2.3.5 Umgang mit Messengern und sozialen Medien

Stichwörter: Messenger, Kommunikation, Smartphone, soziale Medien

› Warum ist das Thema wichtig?

In der Arbeit in cyber-physischen Systemen[1] mit intelligenter Software[2] können sich Teile der Kommunikation innerhalb des Unternehmens, aber auch mit Kunden, Lieferanten und der Öffentlichkeit auf digitale Kommunikationsplattformen wie Messenger oder soziale Medien verlagern. Diese Kommunikation im Arbeitsprozess kann über digitale Assistenzsysteme jederzeit zeit- und ortsunabhängig geführt und verfolgt werden. Die Nutzung der Messenger kann die Kommunikation erleichtern, kann aber auch mit neuen Formen der Abhängigkeiten und anderen Gefahren verbunden sein. Insofern ist ein reflexiver Umgang im betrieblichen Einsatz dieser Dienste sinnvoll.

› Worum geht es bei dem Thema?

Begriff: Messenger
Unter Messengern werden Internetdienste verstanden, mit denen Kommunikation zwischen zwei Empfängern oder innerhalb definierter Gruppen beinahe in Echtzeit möglich ist. Sie funktionieren als installierte Applikation (App) auf technischen Assistenzsystemen wie Smartphones und -watches, Tablets, PCs und anderen Endgeräten, sind häufig aber auch ohne Installation online nutzbar. Sie ermöglichen Personen den Versand und Empfang von Text- und Sprachnachrichten, Bildern und Videos und anderen Dateien. Weitere Funktionen sind Bezahlmöglichkeiten oder die Übermittlung von Standortdaten. Vereinzelte Dienste setzen auch Chat-Bots ein. Die Nutzung setzt in der Regel eine Registrierung voraus. Viele Messengerdienste können auch auf weitere Funktionen und Daten des technischen Assistenzsystems des Nutzers zugreifen.

In der Regel fallen bei der Nutzung von Messengerdiensten keine weiteren Kosten an, weil die Anbieter ihr Geschäft mit den Daten der Nutzer realisieren.

Nutzung von Messengerdiensten im Betrieb

Der Grund für die Betriebe, Messengerdienste zu nutzen, liegt in den Vorteilen dieser Technologie. So können nahezu beliebig viele Personen zeit- und raumunabhängig bilateral oder in einer Gruppe kommunizieren, Absprachen treffen und gemeinsam an Arbeitsaufgaben arbeiten.[3] Denkbar ist auch die Einbindung der Messenger in smarte Personaleinsatzplanung › *siehe Umsetzungshilfe 2.6.1 Digitale Planung des Personaleinsatzes*. Das durch Messengerdienste veränderte Kommunikationsverhalten kann auch Einfluss auf betriebliche Abläufe haben, etwa durch schnellere Reaktionsmöglichkeiten aufgrund transparenterer Arbeitsabläufe durch orts- und zeitunabhängige Information und Visualisierung.

Messenger können auch für das Marketing des Unternehmens, seiner Produkte und Leistungen genutzt werden; sie ermöglichen eine kurze Status- oder Selbstbeschreibung sowie die Platzierung von Logos und Werbebotschaften. Über Messengerdienste kann der Status der Übertragung und Kenntnisnahme der Nachricht nachvollzogen werden. Unabhängig von ethischen Überlegungen ermöglichen Messengerdienste den Einsatz von Chat-Bots zum Beispiel zur Kundenakquisition auf Basis von Kundenprofilen.

Viele Betriebe nutzen diese Messengerdienste zum Beispiel in der Kundenkommunikation und beim mobilen Arbeiten. Mittlerweile sind aber auch viele Betriebe gegenüber den meisten frei angebotenen Messengerdiensten zurückhaltender.[4] Auf diesen Messengerplattformen werden private und berufliche Kommunikation verknüpft, interne betriebliche Daten über Geschäftsprozesse durch Dritte genutzt und es kommt zu Problemen im Umgang mit personenbezogenen Daten von Beschäftigten, Kunden und Lieferanten.

Ein Dilemma der Messengerkommunikation

Bei der Entscheidung zwischen verschiedenen Anbietern ist zwischen der firmeninternen (Kommunikation mit Kollegen oder Vorgesetzten) und der firmenexternen Verwendung (Kommunikation mit Kunden oder Geschäftspartnern) zu unterscheiden. Während die Anwendung für den internen Gebrauch frei gewählt werden kann, ist die externe Nutzung an das Nutzungsverhalten der Kunden oder Geschäftspartner gebunden, da diesen nur schwer eine bestimmte Anwendung empfohlen werden kann. Das hat zur Folge, dass Unternehmen in der Kundenkommunikation unter Umständen freie

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] 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.

[2] 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.

[3] Limits liegen je nach Messenger zwischen 30 und 256 Personen.

[4] vgl. u. a. Astheimer et al. 2018; www.datenschutzbeauftragter-info.de; www.zeit.de

Messengerdienste nutzen müssen, die nicht dem Sicherheitsstandard des Unternehmens entsprechen. Das Dilemma ist in der unternehmensexternen Kommunikation schwer aufzulösen, da Firmen, die diese Plattformen nicht nutzen, möglicherweise einen Wettbewerbsnachteil haben.

Kriterien für die Qualität von Messengerdiensten

Wer die Vorteile von Messengerdiensten nutzen will, sollte auf die Qualität des Dienstleisters achten. Im Folgenden werden einige Kriterien für die Qualität der Dienstleister beschrieben[5].

- *Verschlüsselung der Nachrichten:* Ein wesentliches Qualitätskriterium ist die Verschlüsselung von Nachrichten, die über Messenger ausgetauscht werden. Sie bewirkt, dass diese Nachrichten nicht von Dritten, etwa dem Anbieter oder Personen im selben WLAN, eingesehen und genutzt werden können.
  Der Messengerdienst sollte folgende Verschlüsselungsarten auf allen Betriebssystemen und für alle übertragenen Daten (inklusive Bilder, Videos, Sprachnachrichten oder anderer Dateien) unterstützen:
  - *Transportverschlüsselung* stellt sicher, dass Nachrichten und Metadaten (zum Beispiel Absender, Empfänger, Zeitstempel, Protokolle) auf dem Weg zwischen Geräten der Kommunikationspartner und dem Server des Dienstanbieters verschlüsselt sind. Auf dem Server des Messengerdienstes liegt die Nachricht unverschlüsselt vor.
  - *Ende-zu-Ende-Verschlüsselung* stellt sicher, dass Nachrichten nur auf den Geräten der Kommunikationspartner im Klartext vorliegen. Auf dem Weg zwischen den technischen Assistenzsystemen ist die Nachricht durchgehend verschlüsselt. Anders als bei der Transportverschlüsselung kann der Messengerdienst die Nachricht nicht lesen (Schutz der Vertraulichkeit, der Authentizität und Integrität).
  - *Verschlüsselt Speicherung* stellt sicher, dass auf dem technischen Assistenzsystem private Schlüssel, Chatverläufe und andere sensible Daten verschlüsselt auf dem Gerät des Benutzers abgelegt sind.
- *Verschlüsselung der Daten auf dem technischen Assistenzsystem:* Es besteht die Möglichkeit der Verschlüsselung weiterer Daten (zum Beispiel komplette Kontaktliste, E-Mails, Standort) auf dem Assistenzsystem, von dem die Nachricht gesendet wird. Der Messengerdienst macht transparent, auf welche dieser Daten des technischen Assistenzsystems er zugreifen könnte. Eine Verschlüsselung ist zum Beispiel dadurch möglich, dass die Zugriffe verweigert werden können.
- *Transparenz der Verschlüsselungen:* Die Verschlüsselungen müssen transparent und dem Nutzer ersichtlich sein. Sie sollten nicht erst manuell aktiviert werden müssen. Dadurch soll verhindert werden, dass sensible Betriebsdaten und Daten von Kunden und Beschäftigten unbemerkt Dritten zugänglich werden.
- *Datenschutz:* Der Messengerdienst garantiert in den AGB und in der technischen Realisierung den Schutz von personenbezogenen Daten. Dazu gehört insbesondere, was mit den Daten geschieht, wer auf sie Zugriff hat, wo sie gespeichert werden, wie sie weiter verwendet werden. Es ist auch angegeben, ob der Messengerdienst mit weiteren sozialen Netzwerken verknüpft ist › *siehe Umsetzungshilfe 2.3.2 Datenschutz in 4.0-Prozessen*.
- *Datensicherheit:* Der Messengerdienst garantiert den sicheren Umgang mit den Daten. So wird zum Beispiel die Verbreitung von Schadprogrammen verhindert (wie zum Beispiel Viren, Trojaner) und die Zugangskennwörter sind gesichert › *siehe Umsetzungshilfe 2.3.1 Datensicherheit in 4.0-Prozessen*.
- *Kenntlichmachung von Bot-Nachrichten:* Der Messengerdienst erlaubt die Kommunikation von Social Bots/Chat-Bots nur dann, wenn diese als solche gekennzeichnet sind. Unter dieser Voraussetzung ermöglicht es der Messengerdienst Unternehmen, Chat-Bots für automatisierte Fragen in der Kundenkommunikation einzusetzen.
- *Gebrauchstauglichkeit:* Der Messengerdienst ist intuitiv bedienbar, benutzt einfache Erklärungen und Begriffe und ist softwareergonomisch gut gestaltet › *siehe Umsetzungshilfe 3.3.2 Gebrauchstauglichkeit der intelligenten Software (inkl. KI)*.
- *Vertrauenswürdigkeit des Anbieters:* Der Messengerdienst sollte die Qualität seiner Dienstleistungen nachweisen – zum Beispiel durch Zertifizierungen und Siegel (wie Qualitätsmanagement nach DIN ISO 9001, IT-Sicherheit-Zertifizierung nach DIN ISO 27001), Verweise auf Empfehlungslisten zum Beispiel der Verbraucherschutzverbände.[6] Außerdem sollte der Dienstleister nachweisen wie er das Urheberrecht der Daten garantiert (der eigenen und der Daten von Dritten).
- *Gerichtsstandort:* Im Falle von Auseinandersetzungen gilt das Rechtssystem des Landes, in dem der Messengerdienst eingetragen ist.

Es sollte überprüft werden, ob gegebenenfalls Open-Source-Anwendungen bei der Nutzung von Messengerdiensten Vorteile bieten.

Einführung von Messengerdiensten

Bei der Nutzung von Messengerdiensten im Betrieb sollte zunächst einmal festgelegt werden, welchen Nutzen diese Dienste für die betriebliche Kommunikation und die Kunden-Kommunikation bieten. Dabei ist das oben beschriebene Dilemma zu beachten und aufzulösen. Dann ist ein Verfahren festzulegen, wie die Messengerdienste in die betrieblichen Abläufe integriert werden – vergleiche unten Maßnahmen › *siehe Umsetzungshilfe 2.1.2 Integration von intelligenter Software (inkl. KI) in die Organisation*. Dabei ist auch die Bedienfreundlichkeit der verwendeten technischen Assistenzsysteme zu beachten, die zu den Arbeitskontexten passen müssen (etwa Blendfreiheit, ausreichend großes Display, Stoß- und Bruchsicherheit, Bereitstellung von Touchstiften zur Bedienung mit Handschuhen) › *siehe Umsetzungshilfe 3.3.2 Gebrauchstauglichkeit der intelligenten Software (inkl. KI)*.

Es ist ein Verfahren zum Umgang mit den Messengerdiensten im Betrieb festzulegen sowie mit den Führungskräften und Beschäftigten zu vereinbaren. Dabei

[5] in Anlehnung an die Empfehlungen des BSI – Bundesamt für Sicherheit in der Informationstechnik
[6] siehe diverse Angebote im Internet

sind auch die Aspekte von Datensicherheit und Datenschutz zu beachten. Es ist zu prüfen, ob die Führungskräfte und Beschäftigten technische Assistenzsysteme sowohl privat als auch betrieblich nutzen. Sollte das der Fall sein, sind spezielle Verhaltensregeln zu vereinbaren und technische Schutzmaßahmen vorzunehmen › *siehe Umsetzungshilfe 3.2.2 Smartphone, -watch, -glasses.*

Bei der Einführung von Messengerdiensten im Betrieb sind spezielle Hinweise für Führungskräfte und Beschäftigte zu beachten. Allen Führungskräften und Beschäftigten sollten das Ziel, die Funktion und der Nutzen der Messengerdienste erklärt werden. Zu beachten sind die Unterschiede in den Affinitäten der Führungskräfte und Beschäftigten zum Umgang mit dem Smartphone oder den anderen technischen Assistenzsystemen. So kann die Nutzung von Messengern weniger digital-affine Führungskräfte und Beschäftigte stärker beanspruchen. Der Betrieb sollte diese Führungskräfte und Beschäftigten unterstützen und sie im Umgang mit den Messengerdiensten und den technischen Assistenzsystemen trainieren sowie ihnen gegebenenfalls einen Mentor zur Seite stellen.

› Welche Chancen und Gefahren gibt es?

Kommunikation über Messengerdienste bietet unter anderem folgende **Chancen**:

- Raum- und ortsunabhängige innerbetriebliche Kommunikation beispielsweise bei mobilen Arbeitsplätzen, Crowdworking, virtuellen Teams
- Neue Form der Einbindung von Kunden zum Beispiel in die Produktenwicklung, Kundenfeedback, Erkennen von Kundenbedarfen
- Ansprechen neuer Kundengruppen
- Marketing des Unternehmens, seiner Produkte und Leistungen – Status- oder Selbstbeschreibung, Platzierung von Logos und Werbebotschaften
- Beantwortung von Routineanfragen über Chat-Bots
- Wichtige Hilfsmittel beim Führen auf Distanz
- Erhöhung der Kommunikationsgeschwindigkeit
- Direkter Zugriff auf und schnelles Wiederfinden der benötigten Dateien raum- und zeitunabhängig
- Einbindung der Messenger in smarte Personaleinsatzplanung
- Schnellere Reaktionsmöglichkeiten durch transparentere Arbeitsabläufe, Information, Visualisierung

Kommunikation über Messengerdienste bietet unter anderem folgende **Gefahren**:

- Sensible betriebliche Daten sowie personenbezogene Daten von Beschäftigten, Kunden und Zulieferern können bei fehlender Verschlüsselung missbraucht werden
- Zugriff von Messenegerdiensten auf technische Assistenzsysteme des Betriebes und damit auf interne Betriebsdaten sowie auf personenbezogene Daten von Führungskräften und Beschäftigten
- Durch fehlende Transparenz der Verschlüsselung von Messengerdiensten wird Datenmissbrauch nicht erkannt.
- Fehlende Datensicherheit beim Messengerdienst mit beispielsweise Datenverlusten, unberechtigtem Zugriff auf interne Nachrichten, Angriffen durch Dritte
- Ausländischer Gerichtsstandort, der nicht europäischem Recht unterliegt, mit aufwendiger, langwieriger und komplizierter Konfliktregelung
- Problematische Verbindung zwischen betrieblicher und privater Nutzung von technischen Assistenzsystemen
- Permanente Erreichbarkeit, Arbeitsintensivierung
- Polarisierung zwischen technikaffinen und nicht-technikaffinen Personen im Betrieb
- Reduzierung von wichtiger personenbezogener Kommunikation
- Missverständnisse aufgrund von technischer Kommunikation

› Welche Maßnahmen sind zu empfehlen und einzuleiten?

Maßnahmen zur Anschaffung eines Messengerdienstes

Bei der Anschaffung eines Messengers für betriebliche Zwecke sollten unter anderem folgende Aspekte beachtet werden:[7]

- Die Führungskräfte sollten festlegen, welchen Nutzen und welche Funktion der Messengerdienst für die Kommunikation im Unternehmen und die Kundenkommunikation haben kann und soll. Das oben beschriebene Dilemma der Messengerkommunikation berücksichtigen – gegebenenfalls für die interne Kommunikation eine unternehmenseigene Messengerplattform nutzen und für die Kundenkommunikation einen öffentlichen Messengerdienst. Ein entsprechendes Kommunikationskonzept festlegen.
- Die Führungskräfte sollten wissen, welche Experten zur Bewertung des Nutzens und der Funktion von Messengerdiensten hinzugezogen werden sollen, zum Beispiel IT-Experte, Datenschutzbeauftragter, Fachkraft für Arbeitssicherheit, Digital-Mentor › *siehe Umsetzungshilfe 2.1.8 Digital-Mentor („Kümmerer“).*
- Festlegen, nach welchen Qualitätskriterien die Messengerdienste erfüllen sollen (siehe Kriterien oben).
- Das Kommunikationskonzept für die Messengerdienste mit anderen Führungskräften und den Beschäftigten besprechen.
- Die Führungskräfte sollten festlegen, welche technischen Funktionen und Dienstleistungen der Messengerdienst für das geplante Kommunikationskonzept erfüllen soll, und sich informieren, welche Lösungen verfügbar sind und welche Funktionen diese bieten. Dabei auch prüfen, für welche Geräte die Messenger geeignet sind (mobil, Desktop, Web). Dies ist mit den im Betriebskontext genutzten Geräten abzugleichen.

[7] Brands & Roellgen 2016

- Messengerdienst auswählen und überprüfen, ob er die Qualitätskriterien erfüllt sowie sicher und qualitätsorientiert arbeitet. Nicht jeder Messenger ist für jedes Betriebssystem (Android, iOS, Windows, Blackberry) geeignet. Es existieren aber Multi-Messenger, die auf mehreren Betriebssystemen verwendet werden können.
- Die Führungskräfte sollten überprüfen, ob sie selbst und alle Beschäftigten die technischen Assistenzmittel besitzen, die zum Umgang mit den Messengerdiensten erforderlich sind und diese gegebenenfalls anschaffen › *siehe Umsetzungshilfe 3.2.2 Smartphone, -watch, -glasses*.
- Bei der Integration der Messengerdienste in die betrieblichen Softwareumgebungen die Datensicherheit *sicherstellen* › *siehe Umsetzungshilfen 2.3.1 Datensicherheit in 4.0-Prozessen; 2.2.3 Risikobetrachtung und IT-Sicherheit*.

Maßnahmen zur Einführung und zum Umgang mit Messengerdiensten

- Die Führungskräfte legen ein Verfahren zum Umgang mit den Messengerdiensten im Betrieb fest, um folgende Aspekte zu klären:[8]
  - › Ziele für die Nutzung der Messengerdienste wie Wissensvernetzung, kooperatives Arbeiten Außendarstellung
  - › Soziales Kommunikationsverhalten (Netiquette)
  - › Verantwortlichkeiten der Führungskräfte und Beschäftigten
  - › Zuständigkeiten für offizielle Unternehmensdarstellung
  - › Zulässige/unzulässige Auswertung durch den Betrieb
  - › Selbstverantwortung der Führungskräfte und Beschäftigten und Haftung des Unternehmens für Mitarbeiteraktivitäten
  - › Maßnahmen des Gesundheitsschutzes (wie zum Beispiel Hilfestellung bei Überlastungsproblemen)
  - › Maßnahmen bei Verdacht auf Missbrauch
  - › Dienstliche und private Nutzung von Messengerdiensten
  - › Verhalten bei Konflikten und Schäden, Nichteinhaltung von Formvorschriften zum Beispiel für Geschäftsbriefe
- Die Führungskräfte sollten sicherstellen, dass im Umgang mit dem Messengerdiensten der Umgang mit personenbezogenen Daten vereinbart wird. Dies ist sowohl mit dem Messengerdienst als auch mit den beteiligten Führungskräften und Beschäftigten zu vereinbaren › *siehe Umsetzungshilfen 2.3.2 Datenschutz in 4.0-Prozessen; 2.3.4 Betriebs- und Dienstvereinbarungen zu 4.0-Prozessen*.
- Alle Führungskräfte und Beschäftigten sollten über das Ziel, die Funktion und den Nutzen der Messengerdienste informiert sowie im sicheren und gesundheitsgerechten Umgang unterwiesen werden. Dabei sollten die unterschiedlichen Affinitäten von Führungskräften und Beschäftigten zum Umgang mit den anderen technischen Assistenzsystemen und den Messengerdiensten berücksichtigt werden – gegebenenfalls einen Mentor einsetzen, zum Beispiel den Digital-Mentor › *siehe Umsetzungshilfe 2.1.8 Digital-Mentor („Kümmerer“)*.
- Gegebenenfalls sind Führungskräfte und Beschäftigte im Umgang mit technischen Assistenzsystemen und den Messengerdiensten zu qualifizieren beziehungsweise zu trainieren.

[8] Greve Wedde 2014, S. 132ff.

Quellen und weitere Informationsmöglichkeiten:

Astheimer, S., Freytag, B., Jansen, J., Müssgens, C., Mussler, H., & Preuss, S. (2018). *Whatsapp ist Arbeitgebern zu heiß*. FAZ. https://www.faz.net/aktuell/wirtschaft/diginomics/vom-diensthandy-entfernt-whatsapp-ist-deutschen-arbeitgebern-zu-heiss-15624643.html. Zugegriffen: 20.01.2019.

Brands, G., & Roellgen, C. B. (2016). *Sichere Kommunikation*. https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjqj5jx3_zfAhVCKVAKHbtmB1EQFjAAegQICBAC&url=http%3A%2F%2Fgilbertbrands.de%2Fblog%2Fwp-content%2Fuploads%2F2016%2F04%2FSichere-Kommunikation-Gilbert-Brands.pdf&usg=AOvVaw3LFnkcR7pzjtwRpA5Jj7EG. Zugegriffen: 20.01.2019.

BSI – Bundesamt für Sicherheit in der Informationstechnik (2019). *Messengerdienste beliebt aber nicht unbedenklich*. www.bsi-fuer-buerger.de. Zugegriffen: 20.01.2019.

Greve, S., & Wedde, P. (2014). Social-media-guidelines – Betriebs- und Dienstvereinbarungen. Frankfurt am Main: Bund Verlag.

Kruse-Brandao, T., & Wolfram, G. (2018). *Digital Connection. Die bessere Customer Journey mit smarten Technologien – Strategie und Praxisbeispiele*. Wiesbaden: Springer Gabler.

Schwarz, K. (2018). *Hacker erklären, welche Messenger-App am sichersten ist*. https://motherboard.vice.com/de/article/7xea4z/hacker-erklaren-welche-messenger-app-am-sichersten-ist. Zugegriffen: 21.01.2019.

Statista 2018 (Hrsg.). *Instant Messenger Statista Dossier, study ID 21661*. https://de.statista.com/statistik/daten/studie/873176/umfrage/nutzung-von-facebook-messenger-bots-durch-marketingverantwortliche-weltweit/. Zugegriffen: 13.02.2019.

Weitz, L. (2015): *WhatsApp & Co. Datenschutz bei Smartphone-Messengern*. https://www.uni-muenster.de/Jura.itm/hoeren/itm/wp-content/uploads/Vortrag-Datenschutz-bei-Smartphone-Messengern.pdf. Zugegriffen: 20.01.2019.

Zeit-online (2017). *Verbraucherschützer verklagen WhatsApp*. www.zeit.de/digital/datenschutz/2017-01/verbraucherzentrale-klage-whatsapp-datenweitergabe-facebook. Zugegriffen: 20.01.2019.

Datenschutzbeauftragter.info (2015). *WhatsApp und Datenschutz – Antworten auf die wichtigsten Fragen*. www.datenschutzbeauftragter-info.de/whatsapp-und-datenschutz-antworten-auf-die-wichtigsten-fragen/. Zugegriffen: 20.01.2019.

Zu diesem Thema könnten Sie auch folgende weitere Umsetzungshilfen interessieren:

- 2.1.2 Integration von intelligenter Software (inkl. KI) in die Organisation
- 2.1.8 Digital-Mentor („Kümmerer“)
- 2.2.3 Risikobetrachtung und IT-Sicherheit
- 2.3.1 Datensicherheit in 4.0-Prozessen
- 2.3.2 Datenschutz in 4.0-Prozessen
- 2.3.4 Betriebsvereinbarungen und Dienstvereinbarungen zu 4.0-Prozessen
- 2.6.1 Digitale Planung des Personaleinsatzes
- 3.2.2 Smartphone, -watch, -glasses
- 3.3.2 Gebrauchstauglichkeit der intelligenten Software (inkl. KI)

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