Umsetzungshilfe 1.1.7 Informationsblatt smartes Produkt.*

- Der Umgang mit personenbezogenen Daten im Betrieb sollte vereinbart werden. In größeren Betrieben sollte gegebenenfalls unter Einbeziehung des Datenschutzbeauftragten eine Betriebsvereinbarung abgeschlossen werden (Mitbestimmungsrechte und Datenschutz einhalten).
- Die Führungskräfte und Beschäftigten sollten informiert werden, welche Daten die 4.0-Technologie von ihnen erfasst und wie sie verarbeitet werden. *› Siehe Umsetzungshilfen 1.1.7 Informationsblatt smartes Produkt und 1.4.3 Kompetenzen der Beschäftigten in 4.0-Prozessen.*
- Eine Sensibilisierungsoffensive für eine gelebte aktive Datenschutzkultur im Unternehmen gemeinsam mit den Beschäftigten beziehungsweise dem Betriebsrat und Datenschutzbeauftragten starten (zum Beispiel über Möglichkeiten der Datennutzung durch intelligente Software [inkl. KI] informieren, über 4.0-Technologien mit ihrer Sensorik im Betrieb, über mögliche Verhaltensregeln im Umgang mit CPS).
- Die Beschäftigten über die Vereinbarungen und die Maßnahmen des Arbeitgebers zur Sicherung des Datenschutzes mithilfe technischer und organisatorischer Lösungen (Verschlüsselung, Anonymisierung, Pseudonymisierung, elektronische Signaturen) informieren. Auch die sich daraus ergebenden Pflichten für die Führungskräfte und Beschäftigten darstellen (wie sorgsamer Umgang mit personenbezogenen Daten, Informationspflicht über Datenschutzverletzungen). Das Bewusstsein der Führungskräfte und Beschäftigten für Selbstdatenschutz stärken.

Um sich diesem Thema zu nähern, bedarf es Entscheidungshilfen, wie sie zum Beispiel in der nachstehenden Checkliste bereits existieren. Diese Entscheidungscheckliste[12] des Handelns ermöglicht die Auseinandersetzung mit dem Thema und weist auf mögliche Hilfe durch externe Beratung und Kompetenz hin:

1. Starten einer Sensibilisierungsoffensive in der Geschäftsleitung und in der Belegschaft.
2. Überprüfen, ob ein Datenschutzbeauftragter zu benennen beziehungsweise zu beauftragen ist.
3. Datenschutz zusammen mit Datensicherheit zu einem wesentlichen Zukunftsthema des Betriebes machen und Verantwortlichkeiten festlegen.
4. Schulungen für alle betrieblichen Akteure anbieten – gerade auch im Bereich mobiler Nutzungen (etwa Apps, Social Media et cetera).
5. Festlegen, wer und wie die Wirksamkeit der beschlossenen Schutzmaßnahmen überprüft wird.
6. Analyse und Beschreibung der bisherigen Verarbeitung sensibler und personenbezogener Daten.
7. Kurzes Informationsblatt vom Hersteller einfordern, in dem über den Umgang mit den Daten des jeweiligen smarten Produktes informiert wird.
8. Analyse und Beschreibung der technisch neu gestalteten Verarbeitung sensibler und personenbezogener Daten (zum Beispiel in der Cloud).
9. Offensive Beseitigung von Sicherheits- und Schutzlücken.
10. Vereinbarung einvernehmlich verbindlicher Regelungen (zum Beispiel Betriebsvereinbarungen) mit der Belegschaft.
11. Prüfen, ob verlässliche Dienstleister beauftragt werden (zum Beispiel Clouds), die Datenschutz und Datensicherheit garantieren (zum Beispiel Zertifizierung wie Trusted Cloud).
12. Sicherstellen, dass mit Kundendaten sicher und vertrauensvoll umgegangen wird, und überprüfen, ob hier spezielle Vereinbarungen notwendig sind (Kundendatenschutz).
13. Deklaration des hohen Datenschutzes zu einem aktiven Wettbewerbsfaktor.

Bei der Anwendung von intelligenter Software (inkl. KI) und 4.0-Technologien in über- beziehungsweise zwischenbetrieblichen horizontalen Wertschöpfungsbeziehungen sind vertragliche Vereinbarungen zwischen Unternehmen zu treffen, die eine Nutzung unbefugt via CPS erhaltener Daten rechtlich ausschließen.

Quellen und weitere Informationsmöglichkeiten:

Bergmann, L., Möhrle, R., & Herb, A. (2016). *Datenschutzrecht.* Loseblattwerk Boorberg.

Büttner, K. H., & Brück, U. (2015). Use Case Industrie 4.0: Fertigung im Siemens Elektronikwerk Amberg. In T. Bauernhansl, M. ten Hompel, & B. Vogel-Heuser (Hrsg.), *Industrie 4.0 in Produktion, Automatisierung und Logistik* (S. 121–144). Wiesbaden: Springer Vieweg.

Cernavin, O., & Lemme, G. (2018). Technologische Dimensionen der 4.0-Prozesse. In O. Cernavin, W. Schröter, & S. Stowasser (Hrsg.), *Prävention 4.0 – Neue Perspektiven für Führung, Organisation, Sicherheit und Gesundheit im Betrieb* (S. 21–55). Wiesbaden: Springer Verlag.

DSGVO – *Datenschutz-Grundverordnung*, 04.05.2016.

Krause, R. (2016). *Digitalisierung und Beschäftigtendatenschutz. Expertise erstattet dem Bundesministerium für Arbeit und Soziales.* http://www.bmas.de/SharedDocs/Downloads/DE/PDF-Publikationen/Forschungsberichte/fb482-digitalisierung-und-beschaeftigtendatenschutz.pdf?__blob=publicationFile&v=1. Zugegriffen: 31.07.2018.

Datenschutzkonferenz (DSK) (2017). *Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder. Göttinger Erklärung: Vom Wert des Datenschutzes in der digitalen Gesellschaft.* www.lfd.niedersachsen.de/download/116823. Zugegriffen: 19.07.2018.

Schröter, W., & Scherer, I. (2015). *Entscheidungshilfe: Arbeit 4.0. Fragen der IT-Sicherheit in der „Arbeitswelt 4.0“.* http://www.offensive-mittelstand.de/fileadmin/user_upload/pdf/mittelstand_40/Entscheidungshilfe_05_0604.pdf. Zugegriffen: 19.07.2018.

[12] Schröter & Scherer 2015

Schröter, W. (2016). Digitale Sicherheit. In J. Hübner, J. Eurich, M. Honecker, T. Jähnichen,& M. Kulessa (Hrsg.), *Evangelisches Soziallexikon* (9. Aufl., S. 1381–1384). Stuttgart: Kohlhammer Verlag.

Schröter, W. (2016). Abschied vom alten Arbeitsbegriff? – Ein Zukunftsszenario? Gedanken zur digital-virtuellen Transformation der Arbeit und ihrer Folgen. In M. Richter, & I. Thunecke (Hrsg.), *Paradies now. André Gorz – Utopie als Lebensentwurf und Gesellschaftskritik* (S. 166–186). Mössingen-Talheim: Talheimer Verlag.

Zu diesem Thema könnten Sie auch folgende weitere Umsetzungshilfen interessieren:

- 1.1.7 Infoblatt smartes Produkt
- 1.4.3 Kompetenzen der Beschäftigten in 4.0-Prozessen
- 1.6.1 Neue Anforderungen an Interessenvertretungen
- 1.6.2 Mitwirkung und Mitbestimmung in der Arbeit 4.0
- 2.1.2 Integration von intelligenter Software in die Organisation
- 2.1.5 Beschaffung digitaler Produkte
- 2.3.1 Datensicherheit in 4.0-Prozessen
- 2.3.4 Betriebsvereinbarungen und Dienstvereinbarungen zu 4.0-Prozessen

Herausgeber: „Offensive Mittelstand – Gut für Deutschland“ – Stiftung „Mittelstand – Gesellschaft – Verantwortung“
Kurfürsten-Anlage 62, 69115 Heidelberg, E-Mail: info@offensive-mittelstand.de; Heidelberg 2019