Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

# ARBEITEN IN DER DIGITAL VERNETZTEN WELT

Mittelstand-Digital Magazin
WISSENSCHAFT TRIFFT PRAXIS
Ausgabe 11

# Impressum

**Herausgeber/Redaktion:**
Begleitforschung Mittelstand-Digital
WIK GmbH
Rhöndorfer Straße 68
53604 Bad Honnef
HRB: Amtsgericht Siegburg, 7225
Tel. +49 (0)2224-9225-0, Fax +49 (0) 2224-9225-68
E-Mail: mittelstand-digital@wik.org
www.mittelstand-digital.de

**Verantwortlich:** Martin Lundborg
**Redaktion:** Peter Stamm
**Satz und Layout:** Karin Wagner



**Bildnachweis:**
Titel: auremar - fotolia
Seite 5: nutthaseth - fotolia
Seite 8/9/10: Mittelstand 4.0-Kompetenzzentrum Kaiserslautern/ A. Sell
Seite 12: SITRA Spedition GmbH, Fotograf:http://www.hoefemann.de/seite/business_impressum.html
Seite 20: Henry Krause
Seite 23: Stefan Veres
Seite 24: nd3000 - fotolia
Seite 32/34/35/36/37: Institut für Innovations- und Informationsmanagement GmbH
Seite 39: pixabay
Seite 45: Carlos Yudica - fotolia
Seite 50: Elnur - fotolia
Seite 56: enzozo - fotolia
Seite 66/68/69: IHK Siegen
Seite 67: Sonja Riedel
Seite 72: IHK Akademie OWL
Seite 77: ITA
Seite 83/85/86: LPS an der Ruhr-Universität Bochum
Seite 89: Gorodenkoff - fotolia

**Stand:** Januar 2019

**Druck:**
Medienhaus Plump GmbH
Rolandsecker Weg 33, 53619 Rheinbreitbach

**ISSN (Print) 2198-8544**
**ISSN (Online) 2198-9362**

Carsten Kunkel, Andreas Johannsen, Olga Kunkel

# Digitalisierung first – Beschäftigtendatenschutz second?

## Arbeiten 4.0 im Wandel – Herausforderungen und Empfehlungen für den Datenschutz

**Der Artikel befasst sich mit dem Beschäftigtendatenschutz im Zeitalter von Arbeiten 4.0. Anhand aktueller Praxisbeispiele werden nach einer einführenden Einordnung in den Gesamtkontext die konkreten technisch-organisatorischen Begebenheiten geschildert, diese rechtlich eingeordnet und analysiert, sodann Lösungsmöglichkeiten aufgezeigt und Empfehlungen ausgesprochen, gefolgt von einem abschließenden Fazit.**

### Einführung

Die Digitalisierung verändert das gesamte Lebensumfeld des Menschen, insbesondere seine Arbeitswelt.[1] Diese wird vernetzter und flexibler als je zuvor. Es entstehen neue Formen des Arbeitens, neue Arbeitsverhältnisse, neue Dimensionen des Wissenserwerbs, neue Technologien, die alle in sich sowohl Chancen als auch Risiken für Arbeitgeber und Arbeitnehmer bergen (Arbeiten 4.0). Dabei bedingen neue Technologien die Datenerhebung und den Datenaustausch in einem viel größeren Umfang und zwischen viel mehr Beteiligten als zuvor im „analogen Zeitalter". Unter den zahlreichen aktuellen Herausforderungen im Rahmen von Arbeiten 4.0 greift der vorliegende Artikel zwei repräsentative aktuelle Beispiele der Praxis auf. Er untersucht diese auf ihre rechtlichen sowie technisch-organisatorischen Implikationen und zeigt Lösungsansätze auf, die im Rahmen der Tätigkeit des „Mittelstand 4.0-Kompetenzzentrums IT-Wirtschaft" erarbeitet und empfohlen werden. Diese Empfehlungen orientieren sich insbesondere an der Sicht von IT-Mittelstandsunternehmen.

1 Vgl. Bauer/Hofmann (2018), S. 1 ff.

Hierbei handelt es sich um folgende Szenarien:

- Bring your own device, verstanden als die Möglichkeit der Beschäftigten, eigene Endgeräte auch beruflich zu nutzen (BYOD) sowie
- Digital Footprints, verstanden als die Möglichkeit des Arbeitgebers, durch das Sammeln von Daten unterschiedlichster Anwendungen und Geräte Profile seiner Beschäftigten zu erstellen (Profiling).

## Überblick über den neuen rechtlichen Rahmen des Beschäftigtendatenschutzes

Mit dem Inkrafttreten der Europäischen Datenschutz-Grundverordnung (im Folgenden – DSGVO) am 25. Mai 2018 hat der Datenschutz, und damit auch der Beschäftigtendatenschutz, eine umwälzende Veränderung erfahren: anstelle nationaler Datenschutzgesetze trat mit der DSGVO ein für die gesamte Europäische Union (EU) unmittelbar geltender einheitlicher Rechtsrahmen, der hohe Standards an die IT-Sicherheit und an den Schutz personenbezogener Daten setzt.

Ergänzend zu Vorschriften der DSGVO ist der Beschäftigtendatenschutz § 26 BDSG (in der Neufassung vom 30. Juni 2017) geregelt. Demnach dürfen personenbezogene Daten von Beschäftigten dann vom Arbeitgeber verarbeitet werden, wenn dies für Zwecke des Beschäftigungsverhältnisses erforderlich ist, also etwa zum Abschluss eines Anstellungsvertrags oder zur Erfüllung besonderer Pflichten aus einer Tarif- oder Kollektivvereinbarung. Dabei hat der Arbeitgeber für geeignete Maßnahmen zu sorgen, die die Einhaltung der in der DSGVO (insbesondere in Art. 5) vorgeschriebenen Grundsätze der Datenverarbeitung sicherstellen.

So fordert der Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c DSGVO die Beschränkung der Datenerhebung und -verarbeitung. In diesem Sinne ist das „Ausspionieren" der eigenen Beschäftigten (also über das zur Begründung und Durchführung eines Beschäftigungsverhältnisses erforderliche Maß hinaus) bereits wegen der Verletzung dieses datenschutzrechtlichen Grundsatzes offenkundig unzulässig. Zumal ein solches „Ausspionieren" einen schwerwiegenden Eingriff in die Persönlichkeitsrechte bedeuten kann, welcher neben dem allgemeinen Datenschutzrecht auch noch durch spezielles Recht, nämlich in Form des Straf- und Ordnungswidrigkeitenrechts, geschützt ist, etwa durch § 202a StGB, der das Ausspähen von Daten verbietet, oder § 202b StGB, der eine Freiheitsstrafe für das Abfangen von Daten „aus einer nichtöffentlichen Datenübermittlung" vorsieht.

Ferner sollen alle Datenverarbeitungsvorgänge transparent gestaltet werden, was eine heimliche Speicherung personenbezogener Daten unzulässig macht.

Zudem muss gemäß Art. 5 Abs. 2 DSGVO derjenige, der personenbezogene Daten verarbeitet, das nicht nur im Einklang mit der DSGVO tun, sondern dies auch jederzeit und in Bezug auf jeden Verarbeitungsvorgang nachweisen können. Die durch die Aufsichtsbehörden zu verhängenden Geldbußen sind in der DSGVO dabei so konzipiert, dass sie abschreckend wirken, und können bereits dann verhängt werden, wenn die Maßnahmen zum Schutz personenbezogener Daten nicht nachgewiesen werden können.

## „Bring Your Own Device" (BYOD)

In einem „Bring Your Own Device" (BYOD) Modell nutzen Beschäftigte ihre privaten Endgeräte (insb. Smartphones und Laptops) für berufliche Aufgaben.[2] Dabei gibt es einiges zu beachten, denn die Risiken sind immens: Durch Auswertung privater Endgeräte der Beschäftigten kann der Arbeitgeber leicht private Informationen einsehen (z. B. über Facebook-, Netflix- oder E-Mail-Zugang). Die Möglichkeiten des Überwachens und Ausspähens der Aktivitäten der Beschäftigten sind dabei technisch betrachtet beinahe unbegrenzt.[3]

### Szenario

Nehmen wir als Beispiel ein Software-Unternehmen, in welchem die Beschäftigten zumindest zu einem Teil ihre eigenen Smartphones und Tablets nutzen, die sie sowohl privat als auch beruflich einsetzen. Die mobilen Endgeräte sind praktisch ständig bei dem Nutzer, sie geben detaillierte Auskunft über dessen Persönlichkeit, zeichnen zum Teil auch biometrische Daten auf und bilden mittlerweile den Standard-Zugang zu sozialen Netzwerken. Mobile Endgeräte sind bereits aufgrund ihrer Mobilität schwer zu schützen, so dass sie leichter einem fremden Zugriff ausgesetzt sind als stationäre Geräte des Unternehmens. Dazu kommen noch teilweise ungeschützte Netze, wie z. B. an Flughäfen und in Bahnhöfen. Ferner ist der Zugriff der Unternehmensführung auf die privaten Informationen über Administratoren-Rechte der internen IT-Abteilung oder über das Backup-System des Unternehmens technisch möglich. Auch die Speicherkarten aus den Endgeräten der Beschäftigten können als Speicherort für sensible Daten (u. a. auch

2 Vgl. Kohne/Ringleb/Yücel (2015), S. 2 ff.
3 Vgl. ebenda, S. 36-37.

im Rahmen von Backups) genutzt werden, die jedoch besonders schutzbedürftig sind, da sie einerseits leicht aus dem Gerät entfernt und ausgelesen werden können und andererseits dem Zugriff anderer (auch unsicherer und unberechtigter) Anwendungen ausgesetzt sind. Erwähnenswert ist schließlich, dass Passwörter sowohl für betriebliche als auch für private Anwendungen beispielsweise unter Android im Klartext gespeichert werden und so vor einem unberechtigten Zugriff kaum geschützt sind.

## Analyse

*Technische Überlegungen*

Die Vorteile der heute gerade bei kleinen und mittleren IT-Unternehmen weit verbreiteten BYOD-Szenarien liegen auf der Hand:

- Für das Unternehmen reduzieren sich Anschaffungs- und Betriebskosten.
- Die Beschäftigten können nicht nur betriebliche Anwendungen nutzen, sondern haben potenziell eine große Auswahl an (persönlich präferierten und benutzerfreundlichen) Apps und Programmen jederzeit und an jedem Ort zur Verfügung, und müssen nicht zwei Geräte (ein dienstliches und ein privates) mit sich führen.

Somit erlaubt BYOD explizit eine Vielfalt, Flexibilität und Agilität im Hinblick auf die IT-Infrastruktur des Unternehmens. Dabei ist die Betreuung, Wartung und Sicherheit sowie Datenschutz-Konformität der Geräte genau wegen der Vielfalt an Plattformen und Produkten recht problematisch.

Andererseits ist bei Unternehmen ohne geregelte BYOD-Politik oder gar mit BYOD-Verbot empirisch ein erstaunlich hoher Grad an Vermischung von betrieblichen mit privaten Daten (z. B. Geburtstage, private Adressen, Termine, Notizen, E-Mails, Fotos und Filme) auf den ausschließlich betrieblichen Geräten festzustellen.

Die Nachteile von BYOD sind demgegenüber:

- Konflikte bei Trennung von privaten und Unternehmensdaten (z. B. bei Inanspruchnahme der Fernlösch-Funktion durch einen IT-Administrator, denn in der Praxis werden oft beide Datenarten gelöscht),
- Einschränkungen aufgrund der getroffenen Vereinbarungen und Auflagen für die Beschäftigten,
- Gefühl der Überwachung aufgrund der möglichen Kontrollen durch den Arbeitgeber,
- Technische Organisation deutlich schwieriger als bei unternehmenseigenen Geräten.

Insbesondere in Bezug auf die Trennung von Daten lässt sich anmerken, dass es zwar zahlreiche Container-Apps gibt, die technisch eine sichere Trennung zwischen den privaten und beruflichen Inhalten ermöglichen. Allerdings wird in der Praxis auf diese häufig verzichtet, weil sie bei Beschäftigten auf geringe Akzeptanz stoßen: Bei jedem Wechsel vom privaten in den Unternehmensbereich muss der Beschäftigte die Container-App starten und sich einloggen.

*Rechtliche Überlegungen*

Personenbezogene Daten sind solche, die eine natürliche lebende Person zumindest identifizierbar machen (vgl. Art. 4 Nr. 1 DSGVO). Sie umfassen zahlreiche Informationen, u. a. den Namen, das Geschlecht, Kenntnisse und Anschauungen, den Aufenthaltsort oder auch Passwörter, vgl. im Überblick Abbildung 1.

Bei der Verarbeitung, also grundsätzlich bei jedwedem Umgang mit personenbezogenen Daten (vgl. die weite Definition des Verarbeitungsbegriffs in Art. 4 Nr. 2 DSGVO), muss der Arbeitgeber die strengen Vorschriften der DSGVO und des § 26 BDSG sowie – innerhalb des Anwendungsbereichs des TKG, also im Bereich des eigenen Angebots von Telekommunikationsdiensten[4] – auch § 88 TKG einhalten.[5] In Bezug auf die „mitgebrachten" Geräte, die auch beruflich genutzt werden, lässt sich zunächst feststellen, dass eine Verarbeitung personenbezogener Daten der Beschäftigten aus dem Privatbereich ohne eine eindeutige freiwillige Einwilligung unzulässig ist.[6] Das zwingt den Arbeitgeber zur Trennung zwischen den beruflichen und privaten Inhalten der Beschäftigten, damit er auch den eigenen Pflichten

4 Anm.: So können sich Restriktionen für die Kontrollmöglichkeiten des Arbeitgebers aufgrund des Fernmeldegeheimnisses (§ 88 TKG) und der TK-Datenschutzvorschriften (§§ 91 ff TKG) ergeben. Diese bestehen allerdings nur, soweit die SIM-Card des Smartphones/Tabletts vom Arbeitgeber gestellt wird, da nur dann nach Ansicht der Literatur der Arbeitgeber als Diensteanbieter iSv § 3 Nr. 24 TKG zu behandeln sei, vgl. Conrad in: Auer-Reinsdorff/Conrad (2016), § 37 Arbeitsrechtliche Bezüge, Rn. 288-292 m.w.N. Hier weist die TK-rechtliche Bewertung Parallelen zur privaten E-Mailnutzung am Arbeitsplatz auf: Verwendet der Arbeitnehmer eine eigene SIM-Card, so sei das TKG, insbesondere § 88 TKG, nach überwiegender Auffassung nicht anwendbar. Auch seien §§ 11 ff. TMG nicht anwendbar, soweit der Arbeitnehmer mittels eines privaten Endgeräts private Apps zu dienstlichen Zwecken oder dienstliche Apps zu dienstlichen Zwecken nutze. Dahingegen habe der Arbeitgeber die Vorschriften des Datenschutzrechts z. B. hinsichtlich der Daten, die auf einem Endgerät des Arbeitnehmers gespeichert sind, zu beachten.

5 Vgl. Reiserer/Christ/Heinz (2018), S. 1501 ff.

6 Vgl. Kort (2018), S. 30.

sowohl hinsichtlich des Beschäftigtendatenschutzes als auch im Hinblick auf den Schutz unternehmensbezogener Daten nachkommen kann.[7]

Mögen also die technischen Möglichkeiten zur Überwachung von Beschäftigten bei der Nutzung der eigenen Geräte für berufliche Zwecke recht vielfältig sein, so bleibt die Privatsphäre eines jeden Beschäftigten doch grundsätzlich durch das Datenschutzrecht, sei es in Form des Straf- und Ordnungswidrigkeiten- oder etwa des Zivilrechts (mit seinen Möglichkeiten der Geltendmachung von Schadensersatzansprüchen gegenüber dem Arbeitgeber) geschützt[8, 9]. Dementsprechend muss die Geschäftsführung im Rahmen ihrer unternehmensinternen Compliance sicherstellen, dass entsprechende (personenbezogene) Daten den Privatbereich des Beschäftigten nicht verlassen und keineswegs verarbeitet werden.

7 Vgl. Conrad/Schneider (2011), S. 156.
8 Vgl. Kort (2018), S. 24 ff.
9 Anm.: So sind etwa im 15. Abschnitt des Strafgesetzbuches 10 Paragraphen (§§ 201 ff. StGB) dem Schutz des persönlichen Lebensbereichs eines Menschen gewidmet. Neben den bereits oben erwähnten Ausspähen und Abfangen von Daten ist bereits das Anschaffen von fremden Passwörtern zum Zwecke der Kenntnisverschaffung verboten (§ 202c StGB). Demnach wird derjenige, wer die Daten der Beschäftigten aus ihren privaten Endgeräten „ausspioniert" oder dies zumindest versucht, mit Freiheitsstrafe bedroht. Auch die zivilrechtlichen Möglichkeiten des Schadensersatzes sind nicht zu vergessen, etwa vertraglicher oder deliktischer Natur gem. §§ 280 ff. 823 ff.

Dafür bieten sich sowohl rechtliche als auch organisatorische und technische Lösungsmöglichkeiten, die nachstehend beleuchtet werden.

## Lösungsmöglichkeiten und Empfehlungen:

*Technische Lösungsmöglichkeiten*

Zu den technischen Möglichkeiten gehören vor allem Folgende:

- Sichere Passwörter
- Zugang zum Firmennetz über VPN-Verschlüsselung
- Black- und Whitelisting von Apps
- Löschung von Daten per Fernzugriff nach Diebstahl oder Verlust
- Verschlüsselung von Gerätespeichern und einzelnen Datenbereichen
- Container-Architekturen oder virtuelle Desktop-/Smartphone-Lösungen
- Privacy by Design/Privacy by Default
- Einführung eines Mobile Device Management Systems (MDM)
- Einführung eines Mobile Application Management Systems (MAM)

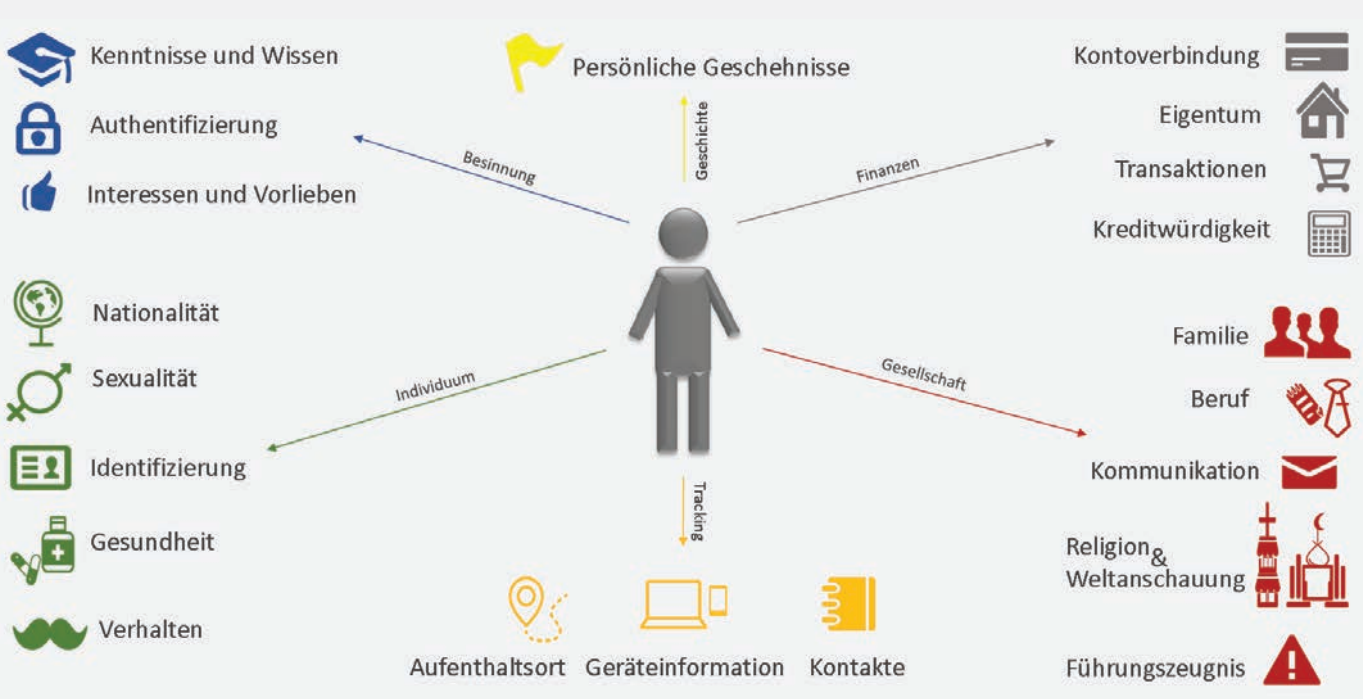



Abbildung 1: Überblick über die Arten der personenbezogenen Daten

Vorbildliche technische Lösungen für das mobile Arbeiten enthalten zunächst nach einer entsprechenden Beschäftigtensensibilisierung und technischen Schulungen die Verwendung von sicheren Passwörtern auf Basis eines Passwortmanagers. Softwareprodukte hierzu sind zahlreich vorhanden. Wichtig ist letztlich, dass alle Dienste und Anwendungen von allen Beschäftigten mit sicheren Passwörtern versehen werden.

Ferner sollten die Beschäftigten beim Arbeiten von unterwegs oder zuhause grundsätzlich mit sicheren VPN-Verbindungen (je nach VPN-Protokoll möglichst mit Verschlüsselung sämtlicher Netzwerkpakete) auf das Firmennetz oder über das Firmennetz auf das Internet zugreifen.

Nach wie vor eines der größten Probleme im Bereich des mobilen Arbeitens sind böswillige Apps, die z. B. das Adressbuch eines Endgeräts auslesen und an Dritte versenden. Hiergegen gibt es mittlerweile Software-Lösungen, die Apps prüfen, und über Blacklists „böse Apps" deaktivieren oder deinstallieren und „gute" bzw. geprüfte Apps über Whitelists im Firmennetz zulassen[10]. Dieser Softwaredienst sollte möglichst nicht von der eigenen Firmen-IT übernommen werden, sondern professionellen IT-Security-Dienstleistern übertragen werden.

Gehen mobile Geräte verloren oder werden sie gestohlen, stellt eine Löschung von Daten per Fernzugriff („enterprise wipe"/"selective wipe") durch entsprechende Security-Softwarelösungen für alle zuvor registrierten mobilen Geräte heute einen gängigen Standard dar[11].

Eine Maßnahme, die viele KMUs noch nicht umgesetzt haben, ist die Verschlüsselung von Gerätespeichern und einzelnen Datenbereichen (z. B. E-Mails, Kontakten, etc.). Auch hierzu ist eine Verschlüsselungssoftware anzuschaffen.

Grundsätzlich sind die oben aufgeführten Maßnahmen als Einzelmaßnahmen durchführbar, da sie einzeln auf jedem mobilen Gerät implementiert werden (auf Betriebssystemebene). Einen hohen und umfassenden sowie unternehmensweiten Schutz erlauben jedoch letztlich nur Änderungen, die die gesamte IT-Architektur betreffen. Solche sind bspw. Container oder virtuelle Desktops. Bei Containerlösungen (auch „Sandbox"-Lösungen genannt) wird auf den mobilen Geräten ein separater, geschützter Bereich eingerichtet, der alle betrieblichen Apps und Dienste beinhaltet[12]. Das Problem dieser technischen Lösungen ist oftmals jedoch, dass sie immer nur einen kleinen Teil aller Sicherheitsbedrohungen adressieren, die eine böswillige App auf einem Smartphone ausüben kann bzw. denen eine App auf einem Smartphone unterliegt. Überdies führt eine strikte technische Trennung des dienstlichen vom privaten Bereich häufig dazu, dass Beschäftigte den dienstlichen Teil ihres Smartphones als zu eingeschränkt und unpraktisch empfinden und daher nur für die notwendigsten Tätigkeiten nutzen. Den Großteil ihrer Tätigkeiten erledigen sie dann im uneingeschränkten privaten Teil. Das Ergebnis ist eine ungewollte Vergrößerung der Angriffsfläche für Sicherheitsbedrohungen[13].

Gerade im IT-Mittelstand fehlen oft die Ressourcen, um IT-Lösungen bereits vor der Installation auf Basis von klaren Sicherheitsanforderungen auszuwählen oder zu entwickeln. Gerade im mobilen Bereich muss jedoch der Datenschutz (DSGVO-Compliance) und die IT-Sicherheit trotz oder gerade wegen der Vielfalt an Betriebssystemplattformen (iOS, Android, Blackberry, Windows Mobile etc.) insbesondere im BYOD-Szenario künftig eine zentrale Stellung einnehmen. So kann z. B. bei der Entwicklung und Bereitstellung eigener Apps deren „Datenhunger" bereits in der Designphase dadurch minimiert werden, dass personenbezogene Daten nur dann einzugeben sind, wenn dies tatsächlich erforderlich ist („Privacy by Design").

Zu empfehlen ist ferner die Einführung eines Mobile Device Management Systems (MDM), auch Enterprise Mobility Management (EMM) genannt[14]. Dieses unterstützt und automatisiert zentral die Registrierung, Einbindung und Konfiguration von mobilen Geräten im Unternehmensnetz sowie das zentrale Update-Management der mobilen Applikationen. Diese Systeme integrieren heute weitgehend die oben beschriebenen Funktionen.

Allerdings bieten auch MDM-Systeme auf Ebene der Anwendungen und Inhalte i. d. R. nur eingeschränkte Sicherheitsfunktionalitäten. Daher ist die Einführung oder Komplettierung des MDM-Systems durch ein Mobile Application Management System (MAM) zu erwägen. Mithilfe von MAM-Systemen legen Administratoren zentral fest, auf welche Anwendungen die Nutzer und Nutzergruppen im betrieblichen Container des Geräts zugreifen können. Beispielsweise kann durch MAM-Software bei einem Nutzer, der entgegen der BYOD-Richtlinie und BYOD-Vereinbarung

10 Vgl. BITKOM (2014), S. 17.
11 Vgl. Leinfelder (2017), S. 3.
12 Vgl. Müller (2018), S. 544; Faber/Behnsen (2018), S. 63.
13 Vgl. BITKOM (2014), S. 18.
14 Vgl. BSI, Mindeststandard für Mobile Device Management nach § 8 Abs. 1 S. 1 BSIG – Version 1.0 vom 11.05.2017.

eine ungewollte App nutzt, eine Information per E-Mail oder auch eine sofortige Alert-Funktion auf sein Gerät gesendet werden.[15]

Abschließend sei darauf hingewiesen, dass Maßnahmenkombinationen in aller Regel sinnvoll sein dürften, z. B. die Verschlüsselung von Daten in der Container-App bei Umsetzung einer Sandboxlösung.

*Rechtliche Empfehlungen*

Aus Unternehmenssicht empfehlenswert ist es, einige Dokumente zu erstellen, die das BYOD-Modell unterstützen und dessen rechtskonformen Einsatz ermöglichen sollen.[16] Zu diesen Dokumenten zählt in erster Linie ein **IT-Betriebskonzept**, das u. a. die Möglichkeit des Einsatzes privater Endgeräte für betriebliche Aufgaben überhaupt erst begründet.

Ferner wäre eine **BYOD-Richtlinie** zu empfehlen. Dort sollten die Grundsätze des Modells dargestellt und einzelne für alle Beschäftigten geltende Aspekte definiert werden. So soll die Trennung privater Inhalte von beruflichen vorgegeben werden und eine oder mehrere Lösungen dazu (wie bspw. „Container" zur Unterteilung dieser Inhalte) gleich vorgeschlagen werden. Datenzugriff, Datenlöschung sowie der Einsatz von Kontroll- und Monitoringtools sollten ebenfalls Eingang in diese Richtlinie finden. Auch klare Verbote wie das Verbot der Nutzung des Endgeräts oder zumindest der dort vorhandenen Unternehmensanwendungen durch unbefugte Dritte oder das Verbot, ungeprüfte Anwendungen zu installieren, können und sollten in der Richtlinie vorgesehen werden. Die Pflicht der Beschäftigten, personenbezogene Daten anderer Personen, unter anderem auch ihrer Kollegen oder Kunden, nur nach der Weisung des Arbeitgebers zu verarbeiten, sowie den Verlust zu melden, gehören ebenfalls in die BYOD-Richtlinie. Hierbei gilt es grundsätzlich auch das Betriebsverfassungsrecht zu berücksichtigen, unterliegen doch derartige Ver- und Gebote regelmäßig der Zustimmung des Betriebsrates

Einzelne Aspekte der Nutzung des BYOD-Modells sollten (individual)vertraglich geregelt und technisch dem Vertrag entsprechend gestaltet werden (**BYOD-Nutzungsvereinbarung**). So könnte eine vertragliche Regelung getroffen werden, dass die Beschäftigten ihre Endgeräte regelmäßiger Kontrolle und Monitoring durch das Unternehmen unterziehen lassen. Während dieses Monitorings kann festgestellt werden, ob das Endgerät rechtskonform, u. a. auch im Einklang mit dem konkreten Vertrag zwischen dem Arbeitgeber und dem Beschäftigten, genutzt wird. Vertraglich sollte dann aber auch geregelt werden, wer die Kontrolle oder das Monitoring durchführt und wer den Zugang zu deren Ergebnissen erhält. Auch die Wahl geeigneter technischer Lösungen sollte im Vorfeld besprochen und sodann vertraglich vereinbart werden, damit der Arbeitgeber zwischen dem privaten Bereich seiner Beschäftigten und der beruflichen (und somit Unternehmens-)Sphäre unterscheiden kann. Bei einer vertraglichen Regelung ist jedoch besonders darauf zu achten, dass die Beschäftigten ihre Zustimmung zur Datenverarbeitung (Einwilligung) auch tatsächlich freiwillig erteilen: Insbesondere die bestehende Abhängigkeit der beschäftigten Person vom Arbeitgeber wird in vielen Fällen als Indiz gewertet, welches gegen eine Freiwilligkeit und somit für eine Unwirksamkeit der unterschriebenen Einwilligung spricht, vgl. § 26 Abs. 2 S. 1 BDSG[17]. Deswegen sollten hier auch andere Möglichkeiten der Beschäftigten, abweichende Lösungen vorzuschlagen oder bspw. einer konkreten Datenverarbeitung (bspw. dem Fernzugriff) zu widersprechen, für eine rechtskonforme Lösung berücksichtigt werden. Wird eine vorgefertigte „Einwilligung" vorgelegt und die Unterschrift faktisch erzwungen, bleibt die hierauf fußende Datenverarbeitung trotz dieses vorhandenen Dokuments rechtswidrig.

Zu berücksichtigen ist ferner, dass ein(e) Beschäftigte(r) grundsätzlich nicht dazu gezwungen werden darf, sein privates Smartphone dem Unternehmen zur Verfügung zu stellen und mit diesem seine beruflichen Aufgaben zu erfüllen.[18] Vielmehr ist das BYOD-Modell als Möglichkeit zu begreifen, mit dem eigenen Gerät beruflich zu arbeiten. Daraus ergibt sich auch das Recht des Beschäftigten, ein vom Unternehmen zur Verfügung gestelltes Gerät zu verlangen, wenn er sich nicht dem Monitoring und einer tiefergreifenden Kontrolle des Arbeitgebers hinsichtlich seines Privatgeräts unterwerfen will.

Abschließend lässt sich eine allgemeine Empfehlung formulieren: Sollte es technisch oder organisatorisch nicht möglich oder nicht umsetzbar sein, die privaten Endgeräte der Beschäftigten so zu administrieren, dass ihre private Kommunikation geheim bleibt, stellt das BYOD-Modell keinen rechtlich gangbaren Weg dar.

15 Anm.: Technisch gesehen gibt es bereits Lösungen, die unerwünschte Apps (gemäß Blacklist) auf Nutzergeräten automatisch wieder deinstallieren, hier ist allerdings im konkreten Einzelfall zu prüfen, inwiefern dies rechtlich zulässig ist.

16 Vgl. Monsch (2017), S. 29 ff.

17 Anm.: Die Regelbeispiele in § 26 Abs. 2 S. 2 BDSG können als Indiz gelten: So etwa die Gewährung wirtschaftlicher oder rechtlicher Vorteile für den Beschäftigten.

18 Vgl. Helfrich (2017), Rn. 68.

## Digital Footprints

Früher beschränkte sich die Verarbeitung personenbezogener Bewegungsdaten der Beschäftigten auf Arbeitszeitmessungen mittels einer Stempel- oder Stechuhr, die je nach Vertrag für die Entlohnung maßgeblich sein könnte oder kann. Mittlerweile jedoch arbeiten viele Beschäftigte (zumindest zeitweise) im Home Office oder von unterwegs[19]. Zudem ist im Zuge der Digitalisierung eine technische Vernetzung von allen möglichen Geräten etwa in Büro, Produktionshalle oder Privatwohnsitz Realität geworden. Vom Lichtschalter über die Kaffeemaschine im Pausenraum bis zur Parkplatzkamera kann alles als sogenannte „IoT-Lösung" (Internet of Things) über Internetverbindung an die zentrale Unternehmens-IT gekoppelt werden, so dass dadurch eine Unmenge von Daten – auch personenbezogenen Daten – gesammelt werden kann[20]. Das zweite Szenario untersucht daher die Überwachung des Beschäftigtenverhaltens in Bezug auf Orte und Räume sowie die damit einhergehende Möglichkeit zur Erstellung örtlicher Bewegungsmuster.

### Szenario

Auch im zweiten Szenario verbleibt es beim Beispiel eines Software-Unternehmens, in welchem die Geschäftsführung eine fortgeschrittene Digitalisierung im eigenen Betrieb vorleben möchte. Daher wurde die Zutrittskarte für das Firmengebäude technisch zu einer Public-Key-Infrastruktur-Karte (PKI-Karte) erweitert, die zunehmend weitere Funktionen übernimmt. Neben dem Zutritt zum Gebäude und zu bestimmten Server-Räumen wird sie für das Buchen und Freischalten von Sitzungsräumen mit entsprechender Videokonferenzsoftware, für die Nutzung der Firmendrucker, für das Bezahlen in der Kantine und an den Kaffeeautomaten in den Pausenräumen, sowie für das Einloggen von Rechnern und Personen in das lokale Netz (LAN) durch Stecken der PKI-Karten in die Notebooks verwendet. Weiterhin wird eine Social-Media-Software zur rechnerbasierten Kommunikation verwendet, die u. a. zeigt, wann man online ist, wann man „gechattet" oder „geskypt" hat. Ebenso werden hier Daten erhoben, von welchem Gerät und Netzsegment aus man kommunizierte, also beispielsweise ob der Standort das Büro oder der Privatwohnsitz des Beschäftigten war.

### Analyse

*Technische Überlegungen*

Die Fülle der im Szenario beschriebenen Bewegungs- und Verhaltensdaten sowie insbesondere die einfache technische Kombinierbarkeit dieser Daten auf Basis von simplen Auswertungs-Programmen („Skripten") der jeweiligen IT-Administratoren erfordert in der Regel die Einbindung des Betriebsrats und des Datenschutzbeauftragten des Unternehmens bei der Konzeption und Inbetriebnahme eines jeden Systems.

Bei der Entwicklung und Einrichtung derartiger Systeme kann eine Voll-Protokollierung der Bewegungsdaten technisch abgeschaltet werden, wo dies nicht erforderlich ist. Ebenso sollte darauf geachtet werden, dass der Personenkreis der IT-Administratoren, die eine Public-Key-Infrastructure betreiben, klein bleibt und zentral geführt wird. Bei einer Public-Key-Infrastruktur (PKI) werden vom IT-Administrator Zertifikate an die Beschäftigten vergeben und verwaltet. Die PKI basiert auf der Empfehlung X.509 der ITU-T21. Diese hat wiederum die ISO/IEC 9594-8:2017, Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks, geprägt22. Die IT-Administratoren sind entsprechend der Vorgaben zu schulen und zu zertifizieren.

*Rechtliche Überlegungen*

Wie bereits oben erwähnt, ist die Überwachung der Beschäftigten mittels Auswertung vorhandener technischer Lösungen datenschutzrechtlich unzulässig und kann sogar zu strafrechtlicher Haftung führen. Um die Vernetzung der Geräte dennoch sinnvoll nutzen und dadurch ggf. Energie- und/oder Betriebskosten weiter rechtskonform senken zu können, muss das Unternehmen dafür Sorge tragen, dass so gesammelte Daten entweder keinen Personenbezug mehr aufweisen, oder die Privatsphäre der Beschäftigten nicht verletzt wird. Bei der Implementierung (einer der) zahlreichen technischen Lösungen ist es somit notwendig, dem Grundsatz der „Privacy by Design" dadurch Rechnung zu tragen, dass derartige Informationen gleich bei ihrer Erhebung anonymisiert werden.[23] So sollten beispielsweise

19 Der Trend der Mitarbeiterführung zu mehr Selbstverantwortung ist in vielen Bereichen seit einigen Jahren gut erkennbar, vgl. Hebestreit (2015), S. 280.
20 Vgl. etwa zu Fragen der strafrechtlichen Haftung sowie zivilprozessualen Verwertbarkeit von Videoaufzeichnungen des Verkehrsraums Kunkel/Kunkel, jurisPR-StrafR 12/2018 Anm. 3 sowie Kunkel/Kunkel, jurisPR-Compl 4/2018 Anm. 4.
21 Telecommunication Standardization Sector innerhalb der ITU (International Telecommunication Union).
22 Vgl. Müller (2018), S. 546.
23 Die Totalüberwachung ist in Deutschland bereits seit dem Jahr 1983 aufgrund des sog. „Volkszählungsurteils" des Bundesverfassungsgerichts (BVerfG, Urt. v. 15. 12. 1983 – 1 BvR 209/83 u. a.) verboten.

die vorgenannten Zutrittskarten bei der Bedienung einer Kaffeemaschine oder beim Betreten allgemein zugänglicher Räume den jeweiligen Nutzer nicht (mehr) als konkrete Person identifizieren lassen (oder gar können), sondern lediglich als Angehörigen des Unternehmens. Liegt eine Anonymisierung vor, findet die DSGVO keine Anwendung mehr.

Dahingegen darf (und sollte aus Unternehmenssicht auch) etwa die Buchung von Konferenzräumen sowie die Zeiterfassung weiterhin personalisiert werden, ebenso wie (wohl regelmäßig) die Zugangskontrolle, da der Arbeitgeber hier ein berechtigtes Interesse an der Kenntnis haben dürfte, welche(r) Beschäftigte wie viele Stunden im Unternehmensräumen verbracht hat.[24] Vorsicht ist aber auch hier geboten, weil eine Zugangskontrolle ausschließlich zur Identifizierung des Beschäftigten verwendet werden (insoweit ein berechtigtes Interesse) und keinesfalls zur Erstellung von Bewegungsprofilen oder zur Kontrolle des Arbeitnehmerverhaltens allgemein führen darf.[25]

## Lösungsmöglichkeiten und Empfehlungen

*Technische Lösungsmöglichkeiten*

Denkbare technische Lösungen sind:

- Verschlüsselung der Bewegungsdaten
- Anonymisierung der Bewegungsdaten

Die erste technische Maßnahme ist die Umsetzung des Prinzips der Datensparsamkeit bei der Einrichtung der diversen IT-Systeme im Betrieb. Personenbezogene Daten werden, wo möglich, nicht persistent gespeichert. Weiterhin sollten nach sinnvollen Fristen bestimmte Daten automatisch gelöscht werden.

Dort, wo Daten erhoben und gespeichert werden müssen, kann durch Verschlüsselung der Daten einem Missbrauch entgegen gewirkt werden. Die Entschlüsselung sollte generell geeigneten Personen übertragen werden, in letzter Instanz dem Datenschutzbeauftragten.

Ebenso stellt die Anonymisierung der Daten eine Lösung dar. In Videomaterial sollten Personen im betrieblichen Kontext im Falle einer öffentlichen Nutzung des Materials ohne vorherige Einverständniserklärung grundsätzlich unkenntlich gemacht werden. Technisch ist dazu die Bildveränderung z. B. durch Cutting-Out/Blanking, Mosaik-Anonymisierung/Verpixelung, Kanten-Filter, Rauschen, das Anzeigen von Avataren oder die Veränderung des gesamten Bildes bzw. von Merkmalen (wie Firmenschildern im Hintergrund), die zur Identifikation führen, üblich[26]. Softwarelösungen, die dies automatisch vornehmen, sind auf dem Markt noch nicht verbreitet. Eine Integration in die Software Security-Suites der IT-Anbieter ist ebenso noch im Forschungsstatus. [27]

*Rechtliche Empfehlungen*

Aus rechtlicher Perspektive empfehlen sich auch hier – wie bereits im ersten Szenario – sowohl interne **Richt- oder Leitlinien** zum Umgang mit personenbezogenen Daten als auch individuelle Aufklärung oder, wenn nötig, **(individual)vertragliche Regelung** bestimmter Bereiche. Da jegliche Datenerhebung und -verarbeitung stets dem datenschutzrechtlichen Transparenzgebot unterliegt, mit Ausnahme von Fällen, wo ausreichende Hinweise auf eine Straftat vorliegen, müssen die Beschäftigten vom Arbeitgeber darüber informiert werden, welche Daten dieser verarbeitet und zu welchem Zweck dies geschieht. Die Mannigfaltigkeit technischer Lösungen gebietet die Berücksichtigung persönlichkeits- sowie datenschutzrechtlicher Vorschriften bereits beim Bestellen oder Inauftraggeben von Hard- und Software. Im Falle von (einzuholenden) Einwilligungen der Beschäftigten muss eine detaillierte maßnahmenbezogene Aufklärung vorausgehen sowie die Möglichkeit gegeben werden, die Einwilligung zu verweigern. Dabei ist jede Prüfung der Erforderlichkeit und der Angemessenheit konkreter technischer Lösungen stets so zu führen, dass diese auch nachweisbar ist.

## Fazit

Das geltende europäische und deutsche Recht mit den zahlreichen neuen Regelungen zielt im Grunde darauf ab, dass der Arbeitgeber nur dann personenbezogene Daten von Beschäftigten erheben und verarbeiten darf, wenn dies für die Zwecke des Beschäftigungsverhältnisses erforderlich und angemessen ist. Sowohl eine Dauerüberwachung von Leistungen oder vom Verhalten der Beschäftigten als auch der Eingriff in die Sphäre des „rein Persönlichen" sind grundsätzlich verboten. Es empfiehlt sich für alle mittelständische Unternehmen, ein Dokument, etwa eine Leitlinie, zum Beschäftigtendatenschutz – ggf.

24 Vgl. Kort (2018), S. 27.
25 Vgl. Byers (2016), S. 54.
26 Vgl. Volkmann et al. (2016), S. 413-426.
27 Vgl. FhG IOSB (2018).

unter Einbeziehung des Datenschutzbeauftragten – zu erstellen, das zumindest Folgendes klar und eindeutig festlegt:

- Heimliche Kontrollen sind ausgeschlossen,
- Bewegungsprofile werden nicht erstellt, eine Lokalisierung der Beschäftigten ist nur in absoluten Ausnahmefällen (die je nach Betrieb sehr unterschiedlich und die auch einzeln aufzuzählen sind) zulässig,
- Eine Dauerüberwachung des Arbeitsverhaltens ist ausgeschlossen,
- Biometrische Daten werden ausschließlich zur Autorisierung und Authentifizierung genutzt und sonst separat gespeichert und zusätzlich geschützt,
- Psychologische Profile werden nicht erstellt,
- Grundlegende Änderungen bezüglich der Verarbeitung personenbezogener Daten von Beschäftigten werden nur mit der Zustimmung des Betriebsrates durchgeführt und vor der Durchführung transparent dargestellt.

Eine transparente Information über die Datenverarbeitung sowie eine vertraglich saubere Regelung der Datenerhebung unter Berücksichtigung der Freiwilligkeit der Einwilligung und Wahrung der Privatsphäre der Beschäftigten erlauben es Unternehmen, die Arbeitswelt von morgen bereits heute rechtskonform zu bereiten: Von der Nutzung privater Smartphones der Beschäftigten über die IT-gestützte Nutzung von Licht und Heizung bis hin zur Kaffeemaschine – alles kann und darf verbunden und vernetzt werden, allerdings nur dann, wenn die durch eine solche Datenerhebung gewonnenen Informationen rechtskonform verwendet werden. Ein hoher Grad an Selbstverantwortung, positive Atmosphäre und Berücksichtigung konkreter Interessen von Beschäftigten stiften auch den Unternehmen schließlich wesentlich mehr Nutzen, als eine ohnehin rechtlich nicht begründbare (Total)Überwachung ihrer Beschäftigten.

**Literatur**


Auer-Reinsdorff, A. / Conrad, I., Handbuch IT- und Datenschutzrecht, 2. Auflage, München 2016

Bauer, W. / Hofmann, J., Arbeit, IT und Digitalisierung, in: Arbeit 4.0 – Digitalisierung, IT und Arbeit: IT als Treiber der digitalen Transformation, hrsg. v. J. Hofmann, Wiesbaden 2018

BITKOM, Apps & Mobile Services – Tipps für Unternehmen, 2. Aufl., Berlin 2014

Byers, P., Mitarbeiterkontrollen, Praxis im Datenschutz und Arbeitsrecht, München 2016

Conrad, I. / Schneider, J., Einsatz von „privater IT" im Unternehmen - Kein privater USB-Stick, aber „Bring your own device" (BYOD)?, ZD 2011, S. 153 ff.

von Faber, E. / Behnsen, W., Joint Security Management: organisationsübergreifend handeln, Wiesbaden 2018

FhG IOSB, Privatsphäre und Datenschutz – dank intelligenter Videoüberwachung, Presseinformation, 08.05.2018

Forgó, N. / Helfrich, M. / Schneider, J., Betrieblicher Datenschutz, 2. Auflage, München 2017

Hebestreit, N., Die Verantwortung des Wirtschaftsakteurs: Eine vertragstheoretische Betrachtung, Wiesbaden 2015

Kohne, A. / Ringleb, S. / Yücel, C., Bring your own Device: Einsatz von privaten Endgeräten im beruflichen Umfeld – Chancen, Risiken und Möglichkeiten, Wiesbaden 2015

Kort, M., Neuer Beschäftigtendatenschutz und Industrie 4.0, RdA 2018, S. 24 ff.

Kunkel, C. / Kunkel, O., Verbotsirrtum bei einer ordnungswidrigen Datenschutzverletzung durch fortlaufende Videoaufzeichnungen des Verkehrsraum, jurisPR-StrafR 12/2018 Anm. 3

Kunkel, C. / Kunkel, O., Zivilprozessuale Verwertbarkeit von Videoaufzeichnungen des Verkehrsraums durch sog. Dashcams, jurisPR-Compl 4/2018 Anm. 4

Leinfelder, A., Zwischen Cybersecurity und DSGVO - Enterprise Mobility Management wird unverzichtbar, in: itsecurity, www.it-daily.net, Nov. 2017, S. 2-3

Monsch, C., Bring Your Own Device (BYOD), Berlin 2017

Müller, K.R., IT-Sicherheit mit System, 6. Aufl., Berlin 2018

Reiserer, K. / Christ, F. / Heinz, K., Beschäftigten-Datenschutz und EU-Datenschutz-Grundverordnung, DStR 2018, S. 1501 ff.

Schmidt, M.G.; Gaentzsch, F.; Pohlmann, N., Mobiles Arbeiten & Bring Your Own Device (BYOD), Dozentenhandbuch, Task Force „IT-Sicherheit in der Wirtschaft", Mainz 2014

Volkmann, L. F.; Zimmermann, C.; Sester, S.; Wehle, L.; Becker, B.: Digitale Tarnkappe: Anonymisierung in Videoaufnahmen, in: H. C. Mayr, M. Pinzger (Hrsg.): INFORMATIK 2016, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, S. 413-426, Bonn 2016

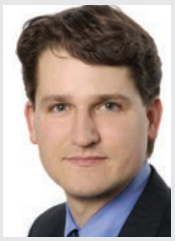
Die Technische Hochschule Wildau und die Technische Hochschule Brandenburg sind Konsortialpartner im Mittelstand 4.0-Kompetenzzentrum IT-Wirtschaft. Zu den Themen dieses Kompetenzzentrums zählen u. a.:

- Laborversuche zur Erprobung neuester Technologien für Arbeit 4.0
- Information und Unterstützung beim Einsatz von Softwareschnittstellen für vernetztes Arbeiten
- IT-Sicherheit und Datenschutz

*www.itwirtschaft.de*

Mittelstand 4.0
Kompetenzzentrum
IT-Wirtschaft

## Autoren



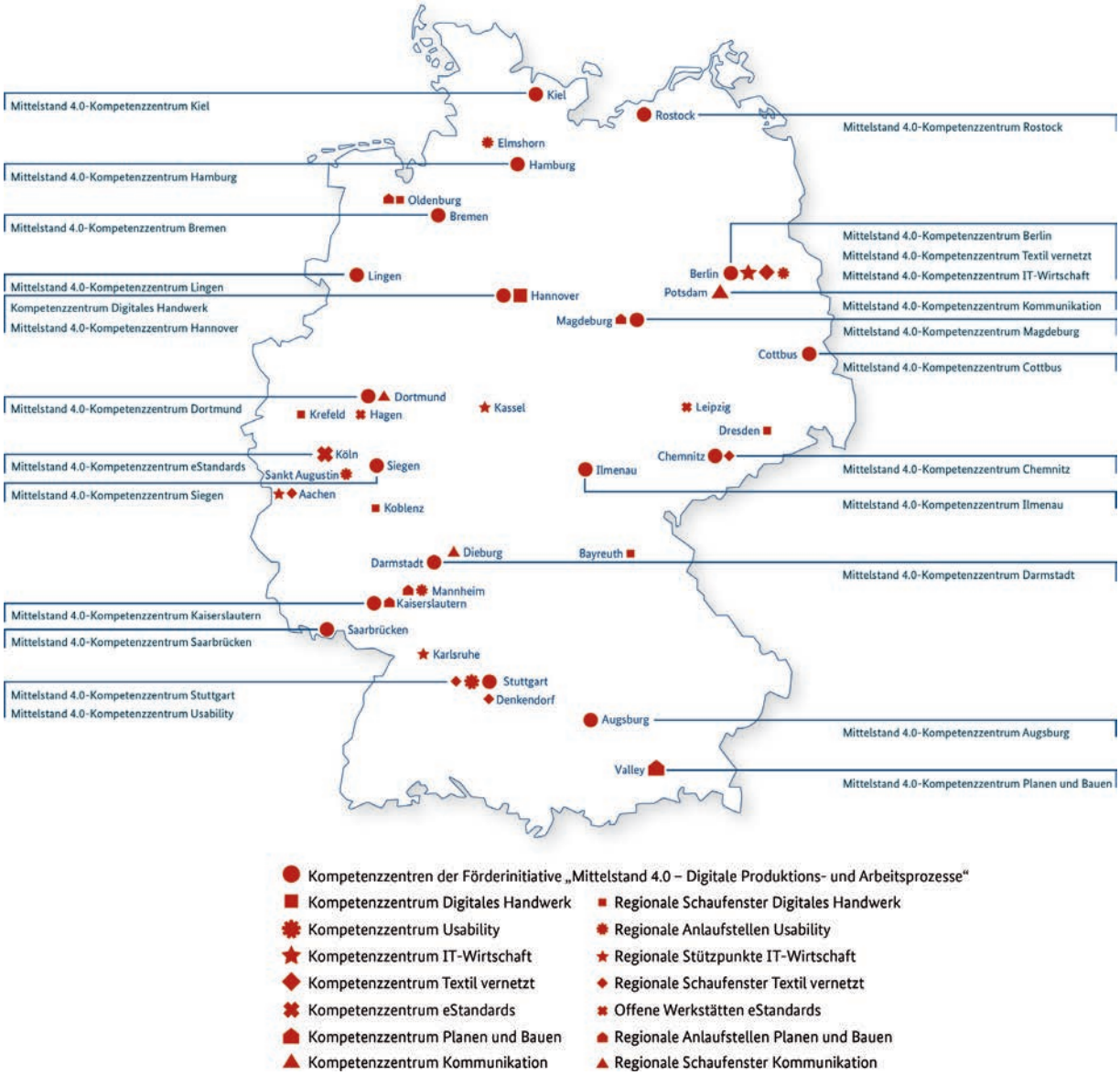
**Dr. iur. Carsten Kunkel** ist Professor für Wirtschaftsrecht, insb. Gesellschaftsrecht, an der TH Wildau. Dort unterrichtet er neben dem Wirtschaftsrecht u. a. auch Vertragsgestaltung, Datenschutzrecht und Compliance. Vor seiner Berufung im Jahr 2011 war er mehrere Jahre als Rechtsanwalt in Berlin, Frankfurt a. M. und London tätig, u. a. in großen international agierenden Kanzleien, sowie als Geschäftsführer und Projektleiter im Bereich der Erneuerbaren Energien. Seit Dezember 2017 ist er u. a. als Leiter des Bereichs „Rechtliche Rahmenbedingungen" des Mittelstand 4.0-Kompetenzzentrums IT-Wirtschaft tätig.

**Dr. rer. oec. Andreas Johannsen** ist Professor für Systementwicklung und -Integration" an der TH Brandenburg. Vor seiner Berufung studierte er Betriebswirtschaft in Tübingen und Edinburgh und war u. a. Projektmitarbeiter in einem Hypermedia-Projekt der Fraunhofer Gesellschaft Darmstadt, wissenschaftlicher Mitarbeiter an der Universität Hohenheim in Stuttgart sowie Berater für SAP CRM, CIM („Consumer and Industrial Products") und Enterprise Applications Consulting. Seit 2007 ist er Inhaber der Johannsen Management Consulting (JMC) in Berlin. Im Mittelstand 4.0-Kompetenzzentrum IT-Wirtschaft verantwortet er mit seinem Team die Bereiche „IT-Sicherheit" und „Schnittstellen und Interoperabilität".

**Olga Kunkel** ist wissenschaftliche Mitarbeiterin des Mittelstand 4.0-Kompetenzzentrums IT-Wirtschaft und dort für rechtliche Rahmenbedingungen zuständig. Nach dem Abschluss ihres Jurastudiums in Russland war sie in mehreren internationalen Rechtsanwaltskanzleien überwiegend im Bereich Gesellschafts- und Kapitalmarktrecht tätig, bevor sie im Jahr 2014 ihr Studium an der juristischen Fakultät der FU Berlin abgeschlossen hat. Sie unterrichtet u. a. Compliance und M&A-Geschäfte an der FOM und promoviert zurzeit an der FU Berlin im Bereich gesellschaftsrechtlicher Compliance.

# Übersichtskarte der Mittelstand 4.0-Kompetenzzentren und -Agenturen

Stand: Januar 2019




Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. 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.mittelstand-digital.de

ISSN (Print) 2198-8544
ISSN (Online) 2198-9362