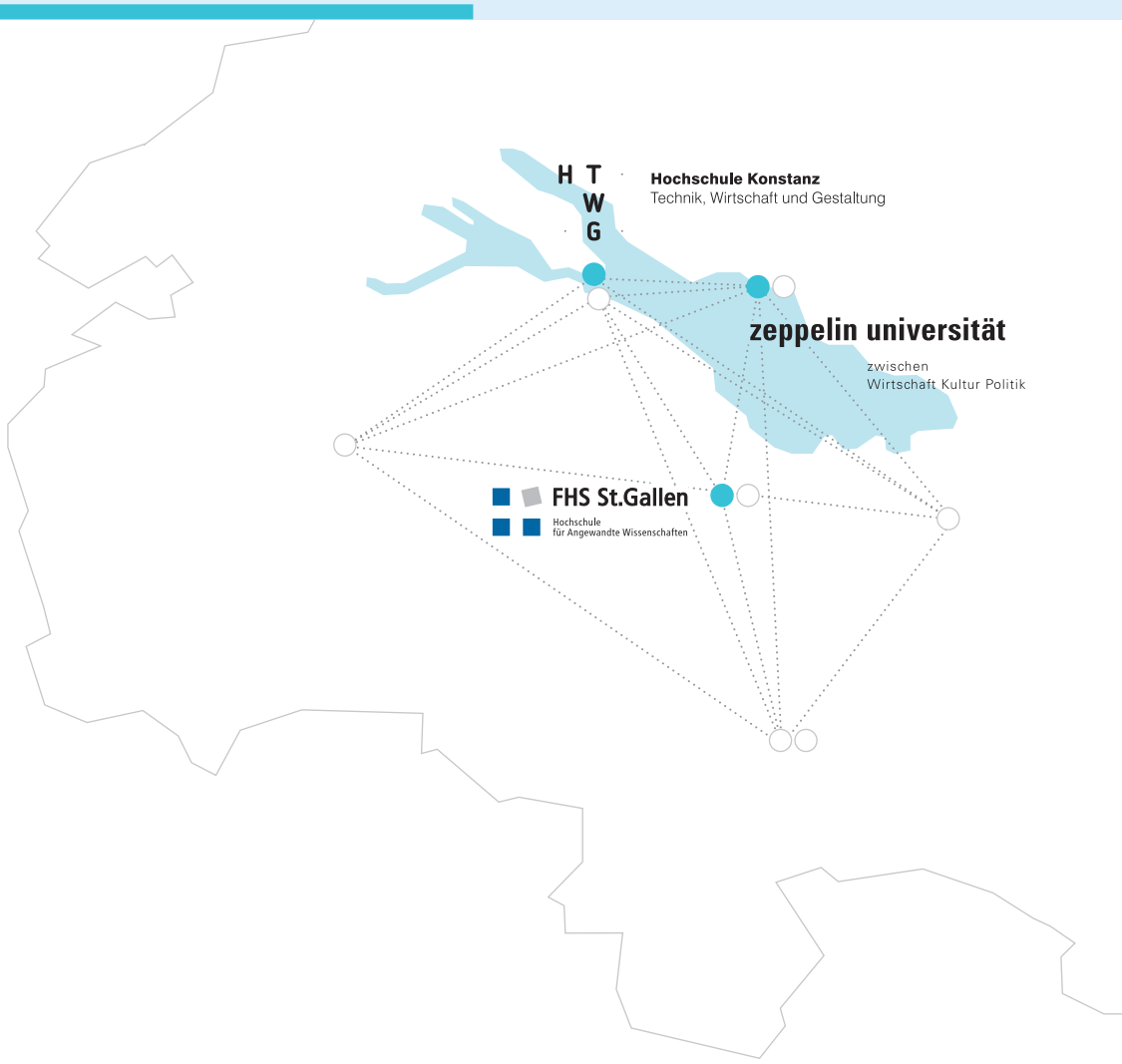
KMU digital

Internationale Bodensee Hochschule Labs



WEISSBUCH 2019

Digitale Agenda Bodensee [DAB]

Digitalisierung für KMU in der Bodenseeregion – Handlungsempfehlungen Politik, Personal und Recht

Vorwort

Liebe Leserinnen, liebe Leser,

die aktive Zusammenarbeit zwischen Bildung, Forschung und der Praxis ist eine der zentralen Faktoren, um die Wettbewerbs- und Zukunftsfähigkeit der Bodenseeregion zu sichern und auszubauen. Insbesondere die Entwicklung und Schaffung von Akzeptanz für technologische und gesellschaftliche Innovationen spielen dabei eine zentrale Rolle. Nicht zuletzt konnte sich die Bodenseeregion sowohl als Spitzenregion für Innovation als auch als führende Wissenschafts- und Hochschulregion etablieren.

Um diese Positionierung noch weiter zu stärken und auszubauen, hat die Internationale Bodensee-Hochschule (IBH) gemeinsam mit der Internationalen Bodensee Konferenz (IBK) und dem Interreg-Programm Alpenrhein-Bodensee-Hochrhein die IBH-Labs ins Leben gerufen. Die IBH-Labs sollen Lösungen für die Bewältigung gesellschaftlicher Herausforderungen in der Bodenseeregion durch die Kooperation von Forschung und Praxis schaffen und implementieren.

Gleichzeitig zeigt sich aber auch, dass Individuallösungen zwar einzelne Akteure weiterbringen, wir in der Bodenseeregion aber zudem an den politischen Rahmenbedingungen arbeiten müssen, um solche Lösungen breit zu integrieren und gesellschaftlich wirksam zu machen.

Genau in dieser Herausforderung liegt der grosse Gewinn des Projekts Digitale Agenda Bodensee, das Teil des IBH-Lab KMUdigital ist: Durch die Analyse, sowohl der Bedürfnisse von kleinen und mittleren Unternehmen (KMU) in der Region, als auch der regionalen und überregionalen Strukturen und Förderprogramme zur Digitalisierung von Unternehmen konnte das Projektteam gemeinsam mit einer Vielzahl von Unternehmen, Wirtschaftsförderern, Kammern, Verwaltung und Politik Empfehlungen dazu herausarbeiten, wie sich die Bodenseeregion noch besser aufstellen kann, um ihre Zukunftsfähigkeit im Wettbewerb mit anderen europäischen und globalen Regionen weiter auszubauen.

Diese teils sehr konkreten Handlungsempfehlungen, gepaart mit Umsetzungsvorschlägen, sind nun im vorliegenden Weissbuch aufbereitet. Um diese Empfehlungen mit Leben zu füllen, werden die Ergebnisse auch in einer Reihe von Veranstaltungen und Gesprächen mit verantwortlichen Akteuren diskutiert und zur Umsetzung gebracht.

Als IBH begleiten wir diesen Prozess der Implementierung gerne und sind überzeugt, dass das Weissbuch eine Anleitung für das politische und wirtschaftliche Handeln in der Bodenseeregion werden wird.

Ich wünsche Ihnen viel Spass bei der Lektüre,
Markus Rhomberg

Prof. Dr. Markus Rhomberg ist Leiter der Geschäftsstelle der Internationalen Bodensee-Hochschule IBH

Editorial

Auf dem Weg vom Grün- zum Weissbuch entwickeln wir Lösungsansätze zu den aufgeworfenen Fragestellungen. Dabei erfahren nicht nur unsere Inhalte Veränderung, sondern angesichts der rasant fortschreitenden Digitalisierung auch der Dialog in den verschiedenen Medien.

Das Interesse, die Neugier sowie die mit der Digitalisierung verbundenen Sorgen prägen Wirtschaft, Politik und Gesellschaft. Die Diskussion verläuft differenzierter, vielfältiger, konkreter und ist je nach Inhalt auch hier und da von Ermüdungserscheinungen geprägt.

Bisher zu optimistische Einschätzungen der Möglichkeiten und Nutzenwirkungen technologischen Fortschrittes werden zunehmend um einen sachlich-reflektierten Dialog angereichert. Beispiele sind Darstellungen von systematischen Fehlleistungen künstlicher Intelligenz, das wachsende Bewusstsein um „Störgeräusche“ im Hoffnungsmeer grosser Datenmengen oder die Frage, wessen Rechte etwa durch Targeting verletzt werden.

Das Bewusstsein in Wirtschaft und Gesellschaft steigt, dass neben Chancen auch die bestehenden Sorgen in Unternehmen sowie der Gesellschaft ernst genommen und aufgegriffen werden müssen. Dies ist insbesondere dann nötig, wenn wir eines Tages die verschiedenen Etappen der digitalen Transformation als nachhaltigen Erfolg verbuchen wollen.

Den Dialog über die Digitalisierung und über Visionen unseres künftigen Zusammenlebens und Arbeitens gilt es fortzusetzen. Wir wünschen Ihnen eine anregende und interessante Lektüre unseres Weissbuches.

Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die gewählte männliche Form schliesst eine adäquate weibliche Form gleichberechtigt ein.

Von links nach rechts: Christopher Köhler, Prof. Dr. Michael Scharkow, Prof. Dr. Marc Strittmatter, Laura Heintz, Abdullah Redzepi, Manuel Treiterer (nicht auf dem Bild: Prof. Dr. Sibylle Olbert-Bock)

Inhaltsübersicht

Projektumfeld 05

Digitalisierungsszenarien 2030 – zurück in die Zukunft 08

Handlungsempfehlungen 10

Politische Rahmenbedingungen und Handlungsempfehlungen 12
- Digitale Politikfelder innovativ gestalten 12
- 5G braucht es (auch) an jeder Milchkanne 12
- Digitale (Weiter-)Bildung als Schlüssel für ein digitales Unternehmen 14
- Ohne Sicherheit kein Vertrauen 15
- Digitaler Staat: Verwaltungsaufwand für Unternehmen reduzieren und digitalisieren 16
- Wirtschaft vernetzen: Aber bitte nicht nur die Maschinen 17

Personalpolitische Rahmenbedingungen und Handlungsempfehlungen 20
- Personalfunktion: ein Zukunftsmodell? 20
- Szenarien in der Gestaltung von HRM 21
- Hohe Technologisierung und Selbstorganisation als mögliche Strategie 22
- Neue Rollen des HRM: Handlungsfelder zur beispielhaften Realisierung 23
- HR hat Nachholbedarf in puncto digitaler Kompetenz 27
- Ansatzpunkte einer Digitalkompetenz bezogen auf HR 28

Rechtliche Rahmenbedingungen und Handlungsempfehlungen 34
- Daten mit Personenbezug 35
- Daten als Asset 41
- IT-Sicherheit 46
- Cyber-Physische Systeme 51
- Cloud-Computing und digitale Plattformen 53
- Branchenspezifische Sachverhalte 58

Verbindende und trennende Elemente der Digitalisierung im Bereich Politik, Personal und Recht 60
- Daten in Kooperationsbeziehungen 60
- Digitale (Weiter-)bildung als Basis digitaler Kompetenzen 62

Fazit 64

Literaturverzeichnis 66

Glossar 74

Impressum 76

Die im Text *kursiv gesetzten Begriffe* werden im Glossar erklärt.

Die Internationale Bodensee-Hochschule IBH
30 Hochschulen – 4 Länder – 1 Verbund

Die IBH ist der grösste hochschulartenübergreifende Verbund Europas. Sie ermöglicht die Zusammenarbeit von 30 Hochschulen aus Deutschland, dem Fürstentum Liechtenstein, Österreich und der Schweiz in Forschung, Lehre und Transfer. Die IBH unterstützt grenzüberschreitende Forschungsprojekte zu gegenwärtigen und zukünftigen Herausforderungen für den Bodenseeraum. Sie koordiniert den Dialog zwischen Wissenschaft und Praxis, fördert den wissenschaftlichen Nachwuchs, ermöglicht Innovationen in der Lehre und unterstützt gemeinsame Angebote der Hochschulservices. Mit ihren Projekten leisten die IBH und ihre Mitgliedshochschulen einen international sichtbaren Beitrag für das regionale Innovationssystem Bodensee.

Weitere Informationen zur Arbeit der IBH finden Sie unter:

www.bodenseehochschule.org

Projektumfeld

Die IBH-Labs

Auf Initiative der Internationale Bodensee-Hochschule (IBH) und der Internationalen Bodensee Konferenz (IBK) wurden IBH-Labs ins Leben gerufen. Hierbei handelt es sich um Forschungs- und Innovationsnetzwerke von Hochschulen und Praxispartnern aus Wirtschaft und Gesellschaft. Sie leisten einen nachhaltigen Beitrag zur Förderung des Wissens-, Innovations- und Technologietransfers und damit zur Standortattraktivität der Bodenseeregion. Die Förderung der IBH-Labs erfolgt aus Mitteln des Interreg V-Programms «Alpenrhein-Bodensee-Hochrhein».

Für die Internationale Bodensee-Hochschule bilden die IBH-Labs einen strategischen Schwerpunkt. Die thematische Ausrichtung der IBH-Labs orientiert sich an regional relevanten Themen und den Entwicklungspotenzialen der Bodenseeregion.

Die IBH-Mitgliedshochschulen starteten 2017 gemeinsam mit Praxispartnern folgende IBH-Labs:

- IBH Living Lab Active & Assisted Living
- IBH-Lab KMUdigital
- IBH-Lab Seamless Learning

Das IBH-Lab KMUDigital – Kompetenznetzwerk für Digitalisierung bei KMU

Das IBH-Lab KMUdigital unterstützt kleine und mittlere Unternehmen (KMU) in der Bodenseeregion bei der Bewältigung, Umsetzung und Implementierung der rasant fortschreitenden industriellen Digitalisierung.
Sieben Konsortialpartner aus drei Ländern erarbeiten dafür anwendungsorientierte Antworten auf die Fragen:

- Wieviel Digitalisierung muss in die KMU?
- Wieviel Digitalisierung passt zu den KMU?

Die Bodenseeregion als einer der wettbewerbsfähigsten und dynamischsten Wirtschaftsstandorte Europas zeichnet sich durch innovative Weltmarktführer, mittelständische Unternehmen und insbesondere KMU aus. Durch den digitalen Wandel wachsen die Anforderungen an die Unternehmen, aus denen sich insbesondere für KMU Problemstellungen ergeben:

- Wie sehen adäquate Digitalisierungsstrategien für KMU aus?
- Wie können die Anforderungen an eine zukünftige Produktion erfüllt werden?
- In wieweit sind Organisationsstrukturen und Führungsmodelle anzupassen?
- Welche neuen Erwerbsquellen ergeben sich?
- Wie können KMU Innovationen vorantreiben?
- Welche politischen, rechtlichen und personalpolitischen Rahmenbedingungen müssen angepasst werden?

Digitalisierung findet, meist getrieben von weltweit agierenden Grossunternehmen und wissenschaftlichen Einrichtungen, bereits in vielen Bereichen des Lebens statt. Das IBH-Lab KMUdigital bündelt die vorhandene Expertise rund um den See, um die Chancen und Auswirkungen für die KMU der Region ganzheitlich zu untersuchen. Dies betrifft den digitalisierten Produktionsvorgang an sich (Shopfloor), den Einfluss auf Geschäftsprozesse, den Wandel vom Produkt- hin zum Dienstleistungsanbieter; die Aus- und Weiterbildung sowie die Betrachtung der Rahmenbedingungen. Das IBH-Lab KMUdigital besteht aus sechs Einzelprojekten:

- Digitale Agenda Bodensee (DAB)
- Nutzenbasierter Digitalisierungsnavigator (DigiNav)
- Internationale Musterfabrik Industrie 4.0 (i4Production)
- Data Science (Data4KMU)
- Digital Transformation Guide (DigiTraG)
- Digitale Landwirtschaft (DigiLand)

Digitale Agenda Bodensee

Die Digitalisierung wirkt sich sowohl auf organisatorische Bereiche, wie die Personalqualifizierung, die Gewinnung von Fachkräften und Organisationsstrukturen, als auch auf die Unternehmensumwelt, wie beispielsweise politische und rechtliche Rahmenbedingungen aus. In dem Einzelprojekt Digitale Agenda Bodensee sollen genau diese Herausforderungen mit den relevanten Stakeholdern umfassend bearbeitet werden.

Darauf aufbauend sollen Rahmenbedingungen entwickelt werden, um den KMU eine bestmögliche Infrastruktur für Innovationen, intelligente Weiterbildungsmassnahmen und eine erfolgreiche digitale Transformation bieten zu können. Die aktive Gestaltung dieser Rahmenbedingungen gelingt über einen interdisziplinären und länderübergreifenden Wissensaustausch der beteiligten Hochschulen und insbesondere im engen Dialog mit den KMU.

Projektpartner:

- Zentrum für Politische Kommunikation an der Zeppelin Universität (Prof. Dr. Michael Scharkow, Dr. Dennis Lichtenstein, Christopher Köhler, Malcolm Schmidt, Frederic Denker, Claire Perrot-Minot und Laura Heintz)
- FHS St.Gallen, Hochschule für Angewandte Wissenschaften (Prof. Dr. Sibylle Olbert-Bock, Abdullah Redzepi)
- Hochschule Konstanz Technik, Wirtschaft und Gestaltung (HTWG) (Prof. Dr. Marc Strittmatter, Manuel Treiterer, Nicole Neubrander, Philipp Kopka, Thilo Jansch, Miriam Ebinger)

Der Weg vom Grün- zum Weissbuch

LAUFZEIT DES PROJEKTS DIGITALE AGENDA BODENSEE: 1. JANUAR 2017 BIS 31. DEZEMBER 2019

Abbildung 1: Projektablauf

Das im Herbst 2018 veröffentlichte Grünbuch „Digitale Agenda Bodensee – Eine Bestandsaufnahme zum Potenzial der Digitalisierung innerhalb KMU in der Bodenseeregion“ stellt sowohl die Grundlage als auch die weiterführende Arbeitsbasis für dieses Weissbuch dar.

Die Ergebnisse des Grünbuches wurden vom Projektteam über verschiedene Wege weiterentwickelt und präzisiert. Es wurden hierfür insgesamt vier Workshops mit relevanten Stakeholdern aus Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft sowie zahlreiche Interviews in Deutschland, Österreich und der Schweiz durchgeführt.

Die Essenz der gesammelten Informationen bestimmt nun den Inhalt dieses Weissbuches. Es soll den handelnden Akteuren Anregungen, Gestaltungsoptionen und Handlungsempfehlungen in den Bereichen Politik, Recht und Personal zur Unterstützung der Digitalisierung von KMU an die Hand geben.

Die Anregungen, Gestaltungsoptionen und Handlungsempfehlungen sind zum einen direkt an die handelnden Akteure innerhalb der KMU adressiert. Zum anderen sollen sie den politischen und intermediären Akteuren als Handreichung für mögliche zukünftige Bemühungen im Bereich der Digitalisierungsunterstützung von KMU dienen.

Digitalisierungsszenarien 2030 – zurück in die Zukunft

Welche möglichen Auswirkungen könnte die Digitalisierung auf die Bodenseeregion als Gesellschafts- und Wirtschaftsregion bis ins Jahr 2030 haben? Dieser Frage sind wir mit relevanten Akteuren aus Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft in einem Szenario-Workshop im Juni 2018 nachgegangen. Szenarien sind in diesem Zusammenhang mögliche zukünftige Entwicklungen in Bezug auf eine bestimmte Fragestellung. Auf Basis dieser Zukunftsbeschreibungen können Herausforderungen identifiziert und Lösungen entwickelt werden. Die einzelnen Szenarien haben ganz unterschiedliche Eintrittswahrscheinlichkeiten: Bei einem Szenario-Workshop geht es darum, alle möglichen Szenarien zu entwickeln und nicht nur solche mit der höchsten Eintrittswahrscheinlichkeit.

Für den Szenario-Workshop wurden im Vorfeld zwei Triebkräfte festgelegt. Die erste Triebkraft beschreibt zwei Akteure, welche die Digitalisierung hauptsächlich treiben können: Zum einen die Politik und zum anderen der Markt. Die zweite Triebkraft beschreibt die Reichweite der Digitalisierung. Entweder werden nur Teilbereiche digitalisiert oder es erfolgt eine gesamtgesellschaftliche Digitalisierung. Diese Triebkräfte bilden dann anhand der Achsen das Koordinatensystem wie in Abbildung 2 dargestellt. Dadurch entstehen vier Felder. Die Teilnehmenden wurden in vier Gruppen aufgeteilt und entwickelten anhand dieser vier Felder vier grundlegende Szenarien und die dazu passenden Prinzipien und eventuelle Trade-offs für diese Prinzipien.

Die Felder und dazugehörigen entwickelten Szenarien sind die folgenden:

1. Digitalisierung wird in Teilbereichen politisch getrieben: politisch initiierter Flickenteppich
2. Digitalisierung wird in Teilbereichen vom Markt getrieben: selbstorganisierte Teilmärkte
3. Digitalisierung wird gesamtgesellschaftlich politisch getrieben: politisch gesteuerte digitale Transformation
4. Digitalisierung wird gesamtgesellschaftlich vom Markt getrieben: digitaler Wilder Westen

Die Abbildung 2 stellt die Arbeitsergebnisse der Gruppen dar und will damit zum Nachdenken anregen: Über die (möglichen) Auswirkungen der Digitalisierung in der Bodenseeregion bis ins Jahr 2030 und insbesondere über die möglichen Szenarien, welche auf diesem Weg eintreten könnten.

Einige gesicherte Erkenntnisse über die politischen, organisationalen und rechtlichen Rahmenbedingungen in Bezug auf die Unterstützung der Digitalisierung von kleinen und mittleren Unternehmen (KMU) werden in den folgenden Kapiteln vorgestellt.

POLITIKGETRIEBEN

Politisch initiierter Flickenteppich

Prinzip: „Stärken stärken“
… und zwar insbesondere in den Kernbereichen bzw. Branchen der Bodenseeregion wie z. B. Industrie, Tourismus und Landwirtschaft

Tradeoff: „Schwächen werden ignoriert“
… da nur in die Stärken investiert wird. Schwächere Bereiche oder Branchen werden ignoriert bzw. aufgegeben

Politisch gesteuerte digitale Transformation

Drei häufig genannte, mögliche Szenarien und ihre Tradeoffs:
1. Politik reagiert bzw. läuft hinterher
   Tradeoff: Politik ist zu langsam und verpasst Trends
2. Politik überreguliert
   Tradeoff: Politik ist eher ein Bremsklotz für digitale Innovationen (Verbots- statt Ermöglichungskultur)
3. Politik reagiert bis zum Tag X gar nicht und dann schlagartig
   Tradeoff: Positive Entwicklungen werden (lange) nicht gefördert und Negative (zu) lange toleriert

TEILBEREICHE

GESAMTGESELLSCHAFTLICH

Selbstorganisierte Teilmärkte

Prinzip: „Digital Champions in digitalisierungsintensiven Branchen“
… da durch die Digitalisierung Profit / Gewinn maximiert werden kann
… Unternehmen ersetzen den Staat als Produzent digitalisierungsrelevanter Güter (wie z. B. Infrastruktur und Bildung)

Tradeoff: „Politische Akteure haben keinerlei Gestaltungsmacht mehr im Bereich der Digitalisierung“

Digitaler Wilder Westen

Prinzipien:
1. „Winner takes it all“
2. „Survival of the fittest“

Tradeoff: Es verlieren immer und überall die Schwachen / Langsamen / Ressourcenabhängigen

MARKTGETRIEBEN

Abbildung 2: Digitalisierungsszenarien der Bodenseeregion bis 2030

Handlungsempfehlungen

Politische Handlungsempfehlungen

1. Flächendeckend mindestens 10.000 Mbit/s (5G) Breitbandverfügbarkeit in der Stadt und auf dem Land: → s. S. 12 ff.
2. Life Long Learning – digitale Bildung muss schon in der Schule beginnen und insbesondere die Unterstützungsangebote im Bereich der digitalen Weiterbildung müssen vermehrt gefördert und attraktiv gestaltet werden, um den Fachkräftebedarf decken zu können: → s. S. 14 f.
3. Intensive Verbesserung der staatlichen Cyberabwehr und Cybersicherheit: Daten sind das höchste Gut der vierten industriellen Revolution: → s. S. 15 f.
4. Einführung einer Verschlüsselungspflicht bei der Übertragung sensibler Daten: → s. S. 16
5. Intensivierung der externen Beratung im Bereich der IT-Sicherheit: → s. S. 16
6. Signifikante Reduzierung des Verwaltungsaufwandes für Unternehmen durch die digitale Abwicklung administrativer Tätigkeiten: → s. S. 16 f.
7. Weitere (finanzielle) Förderung von Vernetzungsmöglichkeiten von Unternehmen mit anderen relevanten Akteuren aus Wirtschaft, Wissenschaft und Zivilgesellschaft. Diese Förderangebote sollten möglichst transparent, niederschwellig und innerhalb der *Bodenseeregion* international koordiniert sein bzw. werden: → s. S. 17 f.

Personalpolitische Handlungsempfehlungen

1. Geschäfts-, Personal- und Technisierungsstrategie sind gemeinsam zu denken und in Einklang zu bringen: → s. S. 20 ff.
2. Kernprozesse des Human Ressource Managements (HRM) – v. a. Rekrutierung, Kompetenzmanagement und Personalentwicklung – sind durch gezielte und kompetente Nutzung von Human Ressource Tech (HR-Tech) zu ergänzen, administrative HRM-Prozesse sind maximal zu optimieren: → s. S. 26 ff.
3. Arbeitsort, Arbeitsplatz und Arbeitszeit sind zeit- und bedarfsgerecht sowie flexibel auszugestalten, Chancen zu nutzen und Gegenmassnahmen zu riskanten Entwicklungen zu ergreifen: → s. S. 26 ff.
4. Arbeitsgegenstände und -inhalte sowie Zusammenarbeitsformen im Zuge der Leistungserbringung sollten für die Ausführenden Sinn stiften: → s. S. 26 ff.
5. Die technologische Transformation erfordert eine menschenzentrierte Gestaltung der Unternehmenskultur, wenn auf den Mensch als Wettbewerbsfaktor gesetzt werden soll: → s. S. 28
6. HR-Fachkräfte und HR-Führungskräfte müssen ihre Digitalaffinität erhöhen und ihre Digitalkompetenz steigern, um technologische Anwendungen in ihrem Bereich verstehen und begreifen zu können: → s. S. 28 ff.
7. HR-Fachkräfte und HR-Führungskräfte müssen Daten mittels Analytics und künstlicher Intelligenz im HR-Anwendungskontext verstehen und zielgerichtet nutzen können: → s. S. 30 ff.

Rechtliche Handlungsempfehlungen

1. Handlungsempfehlung an politische Akteure und Verbände: Bei kleinen und mittleren Unternehmen (KMU) besteht ein dringender Bedarf für praxisnahe rechtliche Orientierungshilfen. Es ist geboten, ein Problembewusstsein für rechtliche Herausforderungen in den Unternehmen zu schaffen. Gleichzeitig sollten ausreichend Informationen bereitgestellt werden, um zumindest einen ersten, strukturierten Abgleich zwischen Digitalisierungsbestrebungen und potenziell einschlägigen Rechtsproblemen bewerkstelligen zu können. Der Informationszugang sollte niederschwellig möglich sein, damit dafür keine Spezialisten eingekauft werden müssen (Orientierung).

2. Handlungsempfehlungen an KMU zu übergeordneten rechtlichen Herausforderungen:

2.1 Personenbezogene Daten: Für eine Sicherstellung der Einhaltung datenschutzrechtlicher Vorschriften ist für KMU die Entwicklung eines Datenschutz-Management-Systems (DMS) langfristig empfehlenswert. Hierfür kann die Einbindung qualifizierter, externer Berater zumindest im Anfangsstadium zielführend und effizient sein. Insbesondere sollten die datenschutzrechtlichen Anforderungen an rechtskonformes Webtracking und Cloud Computing sowie diese bei der Vernetzung von Systemen beachtet werden: → s. S. 35 ff.

2.2 Daten als Asset: Faktische „Datenherrscher“ sollten sich vergegenwärtigen, wo im Unternehmen welche Daten erfasst werden (siehe erste Ebene „Datenerzeugung“ in Abbildung 15 und Abbildung 16). Hieran anschliessend sollte die Kritikalität anfallender Daten hinsichtlich ihrer strategischen Nutzen- und Risikopotenziale bewertet werden. Eine nach diesen Fragen ausgerichtete Datenkartierung gibt Aufschluss über die erforderliche Intensität der vertraglichen Bindung etwaiger Partner: → s. S. 41 ff.

2.3 IT-Sicherheit: Auf Grundlage des vorhandenen Rechtsrahmens lassen sich die rechtlichen Anforderungen an die IT-Sicherheit grob in (1) ordnungsrechtliche und (2) gesellschaftsrechtliche Anforderungen sowie (3) vertragsrechtliche Nebenpflichten und (4) IT-Sicherheit „by design“ unterteilen. KMU sollten sich einen Überblick darüber verschaffen, welche Pflichten ihnen aus diesen Bereichen erwachsen: → s. S. 46 ff.

2.4 Cyber-physische Systeme (CPS) / The Internet of Things: In der Praxis bieten diese Systeme potenziell beachtliche Effizienzvorteile. Neben den technischen Herausforderungen bei ihrer Implementierung werfen sie auch eine Reihe von Rechtsfragen auf. Da sich diese Fragen insbesondere mit der Haftung für eventuelle Fehler des Systems befassen, sind sie nicht nur für Nutzer von CPS relevant, sondern auch für deren Kunden und Geschäftspartner: → s. S. 51 ff.

2.5 Cloud-Computing und digitale Plattformen: KMU sollten bei der Verwendung von Cloud-Computing besonders rechtliche Fragen mit Bezug zum Vertrags-, Urheber- und Datenschutzrecht berücksichtigen. Als Intermediär für Transaktionen ist ausserdem die Frage relevant, welche wettbewerbsrechtlichen Regelungen, vertragsrechtliche und datenschutzrechtliche Pflichten den Betreiber einer digitalen Plattform treffen. Für KMU ist hieran anknüpfend relevant, welche Ansprüche Unternehmen gegen Plattformbetreiber bei Pflichtverletzungen geltend machen können: → s. S. 53 ff.

Politische Rahmenbedingungen und Handlungsempfehlungen

Digitale Politikfelder innovativ gestalten

Politische Rahmenbedingungen im Bereich der *Digitalisierung* sind vielfältiger Natur. Sie beinhalten gesetzliche Regelungen, finanzielle Unterstützung und die Herstellung von Netzwerken und Kooperationen. Zudem befinden sich all diese Rahmenbedingungen in verschiedenen thematischen Bereichen. In der *Bodenseeregion* überschneiden sich länderübergreifend fünf Themenbereiche der politischen Unterstützung. Diese sind:

1. Infrastruktur
2. Bildung
3. Ordnungs- und Rechtsrahmen
4. Verwaltung
5. Wirtschaft

Durch eine Online-Befragung von insgesamt 115 kleinen und mittleren Unternehmen (KMU) wurde deutlich, dass für die Bodensee-KMU in Deutschland, Österreich und der Schweiz grundsätzlich all diese Themenbereiche hochrelevant sind.

Diese und weitere Analyseergebnisse aus der Befragung wurden über mehrere Wege verifiziert: Zum einen wurden verschiedenartige, thematisch detaillierte Workshops mit den relevanten Stakeholdern aus Politik, Intermediäre, Wirtschaft, Wissenschaft und Zivilgesellschaft durchgeführt. Zum anderen dienten die gesammelten Erkenntnisse anschliessend als Grundlage für Einzelinterviews mit Politikern, KMU und Intermediärevertretern (z. B. Wirtschaftsförderer) aus Deutschland, Österreich und der Schweiz.

Die folgenden Unterkapitel fassen diese gewonnenen Erkenntnisse zusammen und entwickeln Handlungsempfehlungen für die politischen Akteure, um die KMU in Deutschland, Österreich und der Schweiz im Bereich der *Digitalisierung* zu unterstützen.

„Unsere Gesellschaft hat in den letzten paar tausend Jahren extrem viel Wissen angesammelt und das verhält sich alles wie eine e-Funktion. Und heute steigt einfach die Komplexität, weil die Kombinationsmöglichkeiten massiv zunehmen. Auf einmal explodiert in allen Bereichen das Wissen [...]. Da kommen ganz viele verschiedene Technologien und die lassen sich alle wiederum miteinander kombinieren."

(CEO eines deutschen Start-ups in der IT-Branche)

5G braucht es (auch) an jeder Milchkanne

Im Bereich der digitalen Infrastruktur fehlt es nach wie vor an geeigneten Netzen für angemessene Datenübertragungsraten. Dies gilt sowohl für den (W)LAN Bereich, als auch für das Mobilfunknetz. Dieses Problem wird insbesondere innerhalb der Befragung deutlich: Von insgesamt 16 nach der Relevanz für das eigene KMU zu beurteilenden Rahmenbedingungen werden die ersten beiden Plätze von nötigen Massnahmen im Bereich der Infrastruktur belegt.

Dies ist nicht sonderlich überraschend, wenn ein jeder sich häufig schon freut, wenn auf dem

Display des Smartphones eine mobile Datenübertragungsrate von 3G angezeigt wird. Entspannung tritt jedoch häufig erst ein, insofern mindestens einmal ein „H“ (für High Speed Packet Access – HSPA) aufleuchtet. Dieses latente Gefühl, dass vermutlich jeder kennt, der sich nicht dauerhaft in den „Bodenseemetropolen“ wie z. B. Konstanz, Romanshorn oder Bregenz mit hervorragender Netzabdeckung aufhält, ist nachvollziehbar. So garantiert 3G eine maximale Downloadrate von 0,384 Mbit/s. HSPA hingegen ist im Optimalfall mit 7,2 Mbit/s fast 20-mal so schnell. Ganz zu schweigen von LTE (300 Mbit/s), 4G (1000 Mbit/s bzw. 1 Gbit/s) und dem nun geplanten 5G (10 Gbit/s). Tatsache ist aber, dass vor allem in ländlichen Gebieten der *Bodenseeregion* teilweise gar keine mobile Datenverbindung möglich ist oder der Buchstabe „E“ (für Edge, 0,256 Mbit/s) aufleuchtet. Aber sind wir ehrlich: Das „E“ steht in diesem Zusammenhang bei der heutigen Komplexität von Webseiten und Apps eher für Endstation.

Diese Betrachtung hat selbstverständlich einen ernsten und realen Hintergrund: Gerade die *Bodenseeregion* lebt von ihren starken Wirtschaftsunternehmen und insbesondere vom wirtschaftlichen Rückgrat der Region – den KMU. Viele dieser Unternehmen sind jedoch nicht direkt in Ballungszentren ansässig, sondern eben in ländlicheren Regionen.

Die Branche Landwirtschaft trägt den Regionstypus sogar schon im Namen und gerade in dieser Branche sind viele KMU in der *Bodenseeregion* tätig. Aber egal ob ein KMU in der Landwirtschaft oder als Hidden Champion in der Industrie tätig ist – die so häufig beschworene Allzweckwaffe wirtschaftlicher Prosperität im vierten industriellen Zeitalter – die Industrie 4.0 – basiert auf einer modernen digitalen Infrastruktur. Maschinen sollen gleichzeitig Arbeit verrichten, Daten generieren, diese Daten verarbeiten und analysieren und auf Basis dieser Analyse relevante Informationen an andere Maschinen oder Systeme weitergeben. Und das ganze natürlich in Echtzeit und nicht nur mit zwei Maschinen und Systemen, sondern mit einer vielfachen Anzahl derselben. Für diese Anforderungen genügt eben eine Datenübertragungsrate im Bereich von 3G und 4G nicht – wie sollte sie auch, wenn bei solchen Übertragungsraten schon der HD-Stream der Tagesschau Probleme bereitet.

Damit die Unternehmen die Herausforderungen der *Digitalisierung* meistern und die gleichermassen vorhandenen Chancen nutzen können, sind Datenübertragungsraten im 5G-Bereich Pflicht. Und zwar sowohl im Bereich des (W) LAN als auch im Bereich des mobilen Internets. In der Stadt und auf dem Land ist eine Netzabdeckung von 100 % der Fläche notwendig.

In der *Bodenseeregion* zeigt sich hier namentlich in Deutschland ein massiver Handlungsbedarf, der sowohl von den KMU als auch von den Wirtschaftsförderungen artikuliert wird. Bezeichnend ist hierfür das Zitat eines Schweizer Vertreters im Bereich der Wirtschaftsförderung und Vernetzung. Er wirkt auf die Frage nach der aktuell zur Verfügung stehenden Breitbandinfrastruktur in der Schweizer *Bodenseeregion* erleichtert und kann mit einem Augenzwinkern sa-

gen, dass diese sehr gut sei, denn „da haben wir Glück und wohnen auf der richtigen Seite vom Bodensee“ (Wirtschaftsförderer Grossraum St. Gallen). Belegt wird diese Aussage zudem durch zwei Vertreter aus Wirtschaftsförderung und Politik, welche sowohl für die ländlichen Bodenseeregionen als auch das bodenseenahe Allgäu mangelhafte Datenübertragungsraten beklagen.

Es sollte also klar sein: Es darf in diesem Punkt keine weiteren Kompromisse oder Verzögerungen geben. 5G muss schnellstmöglich der Minimalstandard einer ordentlichen digitalen Infrastruktur werden. Dies muss in der Stadt und auf dem Land geschehen und zwar besser gestern als heute.

„Breitband und Glasfaser ist ein sehr aktuelles Thema bei den KMU. Immer mehr vereinzelte Unternehmen kommen auf uns als Gemeinde und Wirtschaftsförderer zu mit dem Wunsch, dass schnellere Geschwindigkeiten zur Verfügung stehen müssen.“

(Wirtschaftsförderer in einer ländlichen Gemeinde in der Bodenseeregion)

Digitale (Weiter-)Bildung als Schlüssel für ein digitales Unternehmen

Bildung ist seit jeher ein wichtiger Faktor für die wirtschaftliche Performanz von Ländern und Regionen. Diese Tatsache hat sich auch im digitalen Zeitalter nicht verändert. Ganz im Gegenteil: Personen müssen immer flexibler einsetzbar sein und somit Wissen aus ganz verschiedenen Bereichen ansammeln, um für Unternehmen wertvoll zu sein. Um auch nachhaltig wertvoll zu bleiben sind (digitale) Weiterbildungsangebote unerlässlich.

Die politischen Akteure sind also auf nationaler und föderaler Ebene angehalten, Formate der digitalen Bildung bereits in den Schulunterricht zu integrieren. Fächer wie Informatik dürfen nicht erst als Wahlfach in höheren Klassenstufen angeboten werden, sondern sollten spätestens mit Beginn der weiterführenden Schule Pflichtfach sein. Natürlich benötigt es dafür auch die jeweilige digitale Infrastruktur in den Schulen. Es ist aber nicht damit getan, dass die gute alte Tafel gegen ein interaktives Whiteboard und das Schulheft gegen ein Tablet getauscht werden. Die Lehrkräfte müssen spezialisiert ausgebildet werden, um digitale Inhalte auch entsprechend vermitteln zu können.

Diese schulische digitale Bildung ist speziell für KMU hochrelevant, da viele Mitarbeitende direkt aus der Schule zu diesen Unternehmen gehen, um dort eine Ausbildung zu beginnen. Die Frage ist dann: Bringen diese Personen relevante digitale Kenntnisse bereits mit oder müssen diese erst innerhalb der beruflichen Ausbildung vermittelt werden? Letzteres kostet Zeit und Geld – beides sind insbesondere in KMU knappe Ressourcen.

Neben der schulischen Bildung ist es auch immens wichtig, die vorhandenen Mitarbeitenden fachgerecht und auf eine digitalisierte Wirtschaft hin weiterzubilden. Diese Weiterbildungen sollten

für KMU seitens der Politik gefördert werden. Des Weiteren muss zuvorderst auch der Ausbau von digitalen Weiterbildungsmöglichkeiten vorangetrieben und von Seiten der Politik gefördert werden. So können die Mitarbeitenden berufsbegleitend praxisrelevante, digitale Kompetenzen erwerben, ohne dass die Unternehmen auf sie für mehrere Tage oder Wochen vollständig verzichten müssen. Flexibles Life-Long-Learning ist aus Sicht der Bodensee-KMU hier das Gebot der Stunde. Diese Ansicht teilen zudem alle befragten Experten aus Wirtschaft, Politik und Intermediäre länderübergreifend in Deutschland, Österreich und der Schweiz.

Das Life-Long-Learning kann auch der entscheidende Faktor für das Abmildern des Fachkräftemangels sein. Die KMU in der *Bodenseeregion* konkurrieren um die schlausten (digitalen) Köpfe mit multinationalen Konzernen, welche in den allermeisten Fällen Wettbewerbsvorteile bei einer möglichen Anstellung dieser neuen Mitarbeitenden besitzen. Da sich dies kurz- bis mittelfristig nicht ändern wird, sind es insbesondere Weiterbildungsprogramme des bereits in den KMU vorhandenen Personals, welche einen positiven Einfluss auf das digitale Know-how haben können.

Die Unterstützung und Förderung von digitalen Weiterbildungsangeboten muss demnach eine zentrale Säule bezüglich der politischen Rahmenbedingungen im Bereich der Bildung innerhalb der Bundesländer und Kantone der *Bodenseeregion* darstellen.

„Ich brauche zukünftig andere Mitarbeiter als ich sie heute habe. Ich brauche andere Kompetenzen und ich brauche andere Fähigkeiten. [...] Diese Mitarbeiter zu finden oder so umzustellen, finde ich eine grosse Herausforderung."

(Wirtschaftsförderer Grossraum St.Gallen)

„Die wichtigste Sache sehe ich im Bereich des Personals und da geht es um Wissen, Know-how und Aus- und Weiterbildung."

(Wirtschaftsförderer in Vorarlberg)

Ohne Sicherheit kein Vertrauen

Neben der digitalen Infrastruktur ist das Thema Cybersicherheit aktuell in aller Munde. So trat u. a. 2018 in Deutschland die Datenschutz-Grundverordnung (DSGVO) in Kraft.

Trotzdem mussten wir im Verlauf des Projektes immer wieder feststellen, dass es gerade im Bereich des Ordnungs- und Rechtsrahmens teils immense Unsicherheiten auf Seiten aller Beteiligten gibt.

Die Bodensee-KMU haben den Wunsch geäussert, gerade im Bereich der Cybersicherheit vermehrt Unterstützungsangebote zu erhalten. Die Verbesserung der Cybersicherheit und die Abwehr von Cyberattacken weist in der Befragung folgerichtig auf einer Skala von 1 (irrelevant) bis 7 (sehr relevant) länderübergreifend über alle Bodensee-KMU hinweg einen Mittelwert von 6,2 auf.

Der Staat kann natürlich nicht die Daten der KMU vor Angriffen schützen – das müssen die Unternehmen selbst tun. Jedoch können die politischen Akteure beispielsweise über Kompetenzzentren oder die finanzielle Förderung externer Beratung die KMU unterstützen. Speziell deutsche KMU erachten eine solche finanzielle Förderung externer Beratung im Themenfeld IT-Sicherheit als besonders relevant.

Länderübergreifend benötigen die Bodensee-KMU nach eigener Aussage insbesondere Unterstützung bei den rechtlichen Themen in Bezug auf Daten- und Know-how-Schutz sowie im Bereich der Geheimhaltung.

Einfach ausgedrückt kann man sagen: Cybersicherheit ist eine essenzielle Grundlage für digitales Vertrauen.

„Als Unternehmen würde ich mich nicht darauf verlassen, dass mich jemand von aussen schützt."

(Wirtschaftsförderer innerhalb Vorarlbergs)

„Der Staat sollte auf jeden Fall Richtlinien und Gesetzesgrundlagen schaffen, dass die Provider einer bestimmten Vorsorgepflicht unterliegen. Das heisst, die sollten ihre Netze so absichern, dass da keine Angriffe stattfinden können und meine Daten nicht auf dem Weg verloren gehen können. Zudem sollte man dann so Sachen einführen wie eine Verschlüsselungspflicht."

(CEO eines deutschen Start-ups in der IT-Branche)

Digitaler Staat: Verwaltungsaufwand für Unternehmen reduzieren und digitalisieren

Zeit und Geld sind insbesondere bei KMU knappe Ressourcen. Umso ärgerlicher ist es dann vor allem für diese Unternehmen, wenn die Mitarbeitenden für verwaltungstechnische Routineaufgaben jedes Mal den Gang zur örtlichen Behörde antreten müssen. Jeder kennt das Leid wahrscheinlich aus eigener Erfahrung: Egal ob man seinen Personalausweis verlängern oder eine Anwohnerparkkarte beantragen möchte – das Aufsuchen des Bürgerbüros ist häufig unerlässlich, obwohl die relevanten Daten dafür meistens bereits vorliegen.

Die Verwaltungsaufwendungen und die administrative Last sollten vor allem für KMU auf ein Minimum reduziert werden. Viele administrative Tätigkeiten sind schlichtweg notwendig, jedoch sollten alle Aufwendungen, welche sich digitalisieren lassen, auch digitalisiert werden. Wird nämlich bei der Modernisierung und *Digitalisierung* der (öffentlichen) Verwaltungen gespart, dann müssen die Kosten (Zeit oder Geld) letztlich die Kunden tragen – in diesem Falle die Bodensee-KMU und ihre Beschäftigten.

Werden diese Güter durch zusätzliche Verwaltungsaufwendungen weiter reduziert, muss anderswo gespart werden wie z. B. an den Gehältern der Mitarbeitenden. Selbstverständlich ist die *Digitalisierung* solcher Leistungen insbesondere auch in Bezug auf Unternehmensgründungen, -änderungen und -löschungen von hoher Relevanz.

Die Devise seitens der politischen Akteure muss es also sein, den KMU möglichst Zeit und Geld zu sparen, damit diese sich auf ihr Kerngeschäft konzentrieren können.

„Grundsätzlich sollte man für KMU die Regularien abändern: Weniger Steuerbürokratie!“

(CEO eines deutschen Start-ups in der IT-Branche)

Wirtschaft vernetzen: Aber bitte nicht nur die Maschinen

Wie es bereits im Bereich der Infrastruktur angesprochen wurde, hört man im Zusammenhang mit der *Digitalisierung* der Wirtschaft häufig den Ruf nach Industrie 4.0: Miteinander möglichst intelligent vernetzte Maschinen sollen Entscheidungen ohne menschliche Unterstützung treffen und ausführen.

Massgeblich ist dafür logischerweise die Vernetzung dieser Maschinen. Innerhalb dieses Forschungsprojektes ist aber auch immer wieder der Ruf der KMU nach einer Unterstützung im Bereich der Vernetzung und Schaffung von Kooperationen auf menschlicher Ebene zu vernehmen gewesen. Innerhalb der Befragung hat sich beispielsweise eine Mehrheit der KMU von Seiten der Politik gewünscht, sie hauptsächlich bei der Herstellung von Netzwerken und Kooperationen mit anderweitigen Akteuren (z. B. anderen Unternehmen, Forschungseinrichtungen, Hochschulen, Wirtschaftsförderern, IHKs) zu unterstützen. Hierbei ist den Bodensee-KMU länderübergreifend zudem insbesondere die Vernetzung und Kooperation mit wissenschaftlichen Akteuren wichtig. Diese Vernetzung, sowohl mit wissenschaftlichen Akteuren als auch mit anderen Unternehmen, kann z. B. durch die Schaffung eines digitalen Marktplatzes gefördert werden.

Auch in Zeiten einer digitalen Welt sind Angebot und Nachfrage entscheidende Grössen für wirtschaftlichen Erfolg. Durch die digitale Welt wird aber sowohl das Angebot als auch die Nachfrage dezentral und vor allem digital erstellt. Über einen digitalen Marktplatz könnten KMU digitale Unterstützungsleistungen jedweder Art (z. B. der Implementation eines Enterprise-Resource-Planning-Systems) nachfragen. Die jeweiligen Anbieter bzw. Dienstleister könnten dann direkt mit dem jeweiligen KMU in Kontakt treten. Dadurch könnten sich beide Seiten teils hohe Suchkosten ersparen.

Eine weitere Möglichkeit die KMU im Bereich der Kooperationen und Vernetzung zu unterstützen wäre der Aufbau einer digitalen Kommunikationsplattform. Die Plattform könnte bestimmte, thematisch abgegrenzte Chaträume beinhalten, in denen sich registrierte und zugelassene Akteure über relevante und anstehende Themen wie z. B. den Datenschutz innerhalb des Unternehmens austauschen. Die KMU könnten so auch direkt voneinander lernen, ohne ihre Geschäftsgeheimnisse einander bzw. Dritten offenbaren zu müssen.

In jedem Fall müssen aber alle Unterstützungsangebote, Massnahmen und Rahmenbedingungen transparent sein. Die KMU müssen hierzu

einen einfachen und bürokratiearmen Zugang zu den relevanten Angeboten erhalten. Zudem gilt in diesem Zusammenhang auch das Credo „Weniger ist manchmal mehr“: Im besten Falle werden relevante Unterstützungsangebote von der Politik nicht mit der Giesskanne ausgeschüttet, sondern diese in Kooperation mit allen relevanten Akteuren entwickelt. Die Akteure der bereits bestehenden Unterstützungsangebote können hier als wichtige Informationsquellen dienen. Sie sind im besten Falle innerhalb der *Bodenseeregion* international vernetzt. Auch eine internationale Koordinierung der Angebote wäre sicherlich hilfreich in Bezug auf eine möglichst zielführende Umsetzung.

„Ich wünsche mir Austausch mit allen Akteuren, weil Austausch extrem wichtig ist und meiner Meinung nach auch zu Digitalisierung gehört [...]. Wir müssen heute mehr denn je kooperieren und kollaborieren, weil sich alle Unternehmen mit diesen vielen Fragestellungen und Themenbereichen beschäftigen. Das kann nicht einer alleine machen. Da benötigt es Austausch und zwar in allen Bereichen“.

(CEO eines deutschen Start-ups in der IT-Branche)

Die Zeiten, in denen man als KMU alle unternehmensinternen Herausforderungen auch mit dem Know-how innerhalb des eigenen Unternehmens lösen konnte, neigen sich dem Ende entgegen. Es geht also grundlegend darum, die nationalen wie internationalen Akteursnetzwerke zu stärken und zu erweitern. Damit kann man den KMU die Chance geben, die aktuellen und anstehenden Herausforderungen innerhalb bzw. mit diesem Netzwerk anzugehen.

Autor: Christopher Köhler


Industrie 4.0 – Digital Twin
Agility
Traceability
Product & Process
Systems Engineering
Intelligence
Co-Simulation in Real-Time
Machine Learning

Personalpolitische Rahmenbedingungen und Handlungsempfehlungen

Personalfunktion: ein Zukunftsmodell?

Humane und soziale Ressourcen eines Unternehmens gelten auch in der *Digitalisierung* als nachhaltiger Wettbewerbsfaktor. Ein wesentlicher Trend, der neben der *Digitalisierung* bei der Gestaltung der *Personalpolitik* berücksichtigt werden sollte, ist der demografische Wandel und eine damit einhergehende – zumindest teilweise zu erwartende – wachsende Knappheit an Fachkräften.

Es spricht einiges dafür, dass *kleine und mittlere Unternehmen (KMU)* mit Innovationsfokus eine langfristig orientierte Personalstrategie verfolgen sollten. Ziel dieses Beitrags ist es, KMU mit solchem Wissen zu versorgen, das ihnen ermöglicht, ihre Innovationsbasis „humane Ressourcen" zu erhalten.

An der Personalführung sind verschiedene Akteure in einer Organisation beteiligt: die Funktion Human Ressource Managements (HRM) – soweit vorhanden –, die Geschäftsleitung, die Linienführungskräfte und die Mitarbeitenden selbst. Intensiv werden seit einigen Jahren eine geeignete Verteilung der Zuständigkeiten, die Rollen der Beteiligten sowie die Veränderung der Aufgaben und die Möglichkeiten der Automatisierung von Leistungen und Prozessen diskutiert.

Inwiefern das HRM die an die Funktion gerichteten Anforderungen erfüllt, und seine Leistungsfähigkeit unter Beweis stellt, ist seit einigen Jahren Gegenstand der Diskussion. Während in einigen Branchen hin und wieder gefordert wird, die Funktion HRM abzuschaffen, weist das World Economic Forum in „The Future of Jobs Report" (2018) „Human Resources Specialists" als „Emerging Job Roles" aus.

Unabhängig davon, wer die mit Personalführung verbundenen Funktionen ausübt, ist es wichtig, sich weiterhin systematisch dem wichtigsten Wettbewerbsfaktor zahlreicher Unternehmen aktiv zuzuwenden – dem „Human Factor". Auch ist davon auszugehen, dass die Selbstverantwortung des Einzelnen steigt, sich als wertvolle Ressource zu erhalten. Gleichzeitig behalten Unternehmen ihr Interesse daran, dass Ressourcen für sie verfügbar und zugänglich bleiben. Entsprechend ist es im eigenen Interesse, dass sich auch Unternehmen aktiv um ein geeignetes Management ihrer humanen Ressourcen im Zeitalter der *Digitalisierung* kümmern. Dies ist umso wichtiger, da sowohl Technologisierung als auch moderne Organisationsformen sehr stark dazu geeignet sind, die Effizienz zu steigern und oft vor allem mit dieser Perspektive eingeführt werden. Langfristig birgt eine Vereinseitigung in Richtung effizienter Nutzung der Ressourcen jedoch Risiken im Hinblick auf eine Vernachlässigung ihrer Entwicklung und damit schlussendlich für den Erfolg. *Personalpolitik* in der *Digitalisierung* sollte daher neben der effizienten Nutzung aktiv die gewünschte Entwicklung von Mensch und Zusammenarbeit in den Blick nehmen.

Szenarien in der Gestaltung von HRM

Wie im Grünbuch „Digitale Agenda Bodensee – Eine Bestandsaufnahme zum Potenzial der *Digitalisierung* innerhalb KMU in der *Bodenseeregion*“ dargestellt, werden in der Diskussion um die *Digitalisierung* verschiedene Entwicklungen gemeinsam diskutiert, ohne ihre Implikationen auszudifferenzieren. Technologisierung findet in Unternehmen oft zeitgleich mit Überlegungen über Veränderungen der internen Organisation sowie der unternehmensübergreifenden Organisation von Zusammenarbeit statt. Insbesondere über netzwerkförmige Organisationsmodelle mit höheren Anteilen der Selbststeuerung wird diskutiert, wie z. B. im Fall von Holokratie.

Technologisierung und eine Veränderung der Organisationsform stellen unterschiedliche Anforderungen an die humanen Ressourcen und deren Management. Entsprechend unterschiedlich sind eine Führung durch die Linie, die Selbstführung der Mitarbeitenden sowie Vorgehensweisen und Praktiken der indirekten Führung zu gestalten. Es ist erforderlich, sich mit Blick auf Organisationsprinzipien wie etwa Autonomie vs. Vorgaben sowie Wettbewerb vs. Kooperation eindeutig zu positionieren und Führung daran orientiert zu gestalten.

Abbildung 3:
Gestaltung des Managements humaner Ressourcen – Szenarien entlang von Technologisierung und Organisationsform

Setzt man Technologisierung und Organisationsform in Beziehung zueinander, so ergeben sich entlang des Ausmasses der Technologisierung in einem Unternehmen und dem anvisierten Selbstorganisationsgrad vier unterschiedliche Kombinationsmöglichkeiten für das Management humaner Ressourcen (Abbildung 3).

Je nach Szenario unterscheiden sich die *Personalpolitik*, Führungs- und Unternehmenskultur auf Makroebene, ihre Ziele, Vorgehensweisen und Instrumente des HRM auf Mesoebene sowie die Gestaltung der Arbeitsplätze auf Mikroebene. Die im Grünbuch dargestellten Ergebnisse weisen darauf hin, dass eine Diskrepanz besteht zwischen dem Handeln, das Unternehmen in der Organisation wünschen und dem, was durch den Einsatz von Technologien tatsächlich gefördert wird. So wird beispielsweise von Mitarbeitenden immer höhere Autonomie und Selbstverantwortung erwünscht, für die die Technologiegestaltung allerdings oft wenig Platz lässt. Langfristig verkümmern in einer solchen Situation die für Autonomie und Selbstverantwortung relevanten Kompetenzen, auf die man eigentlich setzen wollte.

Hohe Technologisierung und Selbstorganisation als mögliche Strategie

Unsere zentrale Forschungsfrage bezog sich darauf, wie gut Geschäfts-, Technologie- und *Personalpolitik* aufeinander abgestimmt sind bzw. ob die Technologisierungs- die *Personalpolitik* eventuell ungewollt boykottiert (Abbildung 4).

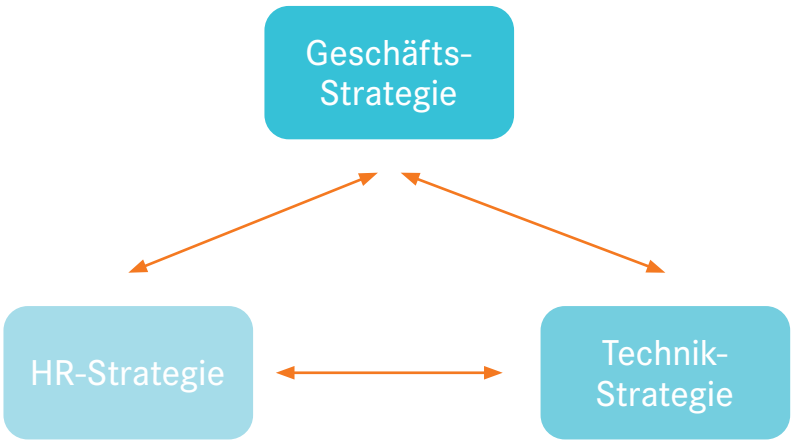


Abbildung 4: Abzustimmende Teilstrategien in der Digitalisierung

Die im Grünbuch dargestellten Erkenntnisse verdeutlichen, dass viele der befragten Unternehmen ein Zusammenspiel von Mensch und Maschine vorsehen, bei dem die Stärken von Mensch und Technik optimal kombiniert werden. Um dies zu erreichen, sollen moderne Technologien eine immer umfassendere Bedeutung erhalten. Den Mitarbeitenden ist ausreichend Autonomie zuzugestehen, damit sie selbstgesteuert ihre Stärken zum Einsatz bringen und sich weiterentwickeln können.
Die befragten Unternehmen sind sich zwar grundsätzlich der hohen Bedeutung der Mitarbeitenden für ihren Erfolg bewusst, setzen sie aber nur wenig an den Ausgangspunkt von Überlegungen der Technologisierung. Bestehende Trade-offs zwischen Geschäftsstrategien, Technologisierung und Human Resource (HR) sind kaum bewusst. Die Geschäftsstrategie, die Organisationsformen zu ihrer Umsetzung sowie die Technologie- und HR-Politik werden wenig aktiv aufeinander abgestimmt.

Dies stellt sich in den Aussagen von Befragten so dar, dass der Mensch die Technik kontrollieren solle, was in letzter Konsequenz erfordere, dass Mitarbeitende überlegener bleiben sollen. Andererseits werden soziale Innovationen als weniger wichtig betrachtet, wird bei der Technologiegestaltung nur wenig auf Menschen und Zusammenarbeit fokussiert und erwartet, dass sich der Mensch an die Technik anpasst. Letztlich sind damit die Angaben bezogen auf die Technologisierung widersprüchlich: Anforderungen mit Blick auf den Menschen werden weniger berücksichtigt und er soll sich an Technik anpassen – die Technik aber gleichzeitig beherrschen.

Eine solche Technologiepolitik passt zudem nicht zu den vielfach angestrebten, modernen Organisationsformen, die die Geschäftsstrategie unterstützen sollen.

Notwendig wäre es zum einen, die Technisierungspolitik deutlich stärker unter humanbezogenen und technologischen Aspekten zu gestalten. Zum anderen ist die HR-Politik mit ihren zugehörigen Vorgehensweisen und Praktiken in Abstimmung mit der Technologisierung und Organisationsform im Sinne von „HR 4“ (siehe Abbildung 3) auszurichten und zu gestalten.

Neue Rollen des HRM: Handlungsfelder zur beispielhaften Realisierung

Die Fragen, ob man nun das HRM als Funktion abschaffen soll und wie das Management humaner Ressourcen in Zukunft aussehen kann, waren Gegenstand eines Workshops mit acht Beteiligten. Basierend auf den Ergebnissen des Projektes wurden zwei sehr unterschiedliche Modelle des HRM entworfen – „‘Cloud‘ia“ und „People Coach“ (Abbildung 5 und 6 auf den Seiten 24 bzw. 25).

„‘Cloud‘ia“ stellt ein vollautomatisiertes System dar, das ausgerichtet an der Strategie des Unternehmens Mitarbeitende und Führungskräfte in ihrer Selbstverwaltung unterstützt und primär auf Self-Services setzt. Die HR-Prozesse sind vollkommen digitalisiert. Der „People Coach“ sieht keine Abschaffung der Funktion HRM vor. Er setzt vor dem Hintergrund der *Digitalisierung* einen Schwerpunkt auf die Schaffung einer ggf. erweiterten Rolle des HRM, die die Gestaltung und Förderung zwischenmenschlicher Beziehungen und der Unternehmenskultur zur Aufgabe hat. Die Diskussion mit den Experten im Workshop erwies zunehmend, dass „‘Cloud‘ia“ und „People Coach“ nicht als Gegensätze zu verstehen, sondern vielmehr komplementär zu betrachten sind.

Die *Digitalisierung* der HR-Prozesse erfährt im Literaturdiskurs in Analogie zu „‘Cloud‘ia“ eher eine Überbetonung. Hingegen werden Fragen nach der kompetenten Gestaltung der digitalen Transformation in Unternehmen bezogen auf humane Ressourcen, Zusammenarbeit und Führung vernachlässigt (Jochmann & Belch, 2016).

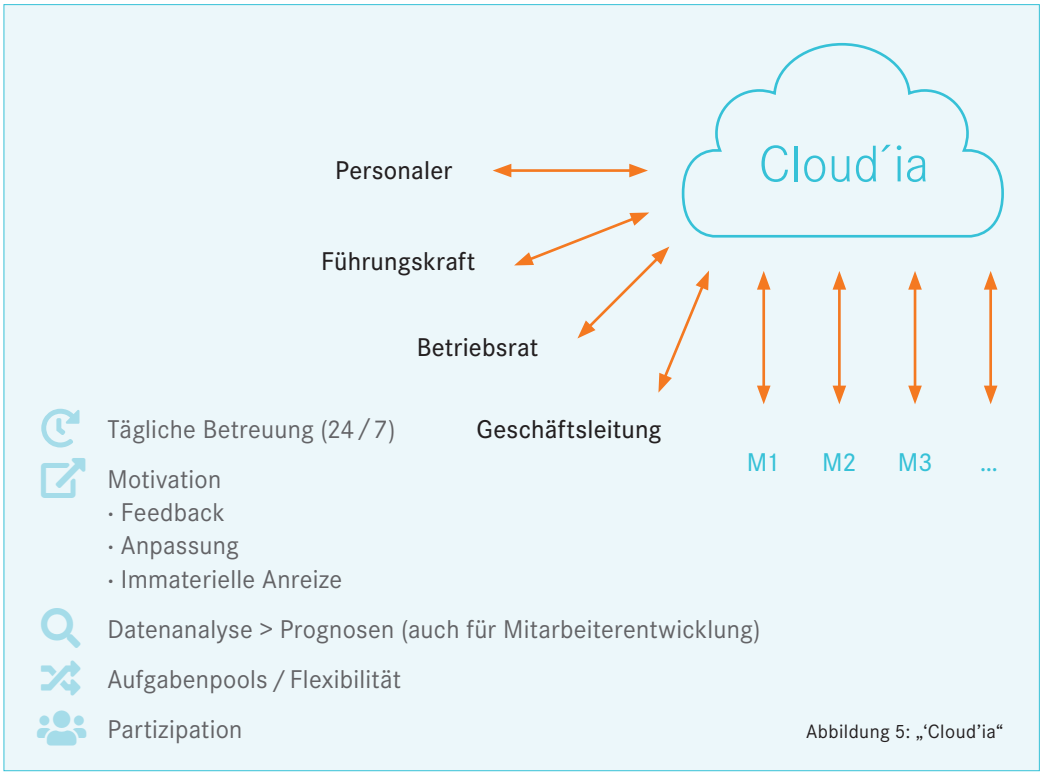


Abbildung 5: „‘Cloud’ia“

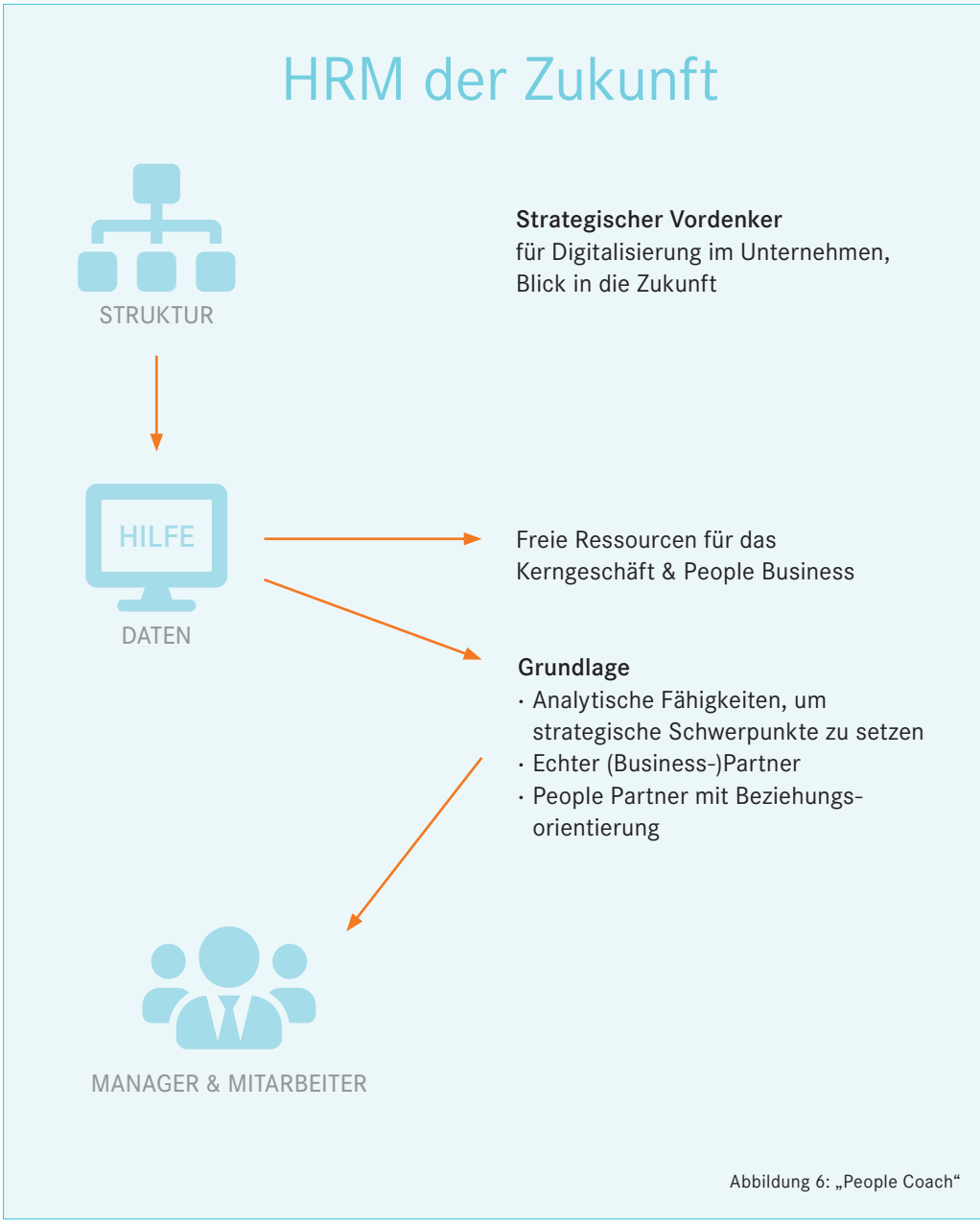


Abbildung 6: „People Coach“

Ein HRM mit einer zu „HR 4“ (Abbildung 3) passenden *Personalpolitik* mit geeigneten Vorgehensweisen und Instrumenten kombiniert den „People Coach“ auf Makroebene sowie „‘Cloud‘ia“ v. a. auf Mesoebene. Dabei hat ein „HR4“ der Zukunft entlang der verschiedenen Ebenen die in Abbildung 7 (nicht abschliessend) dargestellten Aufgaben:

MAKROEBENE	**Personalpolitik**	· Orientierung / Abstimmung der Geschäfts,- Technisierungs- und Personalstrategie · Ausdehnung der Zuständigkeit auf die gesamte Belegschaft / „Workforce“
	Unternehmenskulturentwicklung und Beziehungen gestalten	· Förderung von Zeit- und Leistungskultur, Vertrauenskultur, hierarchieübergreifender Feedbackkultur, Transparenzkultur · Führungsinstrumente (um-)gestalten, Gehalt, Sozialleistungen und Anreize · Führungskräfteentwicklung
	Soziotechnische Gestaltung der Transformation	· aufeinander bezogene technologische und sozioökonomische Gestaltung der Transformation; menschengerechte Gestaltung, Adaption und Implementierung technologischen Fortschritts
MESOEBENE	**Stärkung strategischer Kernprozesse des HRM und Nutzung von HR-Tech**	· Strategic Workforce Analytics und Transformation · Kompetenzmanagement, Rekrutierung sowie Personal- / Karriereentwicklung · Workforce Wellbeing: Daten, Quantifizierung, Impact
	Optimierung administrativer Routineprozesse im HR	· Administrative Basisprozesse wie Payroll, Arbeitszeiterfassung, etc.
MIKROEBENE	**Gestaltung des Arbeitsplatzes**	· Offene Bürostrukturen, aktivitätsbasierte Arbeitsplätze, Büro als Wohlfühlraum · Shared Office Spaces, Desk Sharing, Coworking, mobile Arbeitsplätze
	Gestaltung des Arbeitsorts und der Arbeitszeit	· Zeitlich und örtlich flexibles Arbeiten / Mobilität bzw. Ortsungebundenheit, Home-Office, Coworking · Wahlarbeitszeit, Self Managed Working Time
	Gestaltung der Arbeitsinhalte und der Zusammenarbeit	· Arbeitsgegenstände bzw. technische Devices zur Verrichtung der Arbeit · Variabilität, Flexibilität und Komplexität der Arbeitsinhalte – Autonomie vs. Formalisierung · Virtuelle Formen zur Leistungserbringung (virtuelle Teams, Plattformen, Open Innovation Netzwerke) und projektbezogene Zusammenarbeit, Jobsharing

Abbildung 7: Aufgaben eines HRM bei hoher Technologisierung und hoher Bedeutung humaner Ressourcen für den Unternehmenserfolg (HR4)

Anders als viele Darstellungen in Praktikerliteratur es vorsehen, scheint kein komplett neues Modell des HRM erforderlich. Unternehmen sollten einschätzen, wie gut sie den dargestellten Aufgaben gerecht werden und Ergänzungen in ihren bestehenden Aktivitäten vorsehen. Hier empfiehlt es sich

1. die Art der auf den Menschen bezogenen Technologiepolitik zu bestimmen,
2. die passende Form der Organisation und Zusammenarbeit zu definieren und
3. die sich daraus ergebenden Handlungsfelder für das Management der humanen Ressourcen anzupassen.

Ein Selbsteinschätzungsinstrument, mit dem sich Unternehmen einen ersten Eindruck der eigenen digitalen HRM-Reife machen können, bietet der HRM-Digital-Readiness-Check, der im Rahmen des Teilprojektes Nutzenbasierter Digitalisierungsnavigator im IBH-Lab KMUdigital entwickelt wurde. Die Light-Variante ist via QR-Code-Link abrufbar.

Abbildung 8: HRM-Digital-Readiness-Check (lite)
→ https://www.umfrageonline.ch/s/hrm-drc

HR hat Nachholbedarf in puncto digitaler Kompetenz

Angesichts der zunehmenden *Digitalisierung* wird immer häufiger von den Begriffen der „Digitalkompetenz“ oder „digital literacy“ gesprochen. Sie findet bisher vor allem auf gesellschaftlicher Ebene Anklang, so beispielsweise in Frameworks der Europäischen Union (Ala-Mutka, 2011), des Institute for the Future (Davies, Anna, Filder & Gorbis, 2011) und der International Federation of Library Associations and Institutions (2017). Die Diskussion bezogen auf die Mesoebene der Unternehmen findet dazu verzögert statt und allgemeingültige Definitionen von Digitalkompetenz haben sich noch nicht herausgebildet.

Überträgt man Aussagen auf die Unternehmensebene, so geht es zusammenfassend darum, Technologien mit Blick auf den Anwendungskontext zu verstehen, ihre Funktionen und ihre produzierten Ergebnisse zu begreifen und aufgrund von Erfahrung angemessen in Handlungen zu nutzen. Notwendig ist dafür der Erwerb von

1. neuem, unmittelbar auf Technologien bezogenen Wissens, das in den jeweiligen Anwendungskontext zu setzen ist
2. erweiterten überfachlichen Kompetenzen, um einen angemessenen Umgang mit den Technologien zu gewährleisten. Darunter fallen:
   a) kritisch-reflexives Denken: welche Auswirkungen hat der jeweilige technologische Fortschritt sozial, wirtschaftlich und persönlich
   b) Komplexitäts-, Abstraktions- und Problemlösungsfähigkeiten

c) Kommunikation, Kooperation
d) Fähigkeiten zu lebenslangem Lernen

Des Weiteren sind Datensicherheit und Datenschutz sowie Ethik wichtige Aspekte der Digitalkompetenz. Auch zeigt sich, dass im HR in Vergleich zu anderen betrieblichen Funktionen im Allgemeinen die Digitalaffinität und -kompetenz unterentwickelt ist (Jochmann & Belch, 2016).

Unsere Ergebnisse weisen auf ein bisher eher geringes Interesse von Unternehmen hin, das HRM vor dem Hintergrund der *Digitalisierung* und unter Hinzuziehung von Expertise zu gestalten. Dies halten wir für einen beunruhigenden Befund, denn die Digitalkompetenz bezogen auf HRM ist in zweifacher Hinsicht relevant:

1. Für die Entscheidung, welche auf humane Ressourcen, Zusammenarbeit und Führung bezogene Kompetenz in der Organisation ausgebaut wird. Bisher wird die Rolle der IT-Funktion und ihrer Kompetenzen überbewertet, so dass die *Digitalisierung* vereinseitigt mit der innovativen Evolution von IT-Systemen gleichgesetzt wird (Jochmann & Belch, 2016, S. 60).
2. Um die im HRM zunehmend diskutierten und eingesetzten Technologien angemessen bewerten, einsetzen und den erwarteten Nutzen realisieren zu können.

Ansatzpunkte einer Digitalkompetenz bezogen auf HR

Es ist davon auszugehen, dass Unternehmen notwendige *Digitalisierung*sexpertise zunehmend von aussen beziehen werden. Um entsprechendes, für die Digitalisierung notwendiges Wissen und Kompetenz zu erwerben, streben KMU zunehmend Partnerschaften mit Institutionen aus der Forschung an (Eidgenossenschaft, 2018; Köhler, Olbert-Bock & Strittmatter, 2018). Auch hier müssen interne Spezialisten in der Lage sein, die Güte und Nützlichkeit neuer Technologien unter Berücksichtigung der spezifischen Situation des Unternehmens beurteilen zu können. Am Aufbau einer Digitalkompetenz bezogen auf HR – je nach Arbeitsteilung in der Organisation verankert bei der Geschäftsleitung, bei der Linie oder bei Spezialistenfunktionen – kommt ein Unternehmen nicht vorbei.

Um das Verständnis zu fördern, worum es bei Digitalkompetenz geht, werden im Folgenden beispielhaft zwei relevante Digitalkompetenzen für ein „HR4“ skizziert.

1. Menschenzentrierte Gestaltung des technologischen Wandels

Automatisierung, die sich bisher weitgehend auf die Fertigung bezogen hat, bezieht sich in Form von „Robotics“ zunehmend auch auf Serviceleistungen. Neue Möglichkeiten der Mensch-Maschine-Zusammenarbeit und digital vermittelte Formen der Zusammenarbeit und des Lernens z. B. in virtuellen Räumen oder Lernbegleitung durch Assistenz oder Chatbots verändern die betriebliche Leistungserstellung. Auffällig an unseren Ergebnissen ist, dass die *Digitalisierung* sehr stark von Effizienzüberlegungen dominiert wird. Das gilt auch für neue Organisationsmodelle und Arbeitsmethoden, die sich wenig an Überlegungen einer „Humanisierung“ der Arbeitswelt orientieren. Sollen Mensch und Zusammenarbeit langfristig als Wettbewerbsfaktor nutzbar bleiben, kommt man nicht umhin, die Gestaltung von Technologieeinsatz neben aktueller Kreativität und Effizienz auch förderlich für weitere, vor allem langfristig orientierte Leistungsgrössen zu gestalten.

Um dies zu ermöglichen, gilt es eine „Vision für gelungene Partnerschaft von Mensch und Maschine“ (Seufert, Guggemos, Meier & Helfritz, 2018) zu entwickeln und soziale Kompetenzen

in der Organisation zu fördern, die das „neue soziale Miteinander“ im Kontext von Kollaborationsplattformen und virtueller Zusammenarbeit befruchten (Jochmann & Belch, 2016).

Damit Digitalkompetenz in die Organisation gebracht wird, setzt beispielsweise die Firma Adlon „Transformation Coaches“ ein. Diese setzen sich frühzeitig mit Nutzungsmöglichkeiten neuer Technologien sowie ihren intendierten und nicht-intendierten Wirkungen wie z. B. eines Deskillings durch Technologieeinsatz auseinander. Voraussetzungen einer langfristigen Erhaltung der humanen Ressourcen werden bei der Gestaltung von Technologien und im Enabling der Organisation in ihrer Nutzung berücksichtigt. Soziotechnischer Wandel sieht vor, geplante technologische Veränderungen im Hinblick auf ihre Konsequenzen für Mensch und Zusammenarbeit zu bewerten und ermöglicht die weniger vereinseitigte Gestaltung von Technologien und Veränderung. Bevor ein flächendeckendes Rollout erfolgt, werden Wirkungen in Pilotumsetzungen verfolgt und Optimierungen in der Gestaltung vorgenommen (Abbildung 9).

Abbildung 9: Etappen zur soziotechnischen Gestaltung von Technologien und Veränderung (Olbert-Bock & Lévy-Tödter, 2019)

2. Verstehen und zielgerichtete Nutzung von Daten im HR-Anwendungskontext mittels Analytics und künstlicher Intelligenz

Aus der Analyse der in Unternehmen zahlreich anfallenden Daten, erhofft man sich neue Erkenntnisse für beispielsweise die Rekrutierung, die Bindung von Mitarbeitenden und das Talentmanagement (Abbildung 10). Im Unterschied zum klassischen Personalcontrolling mit der Darstellung von Key Performance Indicators wie z. B. der Fluktuation, steht bei einer Analyse mit Big Data die Suche nach den Einflussfaktoren auf die Fluktuation im Zentrum des Interesses. Vorgehensweisen und Personalpraktiken im Unternehmen lassen sich dann zielgerichteter formulieren.

Je grösser ein Unternehmen, umso umfassendere Datensätze stehen grundsätzlich zur Analyse bereit. Die erste Begeisterung verfliegt allerdings häufig schnell, denn die Qualität der

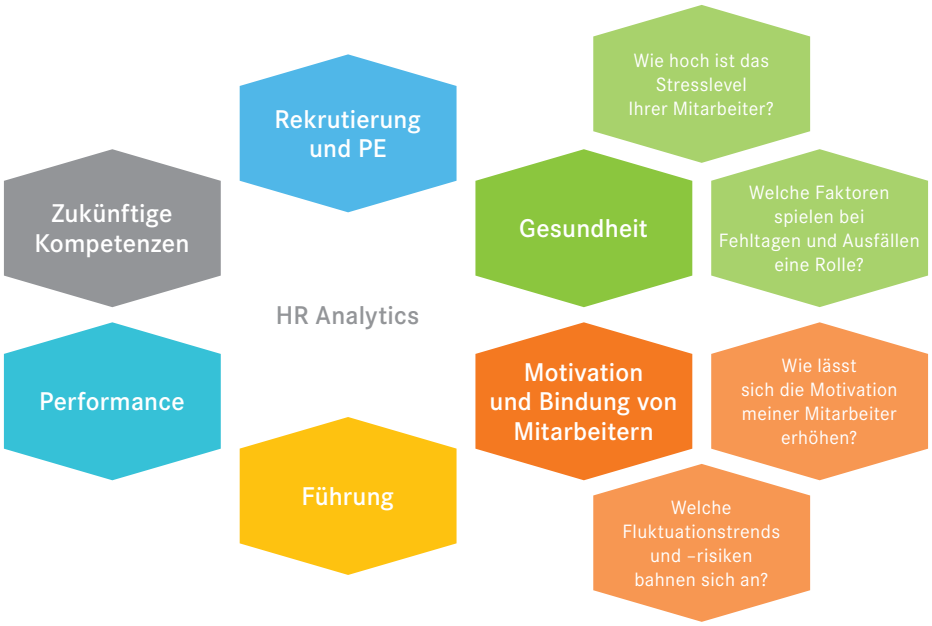


Abbildung 10: Beispielhafte Themen- und Fragestellungen für HR Analytics (Giermindl, Christ & Redzepi, 2019)

Daten ist, verglichen mit dem forschungsbasierten State of Science, nicht immer gewährleistet und die Datenverarbeitung nicht trivial. Nach der anfänglichen Euphorie tritt daher mit Blick auf den tatsächlichen Zusatznutzen eine gewisse Ernüchterung ein.

Das komplexe Verhalten von Menschen entzieht sich auch zu Zeiten von grossen verfügbaren Datensätzen der kompletten Messbarkeit und bedarf einer anderen Form der Interpretation als etwa die Optimierung von *Maschinendaten*.

Wichtig bleibt, dass im HR eine ausgeprägtere Kompetenz im Umgang mit Daten, z. B. auch denen aus wissenschaftlicher Forschung unumgänglich ist. Seit Langem wird mehr Evidenz für die Fundierung von Entscheidungen gefordert (Brodbeck & Woschée, 2012), die der Akzeptanz des HR förderlich wären. Gemeint ist nicht eine Vereinseitigung im Sinne der ausschliesslichen Nutzung von evidenzbasiertem Wissen. Vielmehr geht es darum, dieses Wissen bei der Entwicklung des eigenen Verständnisses zu berücksichtigen und verbleibende Leerstellen mit Erfahrung sowie mit nicht auf Evidenz basiertem Wissen zu füllen.

Des Weiteren sollten die Organisationsmitglieder insbesondere mit Blick auf humane Ressourcen, Zusammenarbeit und Führung zu einer angemessenen Interpretation von Daten befähigt und in der Organisation die Kompetenz im Umgang mit Big Data gefördert werden.

Kompetenter Umgang mit Daten in Form der Ableitung angemessener Schlussfolgerungen verlangt eine kontextbezogene Interpretation. Dies bedeutet für Entscheidende, dass sie über Fähigkeiten verfügen sollten, spezifische Ursache-Wirkungsbeziehungen zu berücksichtigen. Darüber hinaus sollten sie die Reichweite von Aussagen beurteilen können, um „weise" Entscheidungen zu fällen, die sich durch Nützlichkeit und Verantwortungsübernahme auszeichnen (Baden & Higgs, 2018; Brodbeck & Woschée, 2012).

Aufbauend auf der Analyse von grossen Datensätzen werden zahlreiche Verfahren und Instrumente entwickelt, um künstliche Intelligenz (KI) im HR zu implementieren. KI zeichnet sich dadurch aus, dass es in der Lage ist, selbst Regelmässigkeiten zu erkennen und Algorithmen datenbasiert an neue Gegebenheiten anzupassen bzw. weiterzuentwickeln. Dabei imitiert KI „menschliches Verhalten" und kann Routinen anpassen. Beispiele hierfür sind das Erkennen von Gesichtsausdrücken, Geschriebenem oder Gesprochenem sowie das selbstgesteuerte Führen von Gesprächen mit den menschlichen Anwendern (z. B. CoPilot von SAP, Mya von HireMya, Ari von TextRecruit, Sophie von HR Campus).

Eine umfassende Diskussion rund um die Nutzung von KI ist im Rahmen von Auswahl und Förderung von Mitarbeitenden z. B. in Führungsfunktionen entstanden. Auf der einen Seite bestehen Hoffnungen, besser als bisher geeignete Mitarbeitende identifizieren und KI zur Reduktion von Biases in der Personalauswahl anwenden zu können (Daugherty, Wilson, & Chowdhury, 2018). Auf der anderen Seite finden sich Bedenken dahingehend, dass die angewendeten Algorithmen nicht ausreichend bekannt sind und dass

die notwendige Fortschreibung von Daten aus der Vergangenheit auch stereotype Annahmen spiegelt und bestehede Diskriminierungen zementiert.

Zwischenzeitlich verrichten Chatbots viele Dienste: auf Karriereseiten beantworten sie interessierten Kandidaten automatisiert Fragen über offene Stellen und Karrieremöglichkeiten sowie über das Unternehmen, so dass anwendende Unternehmen sich bereits eine Verbesserung der Candidate und Employee Experience versprechen. Es besteht des Weiteren z. B. die Hoffnung, Änderungen im Fluktuationsverhalten von Mitarbeitenden dank dem Einsatz von KI frühzeitig zu erkennen. Dies kann dazu genutzt werden, gefährdete Mitarbeitende zu identifizieren und entsprechende Massnahmen vorzuschlagen, die zu einer wirksamen Bindung dieser Personen beitragen könnten. Von einer vollständig künstlich-autonomen Rekrutierung sind wir dennoch weit entfernt.

Technologiebezogene Kompetenz bezieht sich darauf, wie künstliche Intelligenz zu „trainieren" ist, wie Daten gewonnen, verarbeitet und interpretiert werden können und darauf, wie sie zu gestalten ist, dass unbeabsichtigte Konsequenzen wie etwa Diskriminierungen vermieden werden (Wilson, Daugherty, & Morini-Bianzino, 2017). Welche Mitarbeitenden über welche dieser Kompetenzen verfügen müssen, ist eine Frage der unternehmensinternen Arbeitsteilung. Mit Blick auf ethische Aspekte wird z. B. die Etablierung eines Algorithmen TÜVs vorgeschlagen, bei der die für ethische Fragen zuständige Person und die für die Definition von Algorithmen verantwortliche Person zusammenarbeiten (Wilson, Daugherty & Morini-Bianzino, 2017). Interessant ist in diesem Zusammenhang die Initiative des Ethikbeirats HR-Tech, dessen Ziel es ist, zu rechtlichen und ethischen Fragen in Zusammenhang zu der Anwendung von KI im HR zu informieren und zur Diskussion anzuregen.

Autoren: Prof. Dr. Sibylle Olbert-Bock, Abdullah Redzepi

Abbildung 11: Ethikbeirat HR Tech
→ https://www.ethikbeirat-hrtech.de

Rechtliche Rahmenbedingungen und Handlungsempfehlungen

Im Grünbuch „Digitale Agenda Bodensee – Eine Bestandsaufnahme zum Potenzial der *Digitalisierung* innerhalb KMU in der *Bodenseeregion*“ wurden für *kleine und mittlere Unternehmen (KMU)* relevante Sachverhalte der Digitalisierung jeweils beschrieben und den potenziell einschlägigen Rechtsbereichen zugeordnet, aus deren Anwendung sich Herausforderungen im Umgang mit entsprechenden Phänomenen ergeben können.

Die Befragung aus dem Vorjahr sowie die im Anschluss durchgeführten Workshops belegten zunächst die Praxisrelevanz der untersuchungsgegenständlichen Digitalisierungssachverhalte. Die als „übergeordnete Sachverhalte“ geführten Untersuchungsobjekte wurden hierbei besonders häufig als Teilmengen der *Digitalisierung* erkannt und diskutiert.“

Die Workshop-Gruppen eigneten sich aufgrund ihrer heterogenen Zusammensetzung sehr gut, um die Praxisrelevanz der ausgesuchten Sachverhalte zu bestätigen. So befanden sich unter den Teilnehmenden Repräsentanten von KMU – hierunter auch Geschäftsführung von Start-ups aus dem Bereich Industrie 4.0 und Big Data Analysis, Rechtsabteilungsleitung und Leitung von IT-Abteilungen – sowie Rechtsanwaltskanzleien und Vertreter von Industrie- und Handelskammern.

Neben der Plausibilisierung der untersuchungsgegenständlichen Digitalisierungssachverhalte wurden mit den Teilnehmenden die nachstehenden Thesen diskutiert:

- **These I: Digitalisierung ist nicht schwer**
  „Die rechtlichen Herausforderungen der *Digitalisierung* sind lediglich scheinbar komplex. Durch Aufschlüsselung des weitgefassten Begriffs lassen sich einzelne Phänomene / Sachverhalte identifizieren und eindeutig analysieren.“
- **These II: Digitalisierung braucht nicht mehr Regulierung**
  „Es bedarf keiner weiteren gesetzgeberischen Massnahmen, um rechtlichen Herausforderungen der *Digitalisierung* zu begegnen – bestehende Regelungen reichen aus, um sie zu bewältigen.“
- **These III: Digitalisierung braucht schon gar kein Dateneigentum**
  „... es bedarf insbesondere keiner Normierung eines Dateneigentums.“

Die Teilnehmenden stimmten hierbei insbesondere zu, dass sich Rechtsfragen zu den festgestellten Digitalisierungssachverhalten überwiegend in den bestehenden Rechtsrahmen einordnen und mit diesem beantworten lassen. KMU fehle es hingegen an Zeit, Ressourcen und Kompetenz, um relevante Rechtsfragen frühzeitig zu erkennen und diesen adäquat begegnen zu können. Ausserdem wurde die Forderung nach mehr Fachkräften zur Beurteilung von digitalisierungsspezifischen Rechtsfragen (etwa IT-Anwälte und Richter) sowie nach mehr aufklärenden Informationsveranstaltungen und -materialien vorge-

gebracht. Eine Erweiterung des bestehenden Rechtsrahmens und vor allem die Einführung eines Eigentumsrechts an Daten, traf bei den Workshop-Teilnehmenden eher auf Ablehnung.

Auch ergänzende Experteninterviews, die mit Geschäftsführungen und Rechtsabteilungsleitungen aus KMU geführt wurden, bestätigten die Relevanz der übergeordneten Sachverhalte. Weiterhin zeigte sich, dass sich KMU überwiegend erst bei der Durchführung von Digitalisierungsmassnahmen mit einschlägigen rechtlichen Fragestellungen auseinandersetzen, anstatt diese bereits bei der Planung digitaler Strategien zu antizipieren. Eine Ausnahme bilden hier die Aspekte des Datenschutzes. Einerseits begründeten die Befragten diesen Umstand mit fehlenden Ressourcen und Kompetenzen. Darüber hinaus wurde aber auch ein fehlendes Bewusstsein bezüglich potenzieller Rechtsfragen in den unterschiedlichen Unternehmensfachbereichen als ursächlich befunden – im Vordergrund stünden hierbei vielmehr technische und kommerzielle Aspekte.

Zusammenfassend lässt sich an diesen Feststellungen ein dringender Bedarf bei KMU für praxisnahe, rechtliche Orientierungshilfen erkennen. Es scheint wichtig, in den Unternehmen ein Problembewusstsein für rechtliche Herausforderungen zu schaffen. Gleichzeitig soll den Unternehmen ausreichend Informationen an die Hand gegeben werden, um zumindest einen ersten, strukturierten Abgleich zwischen Digitalisierungsbestrebungen und potenziell einschlägigen Rechtsproblemen bewerkstelligen zu können. Der Abgleich soll niederschwellig möglich zugänglich sein, damit dafür keine Spezialisten eingekauft werden müssen (Orientierung). Im Rahmen der durchgeführten Experteninterviews wurden unter anderem nachstehende, auf KMU abgestimmte Massnahmen angeregt, um eine solche Orientierung bereitzustellen:

- Wissensdatenbanken
- Orientierungspapiere
- Workshops und Vorträge
- Zusammenarbeit mit Hochschulen

Mit der rechtlichen Analyse branchenübergreifender und -spezifischer Sachverhalte, leistet dieses Weissbuch einen ersten Beitrag zu dieser Orientierung. Dies findet im Wissen statt, dass darüber hinaus weitere Massnahmen zur Unterstützung von KMU notwendig sind.

Im Weiteren werden rechtliche Fragen zu den folgenden branchenübergreifenden Digitalisierungssachverhalten näher betrachtet:

- Daten mit Personenbezug
- Daten als Asset
- IT-Sicherheit
- Cyber-physische Systeme
- Cloud Computing und digitale Plattformen

Am Ende dieses Kapitels finden Sie einen Link und QR-Code, welcher Sie direkt zu diesen branchenspezifischen Sachverhalten führt.

Daten mit Personenbezug

KMU müssen bei der *Digitalisierung* von Arbeitsprozessen, der Vernetzung von IT-Systemen oder der Nutzung digitaler Dienste, wie z. B. Cloud

Services regelmässig datenschutzrechtliche Vorschriften, wie insbesondere die EU-DSGVO berücksichtigen. Dies kann auf den weiten sachlichen sowie räumlichen Anwendungsbereich zurückgeführt werden. Im Falle von Verstössen gegen den Datenschutz drohen Bussgelder in Höhe von bis zu 20 Millionen Euro oder 4 % des konzernweit erwirtschafteten Jahresumsatzes (sofern höher). Daher sind KMU angehalten, ihre Geschäftstätigkeiten im Einklang mit dem Datenschutzrecht zu gestalten und die dahingehenden individuellen Handlungsbedarfe nicht nur einmalig zu ermitteln, sondern regelmässig erneut zu evaluieren. Dieses Kapitel beschäftigt sich mit der Frage, wann welche datenschutzrechtlichen Vorschriften für KMU einschlägig sein und datenschutzrechtliche Handlungsfelder im Unternehmen organisiert werden können (Datenschutz-Management-System). Zudem wird skizzenhaft aufgezeigt, welche digitalisierungs- und gleichzeitig datenschutzspezifischen Problematiken in Bezug auf die besonders bedeutungsvollen Themen wie Webanalyse und Reichweitenmessung, Cloud Services und vernetzte Systeme entstehen.

1. Abgrenzung personenbezogener von nichtpersonenbezogenen Daten

Unter der Verarbeitung personenbezogener Daten ist gem. Art. 4 Nr. 2 DSGVO jeder Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten gemeint. Personenbezogene Daten beziehen sich anders als sonstige, nicht *personenbezogene Daten*, wie bspw. reine Sensor- / *Maschinendaten*, auf eine identifizierte oder identifizierbare natürliche Person (Art. 4 Nr. 1 DSGVO). Demgegenüber beziehen sich anonyme oder anonymisierte Daten nicht oder nicht mehr auf eine identifizierte oder identifizierbare natürliche Person, weshalb eine Datenverarbeitung im Einklang mit den strengen Vorschriften des Datenschutzrechts nicht mehr zwingend erforderlich ist. Ist eine Anonymisierung nicht möglich, so können Massnahmen zur Erhöhung der Sicherheit der Verarbeitung personenbezogener Daten getroffen werden, wie insbesondere die Pseudonymisierung und Verschlüsselung (vgl. Art. 32 Abs. 1 lit. a DSGVO). Bei der Pseudonymisierung ist die Personenbeziehbarkeit von Informationen weiterhin möglich und damit auch das Datenschutzrecht anwendbar; es handelt sich damit lediglich um eine andere Form der Speicherung, während die Verschlüsselung eine Sicherheitsmassnahme darstellt, durch welche die unbefugte Kenntnisnahme der Daten durch Dritte erschwert werden soll (Klabunde, 2018, s. Erwägungsgrund 26 DSGVO).

2. Räumlicher Anwendungsbereich der EU-DSGVO

KMU des Bodenseeraums mit Sitz in den Ländern Deutschland und Österreich unterliegen in Bezug auf die Verarbeitung personenbezogener Daten neben den jeweiligen nationalen datenschutzrechtlichen Vorschriften auch den europäischen Vorschriften der DSGVO. Die Anwendbarkeit der DSGVO für KMU mit Sitz in der Schweiz und eine Angleichung der nationalen Schweizer Datenschutznormen an das europäische Recht sind bis zum Jahr 2020 beabsichtigt (Schweizerische Bundesamt für Justiz, 2019). Nachstehend werden daher die Grundlagen des Datenschutzrechts mit dem Fokus auf das europäische Datenschutzrecht erläutert.

Bezogen auf eine identifizierte natürliche Person	Bezogen auf eine identifizierbare natürliche Person	Besondere Kategorien pbD („sensible Daten“ gem. Art. 9 Abs. 1 DSGVO)	Kein Personenbezug
· Name · Geburtsdatum · Adresse · E-Mail-Adresse · Telefonnummer · …	· Ermittlung der Identität einer Person durch Verwendung ergänzender Informationen wie zum Beispiel: · IP-Adresse (EuGH „Breyer“) · Geräte-IDs · Cookies zum Zweck der Identifizierung · Device Fingerprints · Kfz-Kennzeichen · Personalnummer · Ausweisnummer · Kontonummer · Berufliche Aktivitäten · weitere nicht ausreichend anonymisierte (oder pseudonymisierte) Daten	· Daten bezogen auf Rasse / ethnische Herkunft · politische Gesinnung · Religion / philosophische Überzeugung · Gewerkschaftszugehörigkeit · genetische / biometrische Daten, z. B. Fingerabdrücke zur Entsperrung von Apps · Gesundheit · sexuelle Orientierung	· Anonyme Informationen · Daten ohne Bezug auf eine identifizierte oder identifizierbare natürliche Person · anonym erhaltene Daten deren Ursprung nicht oder nicht mehr ermittelbar sind · reine Maschinendaten / Sensordaten ohne Personenbezug

Abbildung 12: Abgrenzung personenbezogener Daten von nicht-personenbezogenen Daten

Auch für in der Schweiz ansässige KMU kann neben dem nationalen Schweizer Datenschutzgesetz (DSG) die EU-DSGVO Anwendung finden, vor allem dann, wenn

a. nach dem sog. Niederlassungsprinzip gem. Art. 3 Abs. 1 DSGVO eine Niederlassung eines in der Schweiz ansässigen Unternehmens *personenbezogene Daten* innerhalb der EU verarbeitet oder
b. nach dem sog. Marktortprinzip gem. Art. 3 Abs. 2 DSGVO ein in der Schweiz ansässiges Unternehmen Waren und Dienstleistungen für EU-Bürgerinnen und Bürger anbietet (z. B. auf Websites) oder wenn dieses auf Websites Webtracking betreibt, durch welches sich das Surfverhalten von EU- Bürgern beobachten lässt.

3. Allgemeine datenschutzrechtliche Pflichten und nationale Besonderheiten sowie Ausnahmen für KMU

Grundsätzlich ist im Falle der Anwendbarkeit der DSGVO regelmässig insbesondere auf die Umsetzung folgender Pflichten zu achten:

- Einhaltung der datenschutzrechtlichen Grundsätze nach Art. 5 DSGVO (Grundsätze der Richtigkeit, Zweckbindung, der Rechtmässigkeit und der Verarbeitung nach Treu und Glauben, der Speicherbegrenzung und der Integrität und Vertraulichkeit) und damit v. a. die Verarbeitung personenbezogener Daten nur auf Basis einschlägiger Rechtsgrundlagen (Art. 6 DSGVO); hierbei ist die Besonderheit der Möglichkeit einer Einwilligung 14-Jähriger in Österreich zu beachten (§ 4 Abs. 4 DSG)

- Einhaltung der Transparenz- / Informationspflichten (Artikel 13 und 14 DSGVO)
- Gewährleistung der Wahrnehmung der Betroffenenrechte (Art. 16 – 22 DSGVO)
- Einhaltung der Benachrichtigungs- und Meldepflichten bei Datenschutzverstössen (Art. 33 und 34 DSGVO), jedoch bestehen bislang keine expliziten Meldepflichten für Datenschutzverstösse in der Schweiz[1]
- Führen eines Verzeichnisses für Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Abschluss von Verträgen zur Auftragsverarbeitung gem. Art. 28 DSGVO (s. Kapitel „Cloud-Computing und digitale Plattformen")
- Sicherstellung eines angemessenen Datenschutzniveaus im Falle einer Übermittlung personenbezogener Daten in sog. Drittländer (Art. 44 DSGVO)
- Ggf. Benennung eines Beauftragten für den Datenschutz (Art. 37 DSGVO), wobei die Konkretisierung der Anforderungen an die Bestellpflicht eines Datenschutzbeauftragten in Deutschland (§ 38 Abs. 1 BDSG) als auch die Besonderheit des Zeugnisverweigerungsrechts und der Verschwiegenheitspflicht des Datenschutzbeauftragten in Österreich (§ 5 DSG) zu beachten ist
- Umsetzung technisch-organisatorischer Massnahmen (TOMs) (Art. 32 DSGVO)

Neben den bereits genannten Besonderheiten der nationalen Datenschutzgesetze im Vergleich zur EU-DSGVO ist auch die jeweilige Konkretisierung des Beschäftigtendatenschutzes in Deutschland und Österreich (§ 26 BDSG, § 11 DSG) hervorzuheben.

Die besondere Situation, welche sich für KMU namentlich in personeller und wirtschaftlicher Hinsicht ergibt, sollte in der DSGVO zwar berücksichtigt werden (Erwägungsgrund 13 zur DSGVO), jedoch halten sich die dahingehenden praktischen Erleichterungen in Grenzen. Dies zeigt sich an den beiden folgenden Beispielen: Art. 30 Abs. 5 DSGVO sieht die Pflicht zum Führen eines Verfahrensverzeichnisses zwar dann nicht vor, wenn eine Einrichtung weniger als 250 Mitarbeitende beschäftigt. Allerdings besteht für KMU diese Pflicht bei risikoträchtigen, nicht nur gelegentlichen Verarbeitungen oder bei der Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 bzw. 10 DSGVO trotzdem. Dadurch ist der Anwendungsbereich dieser Ausnahme nicht allzu gross. In Bezug auf die Umsetzung der TOMs können nach Art. 24 Abs. 1 und 2 DSGVO aufgrund des Verhältnismässigkeitsprinzips dahingehende Erleichterungen, Flexibilität und wirtschaftlich vertretbare Lösungen für KMU bedeuten (Sydow, 2018). Hier sollte eine Abwägung jedoch nicht zulasten der Wahrung der Rechte und Freiheiten der Betroffenen stattfinden. Risikoaverse KMU werden daher im Zweifel eher bestrebt sein, den höheren datenschutzrechtlichen Anforderungen nachzukommen. Wesentliche Erleichterungen in Bezug auf die Umsetzung datenschutzrechtlicher Pflichten können KMU im Verhältnis zu Grosskonzernen damit im Wesentlichen durch die Ab-

[1] Künftig sollen diese nach einem Entwurf des revidierten Schweizer DSG jedoch „so rasch als möglich" stattfinden (vgl. den Entwurf der Schweizerischen Eidgenossenschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz unter: https://www.admin.ch/opc/de/federal-gazette/2017/7193.pdf (Stand: 09.03.2019).

wägung von Risiken bzw. das Eingehen verbleibender Risiken erreichen.

4. Implementierung eines Datenschutz-Managementsystems

Für die Umsetzung der einzelnen datenschutzrechtlichen Anforderungen kann sich die, ggf. auch gesetzlich verpflichtende, Etablierung eines Datenschutz-Management-Systems (DMS) eignen. Sie sollte sich an die sieben Grundelemente (Abbildung 13) eines *Compliance*-Management-Systems (CMS) nach dem Prüfungsstandard 980 des Instituts der Wirtschaftsprüfer (IDW) als Grundgerüst anlehnen (Institut der Wirtschaftsprüfer, 2011; Auer-Reinsdorff & Conrad, 2016) (siehe Abbildung 13).

Um der Bindung einer Grosszahl interner Ressourcen für die Bearbeitung von Datenschutzthemen vorzubeugen, kann es für KMU sinnvoll sein, ein DMS zusammen mit einem externen Datenschutzbeauftragten zu entwickeln. Es kann auch dann ein solcher externer Datenschutzbeauftragter bestellt werden, wenn hierzu keine Verpflichtung besteht (z. B. aufgrund der nicht einschlägigen Beispielfälle aus Art. 37 Abs. 1 DSGVO oder der nicht erreichten Mindestanzahl von Mitarbeitenden, welche die Bestellpflicht auslösen).

Datenschutz-Kultur	Die Schaffung einer Datenschutz-Kultur, insb. Schärfung des Bewusstseins der Mitarbeitenden für datenschutzrelevante Sachverhalte
Datenschutz-Ziele	Festlegung von Datenschutz-Zielen als Teil allgemeiner Unternehmensziele
Datenschutz-Organisation	Entwicklung einer Datenschutz-Organisation, wozu feste Prozesse, Rollen, Verantwortlichkeiten und Berichtswege zählen.
Datenschutz-Risiken	Frühzeitige Ermittlung von Datenschutz-Risiken und Berichterstattung hierzu
Datenschutz-Programm	Massnahmen zur Begrenzung und Vermeidung von Datenschutzverstössen und deren Dokumentation
Datenschutz-Kommunikation	Informierung der Mitarbeitenden und Etablierung eines Prozesses zum Umgang mit Schwachstellen
Überwachung + Verbesserung des DMS	Fortlaufende Prüfung des DMS im Hinblick auf die Angemessenheit und Wirksamkeit auf Basis der Dokumentation des DMS

Abbildung 13: Bestandteile eines Datenschutz-Management-Systems

5. Digitalisierungsspezifische Problembereiche und Handlungsempfehlungen

Aus datenschutzrechtlicher Sicht kommt insbesondere den digitalisierungsspezifischen Themengebieten der Webanalyse bzw. des Webtrackings und der Reichweitenmessung, des Cloud-Computing sowie der Vernetzung von Systemen besondere Bedeutung zu. Durch den Transfer personenbezogener Daten zwischen Geschäftspartnern und Dienstleistern bei vernetzten Systemen stellt sich zuallererst oftmals die Frage, welche Partei welche datenschutzrechtlichen Verantwortlichkeiten übernimmt. Nachstehend werden die Besonderheiten der datenschutzrechtlichen Verantwortlichkeit bei digitalisierungsspezifischen Sachverhalten sowie anschliessend jene der Webanalyse, des Cloud-Computing sowie der Vernetzung von Systemen dargestellt.

5.1 Datenschutzrechtliche Verantwortlichkeit bei digitalisierungsspezifischen Sachverhalten

Werden *personenbezogene Daten* zwischen Unternehmen transferiert, so bestimmen sich die datenschutzrechtliche Verantwortlichkeit und der damit einhergehende Handlungsbedarf danach, wer Mittel und Zwecke der Datenverarbeitung festlegt. Geschieht dies gemeinsam durch zwei oder mehrere Verantwortliche (z. B. aufgrund des gemeinsamen Betriebes einer Datenbank), so ist von einer gemeinsamen Verantwortlichkeit („Joint Controllership") gem. Art. 26 DSGVO auszugehen. Es ist dann ein entsprechender Joint-Controllership-Vertrag abzuschliessen. Darin sind die jeweiligen Verantwortlichkeiten der einzelnen Parteien zu konkretisieren, insbesondere im Hinblick auf die Wahrnehmung der Betroffenenrechte und die Informationspflichten nach den Artikeln 13 und 14 DSGVO (Schneider, 2019). Zusätzlich sind vor allem beim Betrieb gemeinsamer Datenbanken die jeweiligen Datensphären und die TOMs in Abhängigkeit der konkreten Verarbeitungstätigkeiten und der damit einhergehenden individuellen Risiken je Partei zu definieren. Daneben bedarf die Datenübermittlung in diesem, aber auch in jenem Fall, in welchem anstelle der gemeinsamen eine eigene Verantwortlichkeit vorliegt, einer gesonderten Rechtsgrundlage nach Art. 6 DSGVO, da Joint Controller nach Art. 4 Nr. 10 DSGVO sogenannte „Dritte" sind (Dovas, 2016, S. 512). Eine gemeinsame Verantwortlichkeit kann z. B. bei Big Data-Anwendungen, im Bereich des Affiliate-Marketings oder bei der sukzessiven oder gleichzeitigen Verarbeitung bzw. Übermittlung von Daten zwischen Internetplattformen vorliegen (Dovas, 2016, S. 512).

Wird ein Unternehmen lediglich weisungsgebunden und ohne eigene Entscheidungsbefugnis für und im Auftrag einer verantwortlichen Stelle (den Auftraggeber) tätig (z. B. im Rahmen von IT-Support und Wartungsdienstleistungen), so handelt dieses selbst als Auftragsverarbeiter i.S.d. Art. 4 Nr. 8 DSGVO (Auftragnehmer) und ein Vertrag zur Auftragsverarbeitung gem. Art. 28 Abs. 3 DSGVO ist abzuschliessen. Beauftragt ein Auftragsverarbeiter z. B. im Rahmen des Softwarehostings seinerseits selbst einen Auftragsverarbeiter (z. B. einen Cloudanbieter), so ist auch zwischen diesen beiden Parteien ein entsprechender Vertrag unter Berücksichtigung der Besonderheiten der Unterbeauftragung abzuschliessen. Der Auftraggeber sollte sich im Rah-

men seiner Weisungsbefugnis also stets vertraglich zusichern lassen, dass Unterauftragnehmer / Subdienstleister nur mit seiner vorherigen Genehmigung vom Auftragnehmer eingesetzt werden.

5.2 Datenschutzrechtliche Besonderheiten der Webanalyse, des Cloud-Computing sowie der Vernetzung von Systemen

Der Einsatz von Webtracking-Tools (z. B. Google Analytics, Matomo), die Nutzung von Cloudangeboten (z. B. durch Speicherplatz) sowie die Vernetzung von Systemen ziehen jeweils datenschutzrechtliche Besonderheiten nach sich. Dazu sind in Abbildung 14 die jeweiligen grundlegenden Handlungsempfehlungen beispielhaft zusammengefasst. Dabei wird davon ausgegangen, dass *personenbezogene Daten* verarbeitet werden.

Daten als Asset

1. Paradigmenwechsel im Umgang mit Daten ohne Personenbezug

Daten und ihre Verwertung durch Analysemethoden tragen nicht nur zur Realisierung von Effizienzpotenzialen beim Einsatz von Ressourcen bei. Sie eröffnen auch die Weiterentwicklung bestehender und die Einführung neuer Geschäftsmodelle (Geissbauer, Schrauf, Berttram, & Cheraghi, 2017, S. 26). Damit stossen Daten bzw. die hieraus gewonnene Information sukzessive in das Zentrum erfolgsrelevanter Wertschöpfungsfaktoren vor. Das könnte sie zukünftig auf eine Ebene mit Arbeitskraft, Technologie und Kapital als Kernfaktoren der Wertschöpfung heben (Porter & Happelmann, 2015, S. 3; Otto, et al., 2016, S. 10). In Unterscheidung zu den vorgenannten Produktionsfaktoren ist ausserdem zu

Webtracking-Tools (z. B. Google Analytics, Matomo)	Cloud Computing, z. B. in Form von Speicherplatz	Vernetzung von Systemen
· Sicherstes Vorgehen auf Basis einer expliziten Einwilligung · Information der Website-Besucher über Tracking-Methoden in Datenschutzhinweisen · Wahl der jeweils möglichen datenschutzfreundlichen Voreinstellungen	· in der Regel Abschluss einer Vereinbarung zur Auftragsverarbeitung erforderlich · Zusicherung von Serverstandorten in der EU / des EWR empfehlenswert · Anonymisierung der Daten, Einsatz von adäquaten Verschlüsselungstechnologien	· Klärung der datenschutzrechtlichen Verantwortlichkeiten für die Systeme / Systemkomponenten · Wahrung des Grundsatzes der Zweckbindung, Vorsicht bei der Verknüpfung von Datensätzen · Wahrung der Transparenzpflichten gegenüber Betroffenen

Abbildung 14: Handlungsempfehlungen für Webtracking-Tools, Cloud-Computing und der Vernetzung von Systemen

berücksichtigen, dass Daten nicht rivalisierende und nicht abnutzbare (virtuelle) Güter sind (Schmidt, Schmidt & Zech, 2018, S. 627).

Unternehmen stehen in Anbetracht dieses Potenzials nicht mehr nur vor der Frage, wie sie Eigentums- und Nutzungsrechte an herkömmlichen materiellen und immateriellen Wertschöpfungsfaktoren sichern und disponieren, sondern ob und wie entsprechende Rechte auch an Daten als solchen entstehen können.

Im Folgenden wird zunächst auf die Eingrenzung des Datenbegriffs eingegangen. Anschliessend wird aufgezeigt, ob und wie Daten ohne Personenbezug nach geltendem Recht Schutz geniessen.

2. Datenbegriff

Obwohl Daten eine zunehmende wirtschafliche Bedeutung beizumessen ist, sind sie als Rechtsobjekt in den Rechtsordnungen der DACH-Region nur schwer greifbar (Schmidt, Schmidt & Zech, 2018, S. 627; Markendorf, 2018, S. 409). Dort findet sich weder eine Legaldefinition des Datenbegriffs, noch ein allgemeines „Datengesetz" (Schmidt, Schmidt & Zech, 2018, S. 627; Markendorf, 2018, S. 409). Zwar wird im Rechtsgebiet des Datenschutzes der Begriff des personenbezogenen Datums als Information, die sich auf eine identifizierte oder identifizierbare natürliche Person bezieht (Art. 4 Nr. 1 EU-DSGVO) bzw. als Angabe, die sich auf eine bestimmte oder bestimmbare Person bezieht (Art. 3 lit. b DSGVO), definiert. Doch handelt es sich hier lediglich um eine Teilmenge des umfassenderen Datenbegriffs. Vereinzelt ist der Datenbegriff darüber hinaus in straf-[2] und urheberrechtlichen[3] Bestimmungen anzutreffen, jedoch ohne hierin näher definiert zu werden.

Der Versuch einer Schärfung des Datenbegriffs wird von der Literatur zumeist unter Heranziehung der Zeichenlehre (Semiotik) vorgenommen. So lassen sich Daten als maschinenlesbar codierte Information auf der syntaktischen Ebene definieren. Dabei liegen Daten regelmässig auf physikalischer bzw. strukturierter Form auf einem Datenträger vor, der die darstellende Syntaktik ermöglicht (Schmidt, Schmidt & Zech, 2018, S. 627). Auf dieser Ebene sieht die Informatik bei der Zusammenfassung konkreter Wertebereiche und hierauf definierter Operationen zu einer Einheit, bestimmte Datentypen vor. Unter elementaren Datentypen werden ganze, natürliche, Festkomma- und Gleitkommazahlen sowie Aufzählungstypen, logische Werte (sogenannte „Booleans") und Zeichen verstanden (Müller, Käser, Gübell & Klaus, 2009, S. 240). Hiervon werden dynamische und zusammengesetzte Datentypen (Zeichenketten fester, variabler und dynamischer Länge und Zeichenverbund) unterschieden (Müller, Käser, Gübell & Klaus, 2009, S. 240). Oberhalb der syntaktischen Ebene können Daten eine Bedeutung (Semantik) in Form von Information und Wissen aufweisen. Daten lassen sich mithin auf der Bedeutungsebene (semantische Information) und auf der Zeichenebene (syntaktische Information) abgrenzen (Schmidt, Schmidt & Zech, 2018, S. 627).

[2] für Deutschland: §§ 202a ff. StGB, § 303a StGB; für Österreich: §§ 119a, 126a, 225a StGB; für die Schweiz: Art. 143 StGB

[3] für Deutschland: § 4, §§ 87a ff. UrhG; für Österreich: § 40f UrhG, §§ 76a ff. UrhG; Die Schweiz kennt – anders als die EU – kein „Datenbankgesetz" (sui-generis-Schutz) und deshalb auch keine gesetzliche Definition des Begriffs „Datenbank".

Neben dieser semiotischen Eingrenzung des Datenbegriffs können Daten auch nach Ebenen ihrer Entstehung bzw. Verarbeitung kategorisiert werden. Die Abbildung 15 und die Abbildung 16 (s. S. 44) zeigen die Ebenen von Datenerzeugung, Konnektivität, Datenkuratierung sowie -analyse und zuordenbare Datentypen und Verarbeitungszustände exemplarisch anhand des Maschinenparks eines fertigenden Unternehmens.

Ob und wie solche Daten ohne Personenbezug rechtlichen Schutz geniessen können, soll im Weiteren dargestellt werden.

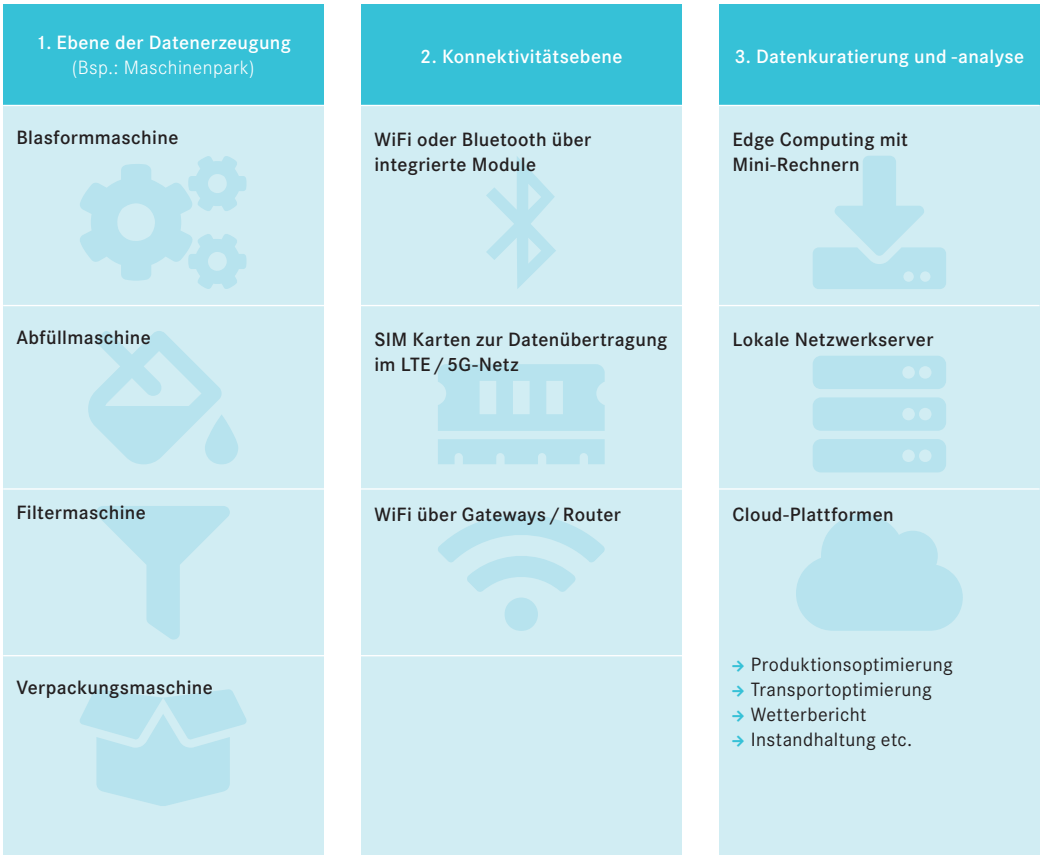


Abbildung 15: Ebenen der Datenverarbeitung am Beispiel eines Maschinenparks (1)

1. Ebene der Datenerzeugung (Bsp.: Maschinenpark)	2. Konnektivitätsebene	3. Datenkuratierung und -analyse
Erzeugungsort Maschine	**Bestimmungsort** Mini-Rechner / Lokaler Netzwerkserver / Cloud-Server	**Weiterer Speicher- / Verarbeitungsort** Mini-Rechner / Lokaler Netzwerkserver / Cloud Server
Inhalt Temperatur	**Inhalt** Temperatur	**Inhalt** Temperatur, Temperaturprofil, Auslastungs- und Abnutzungs-status
Aggregationsstufe Rohdatum	**Aggregationsstufe** Datenpaket	**Aggregationsstufe** Rohdatum, Analyseergebnis, Datenbankelement
Datentyp Primitiv (Zahlen, Zeichen, Wahr-heitswerte) oder Komplex (Arrays, List, Set, Multiset, Zeilen)	**Übertragungsprotokoll** LoRa-WAN-Protokoll	**Datentyp** Primitiv (Zahlen, Zeichen, Wahr-heitswerte) oder Komplex (Arrays, List, Set, Multiset, Zeilen)
Erster Speicherort Lokaler SPS Speicher		
Sphäre intern		**Sphäre** Intern (Edge Computing, lokale Server) und extern (Cloud-Anbie-ter, Applikationsanbieter, etc.)

Abbildung 16: Ebenen der Datenverarbeitung am Beispiel eines Maschinenparks (2)

3. Rechte an nicht personenbezogenen Daten
Wo das Recht einer natürlichen oder juristischen Person Nutzungs- und Verwertungsrechte an materiellen und immateriellen Gütern zuweist, dient dies regelmässig der Schaffung von Rechtssicherheit und Transparenz. Somit können entsprechende Positionen leichter zum Gegenstand vertraglicher Transaktionen gemacht werden (Sattler, 2017, S. 30). Neben der Frage, ob Daten dem sachenrechtlichen oder geistigen Eigentum zugänglich sind, wird in der juristischen Literatur auch ein wettbewerbsrechtlicher und deliktischer Schutz (Recht der unerlaubten Handlung im Zivilrecht) selbiger diskutiert. In Einzelfällen kann ein Zugriff auf Daten auch strafrechtliche Tatbestände erfüllen.

Daten im vorstehend zugrunde gelegten Sinne sind virtuelle Rohmaterialien, die de lege lata keinem normativen Schutzbereich unterfallen (Ensthaler, 2016, S. 3474). Zwar dürfte in Deutschland und Österreich dem Datenbankherstellerrecht bei der methodischen Sammlung, Verarbeitung und Analyse nicht personenbezogener Daten in der Praxis noch die vergleichsweise grösste Bedeutung zukommen (Ehlen, 2016, S. 571; Hürlimann & Zech, 2016, S. 92). Jedoch zielt dieses Recht lediglich auf den Schutz getätigter Investitionen zur Erstellung betreffender Datenbanken ab. Es schützt aber nicht die zugrundeliegenden Einzelelemente, d. h. die Investition in die Erzeugung der Daten als solche. Über den bestehenden normativen Rahmen können höchstens Abwehrrechte aus dem Straf-, Wettbewerbs- oder Deliktsrecht entstehen, die jedoch im Falle der aktiven Zusammenarbeit zwischen vernetzten Wertschöpfungsakteuren (bspw. Lieferanten, Hersteller, Cloud-Anbieter, Softwarehäusern und Kunden) zumeist ins Leere laufen dürften (Żdanowiecki, 2015, S. 23).

Der Vergleich mit Kapitel „Daten mit Personenbezug", führt nun einen wesentlichen Unterschied zum rechtlichen Umgang mit nicht personenbezogenen Daten vor Augen: Das Datenschutzrecht verbietet die Verarbeitung personenbezogener Daten, es sei denn, ein gesetzlicher Erlaubnistatbestand lässt dies zu (Verbot mit Erlaubnisvorbehalt); Daten ohne Personenbezug sind hingegen „vogelfrei", sofern nicht ein gesetzliches oder vertragliches Verbot greift (Erlaubnis mit Verbotsvorbehalt) (Sattler, 2017, S. 46). Nicht *personenbezogene Daten* unterliegen damit dem Grundsatz der Privatautonomie (Sattler, 2017, S. 46).

Hieraus lässt sich also ableiten, dass es aus Unternehmenssicht dringenden Handlungsbedarf für Massnahmen der KMU zur Sicherung des ggf. geschäftskritischen Assets „Daten" gibt.

4. Vertragliche Zuordnung von Daten
Ein Rechtsinstitut zur abschliessenden und eindeutigen Rechtezuweisung an einzelnen Daten, unstrukturierten Datenanhäufungen, aber auch an einzelnen Analyseergebnissen, ist aktuell nicht existent – Daten folgen keiner proprietären Zuweisungslogik (Heymann, 2016, S. 652), ihre Exklusivität kann nur durch faktische Gegebenheiten erreicht werden (Stender-Vorwachs, 2018, S. 1362). Ausserhalb oben beschriebener Rechtskonstrukte kommt deshalb zur Schaffung einer zumindest zwischen Vertragsparteien wirkenden Rechtsklarheit, nur die Ausgestaltung relativ wir-

kender Regelungen im Wege der Vertragsgestaltung in Betracht (Ensthaler, 2016, S. 3474; Chirco, 2016, S. 14; Schlinkert, 2017, S. 224). Streng genommen werden hierbei auch keine Rechte an Daten übertragen, „vielmehr handelt es sich um eine schuldrechtliche Gestattung zur Nutzung der Daten“ (Roßnagel, 2017, S. 12).

Bei einer vertraglichen Zuweisung von Daten und hieran anknüpfender Nutzungsrechte, liegt das rechtliche Risiko zuvorderst bei dem Unternehmen, in dessen Vermögenssphäre die Daten erstmalig generiert werden (Sattler, 2017, S. 46). Um sich im interparteilichen Verhältnis klaren und rechtssicheren Regelungen zu nähern, sollte sich der betreffende faktische „Datenherrscher“ in einem ersten Schritt vergegenwärtigen, wo im Unternehmen welche Daten erfasst werden (siehe erste Ebene „Datenerzeugung“ in Abbildung 16). Anschliessend sollte die Kritikalität anfallender Daten hinsichtlich ihrer strategischen Nutzen- und Risikopotenziale bewertet werden, um letztendlich ableiten zu können, an welchen Schnittstellen welche Daten in welchem Zustand (roh, aggregiert, Datenbank) das Unternehmen verlassen dürfen und sollen (Sattler, 2017, S. 46). Eine nach diesen Fragen ausgerichtete Datenkartierung gibt Aufschluss über die erforderliche Intensität der vertraglichen Bindung etwaiger Partner.

Je nach Bedeutung identifizierter und bewerteter Daten(ströme) sollte dem betroffenen Unternehmen daran gelegen sein, den Umgang mit nicht personenbezogenen Daten entsprechend der festgestellten Kritikalität zu regeln. Einerseits können Regelungen über Daten in den betreffenden Leistungsverträgen der Partner (bspw. Softwarelizenz-, Projekt-, Wartungs- oder Pflegeverträge) aufgenommen bzw. herkömmliche Regelungen solcher Verträge um datenbezogene Aspekte ergänzt werden (Sattler, 2017, S. 48). Alternativ bietet sich die Vereinbarung eines gesonderten Datenlizenzvertrags an.

IT-Sicherheit

Unabhängig davon, in welcher Branche ein KMU angesiedelt ist, wird es sich mittlerweile sehr wahrscheinlich bedeutenden, punktuell sogar existenzgefährdenden Risiken ausgesetzt sehen, die sich in der einen oder anderen Weise auf den Einsatz von Informationstechnologie (IT) zurückführen lassen. Obwohl IT einerseits enorme Nutzenpotenziale für Unternehmen birgt, haben deutsche Unternehmen die Wichtigkeit hiermit verbundener Sicherheitsvorkehrungen erkannt, sei es antizipativ, reaktiv oder – leider – aufgrund der Realisierung entsprechender Risiken im eigenen Unternehmen. Erhebungen, wie die Erfassung der „Hightech-Themen 2018“ oder der „Markt für IT-Sicherheit“ des Bitkom, legen die Richtigkeit dieser These nahe. So wurde IT-Sicherheit in der Umfrage des Bitkom zu den wichtigssten Technologie- und Markttrends zum Topthema 2018 gewählt (Abbildung 17). Der deutsche Markt für IT-Sicherheit scheint diesen Trend mit einem Gesamtumsatzanstieg zwischen 2017 und 2019 (Prognose) in Höhe von 18,9 % (Abbildung 18) widerzuspiegeln.

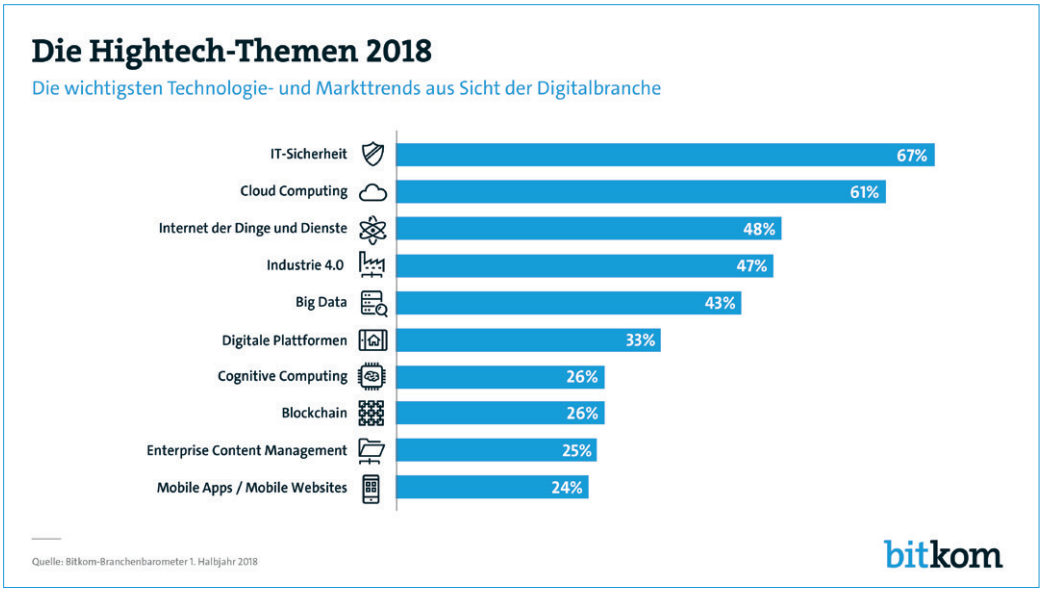


Abbildung 17: Die Hightech-Themen 2018 (Bitkom, 2018a)

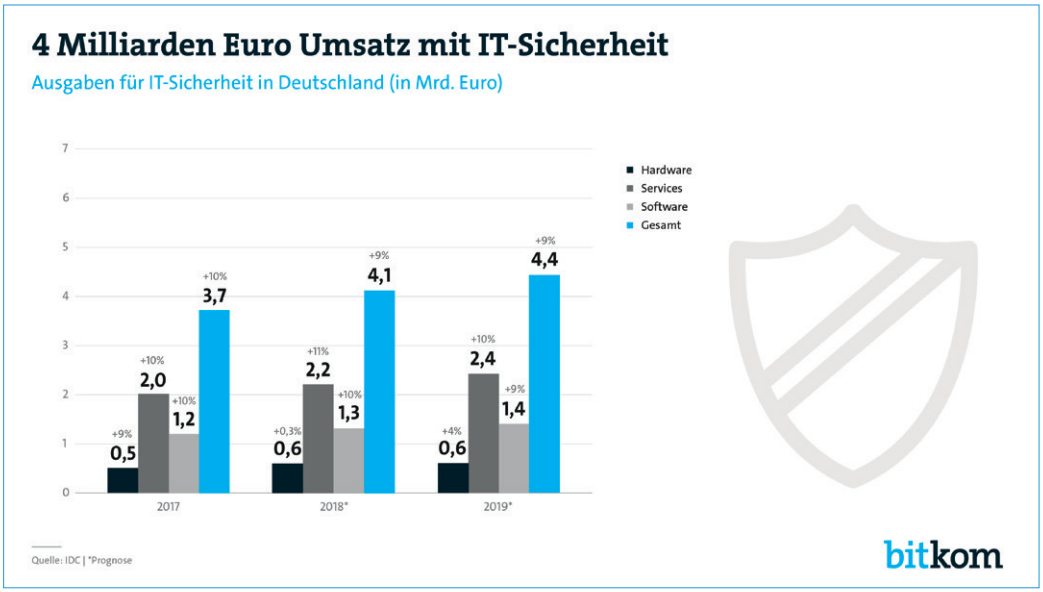


Abbildung 18: 4 Milliarden Euro Umsatz mit IT-Sicherheit (Bitkom, 2018b)

Die Frage, wer für die Implementierung von IT-Sicherheitsmassnahmen im Unternehmen verantwortlich ist, wird von Unternehmen unterschiedlich beantwortet. Während in Schweizer KMU anscheinend grösstenteils die Geschäftsführung das Thema IT-Sicherheit verantwortet (gfs. zürich Markt- und Sozialforschung, 2017, S. 8), trägt hierfür in deutschen Unternehmen überwiegend die hauseigene EDV-Abteilung oder aber ein externer Dienstleister Sorge (Deutsche Telekom / T-Systems, 2014, S. 17).

Ob und wieweit gesetzliche Verpflichtungen über die Implementierung von IT-Sicherheitsmassnahmen bestehen und durch wen diese ggf. wahrzunehmen sind, soll im Folgenden dargestellt werden.

1. Gesetzliche Grundlagen über IT-Sicherheit in den DACH-Staaten

Ein branchenübergreifendes „Gesetz zur IT-Sicherheit" existiert als solches nicht (Voigt, 2018, S. 10). Der rechtliche Rahmen der IT-Sicherheit ergibt sich vielmehr aus der Summe unterschiedlicher Normen. Auf sektoraler Ebene sind dabei insbesondere die NIS-Richtlinie (RICHTLINIE (EU) 2016 / 1148 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union) und die entsprechenden Umsetzungsgesetze in Deutschland und Österreich zu berücksichtigen. Zudem gibt es speziell für Deutschland das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), das Unternehmen, die wichtige Infrastruktur- und Versorgungsleistungen erbringen, zur Einhaltung von Mindest-Sicherheitsstandards verpflichtet (Voigt, 2018, S. 10). Diese rechtlichen Mindestvorgaben beziehen sich zwar nur auf bestimmte Branchen, schaffen aber zumindest in ihrem Anwendungsbereich einen einheitlichen normativen Rahmen. Ausserhalb dieses Anwendungsbereichs ist das Pflichtenprogramm für Unternehmen aufgrund der bestehenden Rechtszersplitterung jedoch nur schwer zu erfassen (Voigt, 2018, S. 10). Auf Grundlage des vorhandenen Rechtsrahmens lassen sich die rechtlichen Anforderungen an die IT-Sicherheit grob wie folgt unterteilen:

(1) ordnungsrechtliche Anforderungen
(2) gesellschaftsrechtliche Anforderungen
(3) vertragsrechtliche Nebenpflichten
(4) IT-Sicherheit „by design"

1.1 Ordnungsrechtliche Anforderungen

Auf europäischer und nationaler Ebene haben die Gesetzgeber die Wichtigkeit hinreichender IT-Sicherheitsmassnahmen erkannt, weshalb auch eine erhöhte legislative Aktivität in diesem Bereich festzustellen ist. Besonders der europäische Gesetzgeber wird zunehmend aktiv, wie die im August 2016 in Kraft getretene NIS-Richtlinie sowie weitere legislative Bestrebungen zeigen (Europäische Kommission, 2018). Auch auf nationaler Ebene werden Unternehmen teils durch neue Gesetze immer stärker in die Pflicht genommen, IT-Massnahmen zu implementieren.

In Österreich wurde die NIS-Richtlinie mit Inkrafttreten des Netz- und Informationssystemsicherheitsgesetzes (NISG) am 29.12.2018 umgesetzt. In Deutschland wurde die NIS-Richtlinie bereits mit dem NIS-Umsetzungsgesetz vom 29.06.2017

umgesetzt, wobei man sich in einer günstigen Ausgangsposition sah, denn in Deutschland besteht mit dem IT-Sicherheitsgesetz seit Juli 2015 bereits ein einheitlicher Rechtsrahmen für mehr IT-Sicherheit bei Kritischen Infrastrukturen (KRITIS), der nur noch angepasst werden musste.

Auch wenn in der Schweiz Forderungen nach einem engmaschigeren normativen Rahmen zur IT-Sicherheit immer lauter werden (Mäder, 2018), findet sich hier bisher nur das „Bundesgesetz über die Informationssicherheit beim Bund". Der Anwendungsbereich dieses Gesetzes ist indes nur auf Behörden und bestimmte Organisationen (die Parlamentsdienste, die Bundesverwaltung, die Verwaltungen der eidgenössischen Gerichte, die Armee, Organisationen nach Artikel 2 Absatz 4 des Regierungs- und Verwaltungsorganisationsgesetzes für ihre Verwaltungsaufgaben) begrenzt, private Unternehmen werden gerade nicht erfasst.

Im Ergebnis dürften ordnungsrechtliche Anforderungen, mit Ausnahme des Datenschutzrechts (siehe hierzu das Kapitel „Daten mit Personenbezug"), für KMU meist unerheblich sein, da in Deutschland und Österreich überwiegend kritische Infrastrukturen in den sachlichen Anwendungsbereich entsprechender Vorschriften fallen. Für kritische Infrastrukturen relevante Rechtsvorschriften können für KMU höchstens im Falle der Wahrnehmung einer Zuliefererfunktion für selbige relevant werden. Telemedien- und telekommunikationsrechtliche Vorschriften zur IT-Sicherheit dürften zwar nur ausnahmsweise einschlägig sein. KMU mit neuartigen Services und vernetzungsfähigen Produkten sollten in diesem Zusammenhang trotzdem prüfen, ob sie als Telemediendienste- oder Telekommunikationsanbieter gelten.

1.2 Pflicht zur IT-Sicherheit aus dem Gesellschaftsrecht

Neben Vorschriften, deren Inhalt sich spezifisch auf den Einsatz von Informationstechnologie stützt, können sich für die Geschäftsleitung eines Unternehmens Pflichten zur Implementierung von IT-Sicherheitsmassnahmen aus Leitungspflichten ergeben. In den Rechtsordnungen der DACH-Region finden sich ähnlich lautende Vorschriften, die der Geschäftsleitung – sei es dem Geschäftsführer einer GmbH oder dem Vorstand bzw. dem Verwaltungsrat einer AG – die Pflicht auferlegen, bei der Geschäftsführung die Sorgfalt eines ordentlichen Geschäftsmannes (GmbH) bzw. eines ordentlichen und gewissenhaften Geschäftsleiters (AG) anzuwenden und die Interessen der Gesellschaft zu wahren.[4] Die Pflichten der Geschäftsleitung ergeben sich dabei einerseits explizit aus gesellschaftsrechtlichen Vorschriften sowie den Statuten der Gesellschaft oder sind andererseits der originären Leitungsaufgabe immanent.

Unter die Pflicht zur sorgfältigen Unternehmensführung fällt nach wohl herrschender Meinung auch die Implementierung von IT-Sicherheitsmassnahmen, als Bestandteil der Organisationspflicht sowie der Pflicht, Schäden vom Unternehmen abzuwenden. Ähnlich der Pflicht zur Compliance, als Ausprägung der sog. Legalitätspflicht, steht der Geschäftsleitung lediglich ein Ermes-

[4] siehe für Deutschland: § 43 Abs. 1 GmbHG, § 93 Abs. 1 S. 1 AktG; Österreich: § 25 Abs. 1 GmbHG, § 84 Abs. 1 S.1 AktG; Schweiz: Artt. 717 Abs. 1, 812 Abs. 1 OR.

sensspielraum hinsichtlich des Umfangs zu implementierender IT-Sicherheitsmassnahmen zu, während das „Ob" zumeist nicht dem „Business Judgement" unterliegen dürfte.

1.3 Vertragsrechtliche Nebenpflichten

Selbst wenn Unternehmen Vertragsbeziehungen eingehen, deren jeweiliger Gegenstand keinen direkten Bezug zu IT-Sicherheit aufweist, können die Parteien im Rahmen der Erfüllung ihrer vertraglichen Nebenpflichten dazu gezwungen sein, IT-Sicherheitsmassnahmen vorzuhalten. Die Verpflichtung zur Rücksichtnahme auf die Rechte, Rechtsgüter und Interessen der anderen Vertragspartei kann die Einhaltung einschlägiger gesetzlicher IT-Sicherheitspflichten auch zu einer vertraglichen Pflicht machen, „da den Vertragspartnern durch Zwischenfälle materielle oder immaterielle Schäden entstehen können" (Voigt, 2018, S. 42). Vertragliche Nebenpflichten zur IT-Sicherheit sind umso bedeutsamer, je abhängiger eine Vertragspartei von den Leistungen und der Wirksamkeit dieser IT-Sicherheit des anderen Vertragspartners ist. Die entsprechenden risikobasierten Massnahmen sind jeweils für den konkreten Einzelfall zu bestimmen (Voigt, 2018, S. 42).

1.4 IT-Sicherheit „by design"

Aufgrund der Vernetzung von Zuliefererkomponenten, Herstellerprodukten sowie unternehmensinternen IT-Systemen werden die vernetzten Objekte selbst zu Quellen für IT-Sicherheitsrisiken (Rockstroh & Kunkel, 2017, S. 77). Von vernetzten Produkten ausgehende Sicherheitsrisiken bedrohen nicht nur Vermögenssphären, in welchen sich betreffenden Produkte letztendlich befinden, sondern alle hiermit sphärenübergreifenden vernetzten Systeme gleichermassen (Bundesamt für Sicherheit in der Informationstechnik, 2013, S. 10; Schlinkert, 2017, S. 222). Daher liegt auch die Vorhaltung produktbezogener IT-Sicherheitsmassnahmen im Interesse aller Wertschöpfungsakteure und Verbraucher.

Hersteller bzw. Verkäufer von IT-Produkten haften für IT-Schwachstellen zunächst regelmässig nach dem allgemeinen kaufrechtlichen Gewährleistungsrecht (Rockstroh & Kunkel, 2017, S. 77). Ein Produkt ist aus kaufrechtlicher Sicht frei von Sachmängeln, wenn es die zwischen den Vertragsparteien vereinbarte Beschaffenheit aufweist oder sich für die gewöhnliche Verwendung eignet.[5] Aus diesem Grund sollten Hersteller und Verkäufer vernetzter Produkte die IT-sicherheitsrelevanten Eigenschaften möglichst umfassend und präzise beschreiben (Rockstroh & Kunkel, 2017, S. 77). Aus delikts-[6] und produkthaftungsrechtlicher Sicht können sich Herstellerpflichten u. a. aus technischen Standards wie IEC 62443 sowie aus den berechtigten Erwartungen der Kunden an die IT-Sicherheit des jeweiligen Produkts ergeben. Es ist dabei stets zu berücksichtigen, dass Software nicht fehlerfrei programmiert werden kann, sich die Bedrohungslagen immer schneller verändern und dass das erforderliche Mass an IT-Sicherheit nur durch Zusammenwirken aller Beteiligten erreicht werden kann (Rockstroh & Kunkel, 2017, S. 77).

[5] für Deutschland: § 434 BGB; für Österreich: § 922 ABGB; für die Schweiz: Art. 197 OR
[6] insbesondere Produzentenhaftung in Deutschland

Cyber-Physische Systeme

Der Begriff des Cyber-Physischen Systems (CPS) beschreibt ein Phänomen der digitalen Vernetzung und Automatisierung. Ein CPS besteht aus einer Vielzahl von Endgeräten, die in ein einheitliches, oft unternehmensübergreifendes Netzwerk integriert sind, in welchem sie miteinander kommunizieren und angesteuert werden können (Bundesministerium für Bildung und Forschung, 2015, S. 6). Ein typisches CPS ist beispielsweise eine digital integrierte, industrielle Wertschöpfungskette, deren Bestelloberflächen, Industrieroboter, Smart-Lager, Logistikroboter und sogar Endprodukte allesamt miteinander Daten austauschen und zentral angesteuert werden können. Wichtiges Merkmal eines CPS ist seine Fähigkeit, koordiniert und ohne menschliches Zutun auf Veränderungen in seiner Umwelt zu reagieren (Bruch, 2015, S. 87). So kann das beschriebene System bei einem Auftragseingang selbstständig Produktionsprozesse anstossen, die notwendigen Bauteile bestellen und Lagerraum freiräumen.

In der Praxis bieten diese Systeme potenziell beachtliche Effizienzvorteile. Sie verursachen aber technische Herausforderungen bei ihrer Implementierung und werfen eine Reihe von Rechtsfragen auf. Da sich diese Fragen vor allem mit der Haftung für eventuelle Fehler des Systems befassen, sind sie nicht nur für Nutzer von CPS relevant, sondern auch für deren Kunden und Geschäftspartner.

1. Vertragsrechtliche Implementierung eines CPS

Die Komplexität eines CPS spiegelt sich in den für eine Implementierung notwendigen vertraglichen Strukturen wider. Im Mittelpunkt steht das Verhältnis zwischen dem Betreiber und dem Hersteller bzw. Provider der CPS-Endgeräte. Da der Provider, neben der reinen Überlassung der Endgeräte, regelmässig auch eine Reihe von internetbasierten Diensten rund um deren Steuerung und Vernetzung erbringt, lässt sich das Betreiber-Provider-Verhältnis meist nur als typengemischter Vertrag zusammenfassen. Dieser kann wiederum, nach den Umständen des Einzelfalls, kauf-, miet-, dienst-, oder werkvertragliche Elemente enthalten (Heuer-James, Chibanguza & Stücker, 2018, S. 2823; Horner & Kaulartz, 2016, S. 24). Wird die Konnektivität der Endgeräte nicht durch die IT-Infrastruktur des Betreibers gewährleistet, so ist es regelmässig notwendig, hierzu zusätzlich einen Mobilfunkanbieter einzuschalten, welcher im Rahmen eines Dienstvertrages Datenvolumen zur Verfügung stellt (Langer, 2016, S. 29).

2. Zurechnung von Systemverhalten

Die Frage der Zurechnung des Verhaltens eines CPS zu einer Vertragspartei ist von grosser Bedeutung für die Praxis, jedoch rechtlich noch in weiten Teilen unklar. Grund hierfür ist die vermeintliche Autonomie eines CPS. Dieses besitzt freilich keinen eigenen Handlungswillen, vielmehr reagiert es auf Basis von Verknüpfungen und Algorithmen auf seine Umwelt. Dieser Entscheidungsfindungsprozess wird durch eine Vielzahl von Faktoren beeinflusst – hierzu zählen insbesondere die zur Steuerung verwendete Software,

die Struktur der Vernetzung sowie die konkret von den verschiedenen Endgeräten erhobenen und eingespeisten Daten (Horner & Kaulartz, 2016, S. 24). Von besonderer Bedeutung ist dabei, dass an einem CPS beteiligte Parteien möglicherweise einen massgeblichen Einfluss auf das Verhalten von nicht in ihrem Besitz stehenden Endgeräten ausüben können (Pieper, 2016, S. 189). Durch die Komplexität des CPS wird die Nachvollziehbarkeit von Systemverhaltensweisen eingeschränkt. Die Schaffung des Rechtskonstrukts einer elektronischen Person zur Bewältigung dieses Problems ist nach herrschender Meinung aus systematischen und praktischen Gründen nicht überzeugend (Kluge & Müller, 2017, S. 31; Heuer-James, Chibanguza, & Stücker, 2018, S. 2818). Mangels einer universellen Lösung gilt es an dieser Stelle stattdessen, bestimmte Zurechnungstatbestände individuell zu untersuchen.

Im Falle eines Vertragsabschlusses durch ein autonomes System hat grundsätzlich der Betreiber des CPS für die Erfüllung dieses Vertrags einzustehen. Freilich mag nicht immer gewiss sein, ob eine Willenserklärung des Systems auch den Willen des Betreibers widerspiegelt, jedoch ist es erst der Betreiber, der durch Einsatz eines CPS ein solches Risiko schafft (ausführlicher hierzu: Heuer-James, Chibanguza & Stücker, 2018, S. 2822; Groß, 2018, S. 5). Zum Schutze der Rechtssicherheit im Geschäftsverkehr sollte dieser daher auch Verantwortung für die Erfüllung der vertraglichen Leistungspflichten tragen.

Verursacht ein CPS eine vertragliche Pflichtverletzung, z. B. eine Fehllieferung, so hat dessen Betreiber diese nicht von vornherein als sein eigenes Verschulden zu vertreten. Das CPS ist nicht als Erfüllungsgehilfe des Betreibers zu behandeln (Heuer-James, Chibanguza, & Stücker, 2018, S. 2829), vielmehr muss sich Letzterer nur seine eigene Einflussnahme auf das System zurechnen lassen. Dies ermöglicht eine Exkulpation im Rahmen der schuldrechtlichen Beweislastumkehr, sofern sich in der Praxis festzustellen lässt, welche Faktoren und Inputs für das Fehlverhalten des Systems massgeblich waren, welche nicht dem Betreiber zuzurechnen waren (Horner & Kaulartz, 2016, S. 24).

Handelt ein CPS schliesslich deliktisch, so bietet sich eine Haftungszurechnung über die Annahme von Verkehrssicherungspflichten an (Rempe, 2016, S. 18). Der Betreiber des CPS handelt demnach kausal deliktisch, wenn er es unterlässt, nach dem Herbeiführen einer Gefahrenlage durch Implementierung eines autonomen Systems, die notwendigen Massnahmen zum Schutze des Verkehrs zu treffen. Bei der Bestimmung des Verschuldens ist dann auf die subjektive Vorhersehbarkeit der Schädigung abzustellen (Rempe, 2016, S. 19). Jedoch ist auch dieser Ansatz in der Anwendung problematisch. Zum einen bedarf er einer klaren Risikoverteilung, d. h. einer Festlegung, welcher CPS-Teilnehmer für welchen Aspekt der übergeordneten „Gefahrenlage“ verantwortlich ist. Zum anderen besteht bislang kein fester Massstab für den Umfang der zur Verkehrssicherung notwendigen Massnahmen (Heuer-James, Chibanguza & Stücker, 2018, S. 2830).

3. Regulatorische Fragen

Die Konnektivität von CPS-Endgeräten wird in der Praxis regelmässig mithilfe von Mobil-

funknetzen gewährleistet. In einem solchen Fall liegt in der Bereitstellung dieser Konnektivität ein Telekommunikationsdienst (TK-Dienst) im Sinne des Telekommunikationsgesetzes vor (Grünwald & Nüßing, 2015, S. 381). Erbringer dieses TK-Dienstes sind entweder der Mobilfunkanbieter selbst oder möglicherweise der Provider, sofern dieser Konnektivität von einem „Primäranbieter" bezieht und dann an seine Nutzer weiterverkauft (Sassenberg & Kiparski, 2017, S. 18). TK-Dienste unterliegen einigen gesetzlichen Sonderregelungen, insbesondere bestimmten Kundenschutzvorschriften, dem Fernmeldegeheimnis, dem Kommunikationsdatenschutz sowie einer Haftungsbeschränkung bei fahrlässig verursachten Vermögensschäden (Grünwald & Nüßing, 2015, S. 381).

Ein CPS erhebt und verarbeitet regelmässig Daten, sowohl mit als auch ohne Personenbezug. Bei deren Implementierung und Nutzung ist daher stets die Gewährleistung des personen- wie auch unternehmensbezogenen Datenschutzes zu beachten, wie er im Kapitel „Daten mit Personenbezug" dargestellt wird.

Cloud-Computing und digitale Plattformen

Die Durchdringung von Wirtschaft und Gesellschaft durch Informations- und Kommunikationstechnologie ist ein zentrales Kennzeichen der heutigen Zeit. Disruptive Innovationen und Geschäftsmodelle mit einer zunehmenden Serviceorientierung zwingen die meisten Branchen zur *Digitalisierung* (Hahn, 2016, S. 595). Lösungsansätze im Zuge dieser digitalen Transformation bieten digitale Plattformen, deren infrastruktureller Kern das Cloud-Computing ist. Im Folgenden werden daher zunächst die Formen des Cloud-Computing und seine typischen Rechtsfragen und dann das Themenfeld der digitalen Plattformen dargestellt.

1. Cloud-Computing

Unter Cloud-Computing wird ein Geschäftsmodell im Informationstechnologie-Sektor verstanden, bei dem der Cloud-Anbieter dem Cloud-Nutzer IT-Leistungen wie Speicherplatz und Anwendungsprogramme über das Internet zur Verfügung stellt (Böhm, Leimeister, Riedl, & Krcmar, 2009, S. 8). Diese IT-Leistungen werden in der sogenannten Cloud bereitgehalten, einem Verbund aus mehreren Servern, der vom Cloud-Nutzer „wie ein grosser Computer verwendet werden kann" (Lehmann & Giedke, 2013, S. 609). Cloud-Computing kann anhand der drei Leistungsarten Software as a Service (SaaS), Platform as a Service (PaaS) und Infrastructure as a Service (IaaS) unterschieden werden. SaaS-Angebote erlauben den Zugriff auf Anwendungsprogramme, die auf der Infrastruktur des Cloud-Anbieters installiert sind. PaaS-Angebote ermöglichen dem Cloud-Nutzer den Zugriff auf Programmier- und Entwicklungsumgebungen zur Entwicklung und zum Betrieb von Software. Bei IaaS-Angeboten stellt der Cloud-Anbieter seiner Kundschaft eine virtualisierte Rechenzentrumsinfrastruktur (z. B. Server, Storage, Netzwerk) über das Internet zur Verfügung. Erhebungen von Eurostat und der Hochschule für Wirtschaft Zürich zeigen, dass die Nutzung von Cloud-Computing in Unternehmen zunimmt, mithin also immer mehr Unternehmen ihren Betrieb von E-Mail-, Office- oder Kommu-

nikationsprogrammen in die Cloud auslagern Dies sind zumeist jedoch grosse Unternehmen (Eurostat, 2018; Institute for Digital Business, 2018). Der Vorsprung ist nicht zuletzt auf den Umstand zurückzuführen, das grosse Unternehmen häufiger als kleine Unternehmen eine Digitalisierungsstrategie verfolgen, wodurch Cloud-Computing eine stärkere Beachtung erfährt (Brink, Dienes, Icks, & Schröder, 2017, S. 6). Gleichwohl profitieren auch KMU von Cloud-Computing: Die *Digitalisierung* von Geschäftsprozessen und die Gestaltung neuer Geschäftsmodelle können mit reduziertem Investitionsaufwand verwirklicht werden, weil die Beschaffung und der Betrieb eigener Infrastrukturen und Anwendungen entfallen. Erfolgt die Abrechnung mit dem Cloud-Anbieter zudem nach Massgabe der tatsächlichen Nutzung, können Fixkosten variabilisiert werden (sogenanntes „pay as you go"-Prinzip).

Die nachfolgende Betrachtung erfolgt aus der Perspektive eines KMU, das Cloud-Computing-Dienste bezieht. In diesem Kontext stellen sich insbesondere rechtliche Fragen mit Bezug zum Vertrags-, Urheber- und Datenschutzrecht.

1.1 Vertragsrechtliche Fragestellungen

Bezieht das Unternehmen Cloud-Dienste, so schliesst es mit dem Cloud-Anbieter einen Cloud-Computing-Vertrag ab. Das eröffnet Fragen in Bezug auf die Vertragsgestaltung und die rechtliche Einordnung als Miet-, Dienstleistungs- oder Werkvertrag (der Dienstvertrag des deutschen Rechts entspricht dem Auftrag im schweizerischen Recht). Im Zuge der Vertragsgestaltung hat der Cloud-Nutzer auf Regelungen zu achten, die ihm eine ausreichende Kontrolle und Einflussnahme auf den Cloud-Anbieter gewähren, um seinen Pflichten bezüglich einer angemessenen Risikosteuerung nachzukommen. Beispielhaft zu nennen sind Regelungen, die Vor-Ort-Prüfungen oder einen Zustimmungsvorbehalt bei der Beauftragung von Unterauftragnehmern gewähren[7]. Die rechtliche Einordnung des Cloud-Computing-Vertrags ist bedeutsam, um bei auftretenden Mängeln, etwa der Nichtverfügbarkeit gespeicherter Daten oder deren Verlust, eine rechtliche Lösung zu finden. Aufgrund der Vielseitigkeit von Cloud-Diensten ist eine einheitliche Zuordnung des Vertrags zu einem Vertragstyp weder möglich noch sinnvoll (De la Cruz, 2013). Diese kann nur im Einzelfall und unter Beachtung des rechtlichen oder wirtschaftlichen Schwerpunkts jedes einzelnen Vertragsbestandteils erfolgen (Grüneberg, 2019). Indes geht die rechtswissenschaftliche Literatur der DACH-Region dazu über, die gängigen Cloud-Leistungen, namentlich das Bereitstellen von Speicherplatz und Software, mehrheitlich dem Mietrecht zu unterwerfen[8], sodass der Cloud-Anbieter für Schäden an der überlassenen Sache haftet, die infolge eines Mangels auftreten.

1.2. Urheberrechtliche Fragestellungen

Mit dem Abschluss eines Cloud-Computing-Vertrags stellt der Cloud-Anbieter dem Nutzer regelmässig digitale Inhalte, zumeist Software,

[7] Weitere Empfehlungen mit Bezug zur Finanzbranche sind etwa dem Merkblatt „Orientierungshilfe zu Auslagerungen an Cloud-Anbieter" (Bundesanstalt für Finanzdienstleistungsaufsicht, 2018) zu entnehmen.

[8] für Deutschland siehe u.a. Nägele & Jacobs, 2010, S. 284 und Wicker, 2014, S. 786; für Österreich siehe u.a. Stögerer, 2013, S. 66; für die Schweiz siehe u.a. De la Cruz, 2013.

über das Internet zur Verfügung. Obgleich der Begriff „Cloud" suggeriert, dass die zum Abruf bereitgestellten Daten nicht fassbar und sozusagen in Luft aufgelöst wären, befinden sich sämtliche digitalen Inhalte auf einem physischen Datenträger (Stieper, 2019, S. 1). Die Cloud-Nutzung, also die Verwendung der bereitgestellten Software und Hardware, kann somit einen Eingriff in die Rechte des Urhebers der Inhalte bedeuten und erlaubnispflichtig sein[9]. Daher ist zu prüfen, ob die Cloud-Nutzung ein entsprechendes Recht, namentlich das Recht zur Vervielfältigung, bedingt. Mit Blick auf die Rechtsordnungen der DACH-Region kann hierauf eine einhellige Antwort gegeben werden: Die mit einem SaaS-Modell verbundene reine Softwarenutzung durch das KMU erfordert kein Nutzungsrecht, unabhängig davon, ob auf die Software mittels eines auf dem Rechner des Nutzers installierten Cloud-Clients zugegriffen wird oder sich eine vorübergehende Kopie der Software im Arbeitsspeicher des Nutzers befindet (Strittmatter, 2016; Stögerer, 2013, S. 157; Neuenschwander, 2014, S. 40). Während das Anmieten von Cloud-Infrastruktur, z. B. von Speicherplatz, urheberrechtlich bedeutungslos ist (Stögerer, 2013, S. 176), stellt das Hochladen urheberrechtlich geschützter Inhalte in diesen „eigenen" Cloud-Speicher eine erlaubnispflichtige Vervielfältigungshandlung dar, für die der Cloud-Nutzer ein entsprechendes Recht benötigt (Schäfer, 2014; Stögerer, 2013, S. 176; Beranek Zanon & De la Cruz, 2013, S. 672). Nutzerseitig ist daher zu prüfen, ob der Vertrag, auf dessen Grundlage die Inhalte erworben wurden, eine Nutzung in der Cloud gewährt.

1.3. Datenschutzrechtliche Fragestellungen

Werden bei der Nutzung von Cloud-Computing *personenbezogene Daten* verarbeitet, sind datenschutzrechtliche Bestimmungen zu beachten. Unter dem Regime der europäischen EU-DSGVO und des schweizerischen Bundesgesetzes über den Datenschutz stellt Cloud-Computing eine Datenverarbeitung durch Dritte dar (Kramer, 2018, S. 54; Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, 2018), weswegen datenschutzrechtliche Fragestellungen im Wesentlichen um die rechtskonforme Einbindung des Cloud-Anbieters als Auftragsverarbeiter und dessen Kontrolle durch den Cloud-Nutzer kreisen. Regelungen hierzu sind vertraglich (z. B. in einem Auftragsverarbeitungsvertrag) festzuhalten. Sie umfassen neben Art, Dauer und Zweck der Verarbeitung vor allem die vom Cloud-Anbieter getroffenen technischen und organisatorischen Massnahmen, um die Daten gegen einen unbefugten Zugriff zu schützen. Folglich hat der Cloud-Nutzer den Cloud-Anbieter sorgfältig und anhand einer umfassenden Risikoeinschätzung auszuwählen. Der US-Kongress verabschiedete den „Clarifying Lawful Overseas Act" (CLOUD Act), der amerikanische Cloud-Anbieter zur Offenlegung der gespeicherten Daten verpflichten kann (Cording, 2018, S. 637). Diesbezüglich ist auf den Grundsatz hinzuweisen, dass von einer Auslagerung der Daten in die Cloud, insbesondere eine ausländische Cloud, abzusehen ist, „je vertraulicher, geheimer, wichtiger [...] oder sensitiver [...] die Daten sind" (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, 2018).

[9] Eine nicht abschliessende Aufzählung der Rechte des Urhebers ist den folgenden Vorschriften zu entnehmen: § 15 UrhG [Deutschland]), § 14 ff. UrhG [Österreich], Art. 10 URG [Schweiz].

2. Digitale Plattformen

Digitale Plattformen gehören zu den Hauptakteuren der *Digitalisierung*. Dabei handelt es sich um internetbasierte Foren für digitale Interaktion und Transaktion, welche sich in praktisch jeder Branche finden (Bundesministerium für Wirtschaft und Energie, 2017, S. 21). Indem digitale Plattformen als Intermediäre die Interaktion zwischen verschiedenen Nutzergruppen ermöglichen oder erleichtern, fördern sie deren Beteiligung, wodurch ein zweiseitiger oder mehrseitiger Markt entsteht (Bundeskartellamt, 2016, S. 21).

Durch die Interaktion verschiedener Nutzergruppen entwickeln sich Netzwerkeffekte, welche sowohl in direkter Form innerhalb einer Nutzergruppe, als auch in indirekter Form zwischen verschiedenen Nutzergruppen auftreten können. Gerade für KMU bedeuten digitale Plattformen einen neuen Marktzugang, der aufgrund der mit der Unternehmensgrösse verbundenen geringen Reichweite und Marktbekanntheit sonst nicht möglich wäre (Engert, 2018, S. 308). Durch die Nutzung digitaler Plattformen als eine neue Art der „Marktinfrastruktur" (Engert, 2018, S. 307) ergeben sich jedoch auch zahlreiche rechtliche Unsicherheiten, die im Folgenden kurz dargestellt werden. Plattformen können sowohl als Vermittlerinnen von Transaktionen auftreten, als auch die Rolle des Nutzers einer Plattform, als Anbieter oder Nachfrager von Waren oder Dienstleistungen einnehmen. Als Intermediär für Transaktionen ist insbesondere die Frage relevant, welche wettbewerbsrechtlichen Regelungen sowie vertragsrechtliche und datenschutzrechtliche Pflichten den Plattformbetreiber treffen. Als Nutzer der Plattform ist hingegen von Bedeutung, welche Ansprüche Unternehmen gegen Plattformbetreiber haben.

2.1. Wettbewerbsrechtliche Fragestellungen

Da kleinere Unternehmen im Bereich des Internethandels oft von der Infrastruktur grosser Plattformen abhängig sind, stellt sich die Frage inwieweit sie sich vor unlauteren Geschäftspraktiken der Plattformbetreiber schützen können. Sind die Aktivitäten des Plattformbetreibers, wie beispielsweise die Vermittlung von Transaktionen oder das zur Verfügung stellen von Informationen als geschäftliche Handlung zu sehen, fallen sie unter die Bestimmungen des Lauterkeitsrechts [10]. Die strengeren unter den lauterkeitsrechtlichen Regelungen schützen sowohl Anbieter als auch Nachfrager vor unlauteren Geschäftspraktiken der Plattformbetreiber. Vor allem Vermittlungs- und Vergleichsplattformen lassen sich die Aufnahme eines Anbieters vergüten, wodurch KMU durch ihre geringere Finanzkraft einen Nachteil gegenüber grossen Konkurrenten erleiden (Engert, 2018, S. 318) (Bundesgerichtshof, 2014, S. 879). Weist der Plattformbetreiber nicht entsprechend auf derartige Praktiken hin, kann sich daraus ein wettbewerbsrechtlicher Unterlassungsanspruch auf Seiten der Plattformnutzer ergeben. [11]

2.2. Kartellrechtliche Fragestellungen (insbesondere Datenzugang)

Nehmen Plattformen eine marktbeherrschende Stellung ein, kann dies zum Nachteil für Anbieter führen, die von dieser Infrastruktur abhängig sind. Um KMU einen diskriminierungsfreien Zu-

[10] für Deutschland § 2 Abs. 1 Nr.1 UWG; für Österreich § 1 Abs. 1 Nr. 1 UWG; für die Schweiz Art. 2 UWG.
[11] Unterlassungsanspruch in Deutschland gem. § 8 Abs. 1 UWG; Österreich § 15 UWG und Schweiz gem. Art. 9 Abs. 1 UWG.

gang zum Markt zu gewähren, müssen die kartellrechtlichen Regelungen an das digitale Zeitalter angepasst werden. Die einleitend erwähnten Netzwerkeffekte können auch eine kartellrechtliche Bedeutung erlangen, wenn sich ein Selbstverstärkungseffekt entwickelt, der das Unternehmen exponentiell schnell wachsen lässt (Sura, 2017, S. 194). Bisherige Kriterien der marktbeherrschenden Stellung, wie z. B. hohe Marktanteile bei digitalen Plattformen, sind nicht zwingend Anzeichen für Marktmacht. Deshalb wurden im deutschen Gesetz gegen Wettbewerbsbeschränkungen bezüglich einer Beurteilung der Marktbeherrschung neue Kriterien aufgenommen, die das Kartellrecht an die Eigenschaften digitaler Märkte anpassen sollen (Deutscher Bundestag, 2016, S. 38). Auf europäischer Ebene fehlen dementsprechende Vorschriften bisher. Dieser Katalog beinhaltet unter anderem den Zugang zu wettbewerbsrelevanten Daten und soll insbesondere kleineren Unternehmen einen diskriminierungsfreien Zugang zum digitalen Markt gewährleisten. Für Anbieter kann der fehlende Zugang, bspw. zu Kundendaten, durch die Nutzung der Plattform einen erheblichen Nachteil darstellen (Busch, 2018, S. 151). Ein Recht auf Datenzugang ist in den Rechtsordnungen der DACH-Region bisher nur aus wettbewerbsrechtlicher Sicht denkbar, wenn der Marktzugang explizit vom Zugang zu spezifischen Daten abhängt. Dies ist jedoch auch nur dann relevant, wenn die Zugangsverweigerung einen Missbrauch der marktbeherrschenden Stellung darstellt (Peitz & Schweitzer, 2018, S. 279).

2.3. Vertragsrechtliche Fragestellungen

Plattformen bieten Händlern eine Infrastruktur, durch die sie ihre Produkte einer breiten Masse an potenziellen Kunden anbieten können, während Nutzer sich einen Überblick über die Marktsituation verschaffen und Angebote miteinander vergleichen können. Für die Bereitstellung dieser Infrastruktur erhält der Plattformbetreiber in der Regel eine Vergütung und für zustande gekommene Transaktionen eine Vermittlungsprovision. Auch wenn kein Vertrag zwischen Nutzer und Plattformbetreiber zustande kommt, lassen sich die Grundsätze der Haftung Dritter auf den digitalen Plattformmarkt übertragen (Hauck & Blaut, 2018, S. 1427). Bei Vergleichsplattformen ist ebenfalls für eine Haftung entscheidend, ob der Plattformbetreiber mit dem Anbieter einen Vertrag über die Positionierung seiner Angebote in einer Rangliste gegen eine Vergütung geschlossen hat oder ob ein Plattformanbieter nur Anbieter miteinbezieht, für deren Angebote er eine solche Vergütung erhalten hat. Entscheidend ist, ob dies für den Nutzer erkennbar ist oder nicht und ob der Nutzer auf die Richtigkeit und Vollständigkeit des Produktvergleichs vertrauen darf. [12]

2.4. Datenschutzrechtliche Fragestellungen

Für digitale Plattformen sind vor allem Nutzerdaten im Austausch gegen Leistungen fester Bestandteil des Geschäftsmodells. Das Datenschutzrecht fordert für jede Verarbeitung personenbezogener Daten entweder eine Einwilligung des Betroffenen oder einen gesetzlichen Erlaubnistatbestand. Dieser Austausch wirft jedoch die Frage der Wirksamkeit einer solchen

[12] AGB-Kontrolle nach jeweils geltendem Recht: Deutschland §§ 305 ff. BGB, Schweiz und Österreich beziehen Regelungen aus Lehre und Rechtsprechung; in Österreich zudem noch § 6 KschG für Verbraucher.

Einwilligung auf, die nach Art. 7 Abs. 4 DSGVO freiwillig zu erfolgen hat und eben gerade nicht die Bedingung zur Erfüllung eines Vertrages sein darf. Je nach Beurteilung der Angemessenheit dieses Austauschverhältnisses „Dienste gegen Daten" kann die Einwilligung in solchen Fällen unwirksam sein (Peitz & Schweitzer, 2018, S. 276).

Die Zulässigkeit der Datenverarbeitung kann sich auch aus einem gesetzlichen Erlaubnistatbestand ergeben. Die Generalklausel des Art. 6 lit. F. DSGVO fordert für die Erlaubnis zur Datenverarbeitung eine Interessenabwägung. Je nach Geschäftsmodell ist das Interesse des Dienstanbieters darauf ausgerichtet die Dienstleistung, insbesondere wenn sie unentgeltlich angeboten wird, durch Werbung oder die anderweitige wirtschaftliche Verwertung der personenbezogenen Daten des Nutzers zu finanzieren (Schweitzer, 2017, S. 273). Die für solche Geschäftsmodelle benötigte Rechtssicherheit ist auf Seiten der Unternehmen jedoch weder durch die Einzelfallabwägung der zulässigen Einwilligung noch durch eine Interessenabwägung gegeben. Fehleinschätzungen bezüglich der Einwilligung oder des gesetzlichen Erlaubnistatbestandes können Sanktionen nach sich ziehen, welche besonders für KMU ein erhebliches finanzielles Risiko darstellen (Schweitzer, 2017, S. 282).

Die Verarbeitung ist ausserdem gem. Art. 6 Abs. 1 lit. b dann rechtmässig, wenn sie zur Erfüllung eines Vertrages erforderlich ist. Dies ist dann der Fall, wenn der Vertrag ohne die Verarbeitung nicht erfüllt werden könnte (Frenzel, 2018).

Branchenspezifische Sachverhalte

Neben branchenübergreifenden Sachverhalten wurden im Rahmen des Forschungsprojektes auch spezifische Sachverhalte einzelner Branchen untersucht. Die Ergebnisse können über den nachstehenden QR-Code abgerufen werden.

- Gesundheit und Sozialwesen
- Gastgewerbe, Tourismus, Freizeitgestaltung und Verkehr
- Handel und Vertrieb
- Fertigende Industrie
- Handwerk und Bau
- Logistik

Autoren: Manuel Treiterer, Nicole Neubrander, Philipp Kopka, Thilo Jansch, Miriam Ebinger

Abbildung 19: Branchenspezifische Sachverhalte
→ http://www.kmu-digital.eu/de/projekte/dab-recht


PRIAMUS

Verbindende und trennende Elemente der Digitalisierung im Bereich Politik, Person

Daten in Kooperationsbeziehungen

Bereits das Grünbuch „Digitale Agenda Bodensee – Eine Bestandsaufnahme zum Potenzial der *Digitalisierung* innerhalb KMU in der *Bodenseeregion*“ konnte zeigen, dass *kleine und mittlere Unternehmen (KMU)* der *Bodenseeregion* hauptsächlich an Kooperationsmöglichkeiten mit anderen Akteuren innerhalb und ausserhalb ihrer Branche interessiert sind. Ihr Ziel ist es, voneinander zu lernen und miteinander zu kooperieren.

In der Relevanzbewertung nehmen die Themenbereiche Infrastruktur und Ordnungs- und Rechtsrahmen eine zentrale Rolle ein. Innerhalb des Bereiches des Ordnungs- und Rechtsrahmens sind es dann insbesondere offene Fragen im Umgang mit Daten, welche die Bodensee-KMU umtreibt. Verknüpft man diese Themenbereiche miteinander, kann man feststellen, dass sich auf der einen Seite natürlich auf Basis neuer digitaler Infrastruktur (z. B. Cloud-Plattformen) völlig neuartige Möglichkeiten und Chancen der Kooperation ergeben. Auf der anderen Seite stellen sich auch neue Fragen zum Umgang mit den Daten.

In Zukunft werden sicherlich vermehrt kooperationsartige Zusammenschlüsse zwischen Wertschöpfungsakteuren auftreten. Damit werden perspektivisch auch KMU intensiver auf den möglich gewordenen Daten- und Informationsaustausch mittels digitaler Plattformen und hierüber vernetzter Cyber-physische Systeme zurückgreifen.

Aufgrund technischer Gegebenheiten und der gesetzlichen Ausgangslage (siehe hierzu Kapitel „Daten als Asset“) sollte die Regelung vertraglicher Nutzungsrechte an Daten eine zentrale Rolle in Kooperationsvereinbarungen einnehmen. Im Unterschied zu Verträgen über datenbasierte Leistungen sollten bei kooperativen Vorhaben Überlegungen angestellt werden, Daten nicht als proprietäres, sondern als kooperatives Gut anzusehen, an welchem auf vertraglichem Wege Nutzungsgemeinschaften im Sinne einer Quasi-Bruchteilsgemeinschaft vereinbart werden. Dieser Ansatz steht mithin in Konkurrenz zur relativ wirkenden Vereinbarung eines „Datenherrschers“ im Vertragsverhältnis, der im Innenverhältnis zwischen den Vertragsparteien nach einem proprietären Modell bestimmt, wer Daten wie nutzen darf.

Im Rahmen einer solchen kooperativen „Data Governance“ (Otto, et al., 2016, S. 19) ist eine Abwägung über Chancen und Risiken im Umgang mit Daten zu treffen. Hieraus abgeleitete Regelungen sind zu formulieren, welche die teilnehmenden Akteure gleichermassen verpflichten und berechtigen. Schliesslich gewähren Daten aus der Sphäre des jeweiligen Übermittlers bisweilen tiefe Einblicke in die Nutzung und Funktion von Komponenten, Produkten sowie Dienstleistungen (Peschel & Rockstroh, 2014, S. 574; EU-Kommission, 2017, S. 27). Deshalb ist neben den positiven Effekten einer gemeinsamen Datennutzung auch stets das Risiko einer nachteiligen Zweckentfremdung überlassener Daten zu bedenken.

Aufgrund des Interesses am kooperativen Wirken sollten deshalb Rahmenbedingungen zur

al und Recht

Datennutzung als Antwort auf das zwiespältige Potenzial vorgesehen werden.

Die vereinbarte Data Governance sollte abgrenzen, zu welchen Zwecken die beitragenden Parteien ihnen übertragene oder auf gemeinsamen Data Spaces abgelegte Daten verwenden dürfen. Darüber hinaus ist der Modus einer Übertragung betreffender Daten an Dritte zu regeln. So könnte beispielsweise eine Weitergabe von Daten an Dritte stets von der Zustimmung der anderen Kooperationspartner abhängig gemacht werden oder nur nach erfolgter Anonymisierung betreffender Daten im Sinne der Auflösung eines gegebenenfalls bestehenden Unternehmensbezugs erfolgen. Ein alternativer Regelungsweg sähe Benachrichtigungspflichten über das Vorhaben einer Weiterleitung in Kombination mit Widerspruchsrechten vor, wobei die Entstehung eines Sperrmonopols bei Möglichkeit verhindert werden sollte (Ensthaler, 2016, S. 3477; Schlinkert, 2017, S. 224).

Bei einer ernsthaft kooperativen Motivation ist auch möglichst von der Regelung etwaiger Löschungspflichten der Parteien abzusehen. Dies gilt insbesondere für solche Regelungen, die zu einer Löschung nach Beendigung des zugrundeliegenden Vertragsverhältnisses verpflichten (Garbers-von Boehm, et al., 2016, S. 19).

Auch sind in der vereinbarten Data Governance gegenseitig verpflichtende Regelungen zur Geheimhaltung und IT-Sicherheit vorzusehen. Ergänzend sollten Risiken der Verletzung von Pflichten der Data Governance im vertraglichen Sanktionssystem, etwa in Form von Pönalen, berücksichtigt und im Weiteren von Dokumentations-, Benachrichtigungs- sowie Auditierungsrechten flankiert werden.

Es handelt sich hier um relativ wirkende Regelungen über den Umgang mit Daten in Form einer gemeinsamen Data Governance, kombiniert mit informationstechnischen Vorkehrungen zur IT- beziehungsweise Datensicherheit. Zu deren Vornahme verpflichten sich die Parteien. Daher könnte im Ergebnis sogar eine „quasi-dingliche Wirkung“ (Żdanowiecki, 2015, S. 25) entstehen, da insgesamt der Zugang und die Nutzung durch Unbefugte verhindert werden sollen.

Abschliessend ist anzumerken, dass bei der Vereinbarung einer kooperativ geprägten Data Governance gegebenenfalls auch kartellrechtliche Aspekte zu berücksichtigen sind, wobei Ensthaler davon ausgeht, dass hierin regelmässig keine Wettbewerbsbeschränkung i.S.v. Art. 101 Abs. 1 AEUV zu sehen ist (Ensthaler, 2016, S. 3478). Allerdings sei auf ein diesbezügliches Prüferfordernis im Einzelfall hingewiesen, da gemeinsame Datenbestände durchaus sowohl Marktzutrittsschranken als auch Koordinationspotenziale bieten können.

Autoren: Manuel Treiterer, Christopher Köhler

Digitale (Weiter-)bildung als Basis digitaler Kompetenzen

Digitalisierung erfordert eine solide digitale Grundbildung, um eine digitale Spaltung der Gesellschaft zu verhindern. Bildungsangebote, welche ein lebenslanges Lernen ermöglichen, sind existenziell für die Entwicklung des nötigen Knowhows bezüglich diverser relevanter Themen im Bereich der *Digitalisierung*. Auch die politischen Akteure scheinen dies mittlerweile verinnerlicht zu haben – auch wenn die Geschwindigkeit des Ausbaus dieser dringend notwendigen Angebote durchaus ausbaufähig ist.

Die Grundschule kann bereits die Grundlagen digitaler Kompetenzen schaffen, in dem sie z. B. die Neugier am Programmieren weckt. Bereits dort lernen Schüler die Grundzüge der englischen Sprache. Wieso werden ihnen dann nicht auch die Grundzüge der Programmiersprache(n) nahegebracht? Wie soll ein Mitarbeitender beispielsweise den technologischen Wandel gestalten oder die zielgerichtete Nutzung von Daten sinnvoll umsetzen, wenn er über keine digitalen Kompetenzen verfügt und nicht ansatzweise das Grundverständnis für z. B. Technologie oder Informatik mitbringt?

Digitale Kompetenzen, namentlich digitale Basiskompetenzen wie Datenverarbeitung, Problemlösung, Erstellen von (digitalen) Inhalten, (Daten) Sicherheit sowie Kommunikation und Zusammenarbeit (Vuorikari, Punie, Carretero Gomez & Ven den Brande, 2016), sind in den weiterführenden Schulen weiter auszubauen. Denn nach dem Schulabschluss sind diese digitalen Kompetenzen innerhalb einer Ausbildung, eines Studiums und bei einem direkten Berufseinstieg gefragt.

Sowohl die Politik als auch die Wirtschaft haben ein Interesse daran, dass die digitale Bildung langfristig und auf gutem Niveau garantiert wird. Hierfür sind auf politischer Ebene entsprechende Rahmenbedingungen zu schaffen und Unternehmen müssen Mitarbeitenden stetige, zukunfts- und bedarfsorientierte Kompetenzaneignungs- und -weiterentwicklungsmöglichkeiten anbieten. Wirtschaftlich gesehen führt dies u. a. zur Steigerung der Standortqualität, der Leistungs- und Innovationsfähigkeit in Unternehmen. Die konstante Aneignung und Weiterentwicklung von Kompetenzen trägt auch zur Aufrechterhaltung der langfristigen Beschäftigungsfähigkeit bei und aus Sicht des Einzelnen ermöglicht sie vielfältige Entwicklungs- und Karrierechancen.

Dies bedingt aber, dass Bildungskonzepte überprüft und so ausgerichtet werden, dass es damit möglich ist, die beteiligten Personengruppen eines Unternehmens an die Anforderungen der Zukunft des digitalen Lernens stets anzupassen bzw. hinzuentwickeln. Es müssen kontinuierlich Analysen von Bildungsbedarfen durchgeführt werden, um massgeschneiderte digitale Bildungsangebote für Berufstätige in einer digital transformierten Gesellschaft zu ermöglichen. Auch die Übersichtlichkeit und Qualität von Weiterbildungsangeboten muss kontinuierlich verbessert und vorausschauend an die sich stetig wechselnden Anforderungen angepasst werden.

Der Erwerb dieser Kompetenzen sollte über verschiedene Weiterbildungen erfolgen können, denn die digital ausgerichtete Weiterbildung wird der Schlüssel künftigen lebenslangen Lernens sein. Hier besteht dringender Nachholbedarf, insbesondere im ersten und im zweiten Wirtschaftssektor. Die sich transferierende Arbeitswelt unterliegt einer starken Dynamik und die Halbwertszeit des Wissens nimmt in vielen Berufen und Branchen rapide ab (Weck, 2018). Deswegen ist eine kontinuierliche Weiterentwicklung gegenwärtiger Kompetenzen und die Aneignung neuer, erforderlicher (digitaler) Kompetenzen eine zwingende Notwendigkeit – wer sein Wissen nicht auf dem aktuellen Stand hält, ist sehr schnell „weg vom Fenster". Dies gilt für einzelne Person als auch für ganze Organisationen einschliesslich dem Human Resource-Bereich (HR).

Um mit den Herausforderungen der *Digitalisierung* umgehen zu können, bedarf es in vielen HR-Abteilungen selbst (d. h. bei den Fach- und Führungspersonen) der Aneignung und zunehmenden Schärfung digitaler Kompetenzen. Im Vordergrund stehen sollten die Steigerung der IT-Affinität und die Fähigkeit zur Analyse von Daten (Big Data). HR-Mitarbeitende sollten zudem sachkundig HR-IT-Systeme anwenden können, um Vorhersagen und Entscheidungen aufgrund von Auswertungen grosser Datenmengen vorbereiten bzw. treffen zu können.

Damit die *Digitalisierung* im Bildungswesen gelingen und digitales Lernen seine Vorteile ausspielen kann, müssen Politik und Wirtschaft enger zusammenarbeiten. Sie müssen digitale Medien, digitale Infrastrukturen, Cloud-Dienste, Mediendienpädagogik, Qualifizierung etc. als Einheit denken, ausrichten und gemeinsam Entwicklungsmöglichkeiten zur Forcierung der digitalen Bildung und mit dem Ziel des Aufbaus digitaler Kompetenzen anbieten.

Autoren: Abdullah Redzepi, Christopher Köhler

Fazit

In Deutschland, Österreich und der Schweiz gibt es fünf Themenbereiche, die im Bereich der Digitalisierung relevant für die kleinen und mittleren Unternehmen (KMU) und politisch aufgegriffen sind: Infrastruktur, Bildung, Ordnungs- und Rechtsrahmen, Verwaltung und Wirtschaftsinfrastruktur. Zentral relevant für die Bodensee-KMU sind die Themenbereiche Infrastruktur sowie Ordnungs- und Rechtsrahmen.

Im Bereich der direkten politischen Unterstützung wünschen sich die Bodensee-KMU insbesondere Hilfestellung bei der Vernetzung mit verschiedenen Akteuren (z. B. andere Unternehmen, Forschungseinrichtungen, Hochschulen, Wirtschaftsförderern, IHKs), um schneller und unmittelbarer von Wissensbeständen dieser Akteure lernen und mit diesen kooperieren zu können. Der Netzwerkgedanke ist hier zentral. Die Politik kann im besten Sinne ein unternehmensexterner „Enabler" der *Digitalisierung* innerhalb der KMU sein. Erst an zweiter und dritter Stelle stehen die Wünsche nach allgemeinverbindlichen Rahmenbedingungen und finanzieller Förderung.

Zentrale (indirekte) Aufgabe der Politik ist aber die Schaffung geeigneter Rahmenbedingungen durch Infrastrukturen, Forschungsförderung und Vernetzungsplattformen. Diejenigen politischen Rahmenbedingungen, die in einer globalisierten Welt *Digitalisierung* beeinflussen, werden nur zum kleinen Teil von den politischen Akteuren der Region beeinflusst. Umso wichtiger erscheint es, dass diese ihre Stimmen in den nationalen und europäischen Gremien im Sinne einheitlicher und offener Wettbewerbsbedingungen erheben.
Der vorhandene Rechtsrahmen der *Digitalisierung* ist weitestgehend ausreichend, um vorhandene regulatorische und vertragsrechtliche Fragen zu behandeln. Die EU-Aussengrenze zur Schweiz ist nur bedingt problematisch, da sich die Rechtssysteme bereits grundsätzlich ähneln und sich die zur Anwendung kommenden Rechtsregeln (z. B. im Datenschutz oder dem Vertragsrecht) durch die EU-Harmonisierung und bilaterale Vereinbarungen mit der Schweiz angenähert haben. Juristen können sich daher ohne grössere Brüche zwischen den Rechtssystemen gut verständigen bzw. die Regeln sind sogar so gut verständlich und zugänglich, dass KMU mit überschaubarem Aufwand den Rechtsrahmen zuverlässig abklären können. Übergreifende Rechtsthemen sind:

- Daten, insbesondere deren Zuordnung und Fungibilität über Unternehmens- und Rechtssystemgrenzen hinweg
- Schutz personenbezogener Daten nach europäischem und nationalem (Deutschland, Österreich, Schweiz) Recht
- IT-Sicherheit als Rechtsfrage
- Urheberrecht und Schutz von Know-how über Unternehmensgrenzen hinweg
- Vertragsrecht als Gestaltungsinstrument aber auch Arbitragemöglichkeit bei grenzüberschreitenden Kooperationen

Verbänden und politischen Akteuren in der IBH-Region sollte besonders daran gelegen sein, den KMU praxisnahe Orientierungshilfen und Präsenz- sowie digitale Plattformen anzubieten, welche die Umsetzung digitaler Strategien im bestehenden Rechtsrahmen unterstützen. Dabei muss ein erstes Ziel in der Schaffung eines Bewusstseins für rechtliche Herausforderungen be-

stehen, das über datenschutzrechtliche Fragestellungen hinaus vor allem die oben genannten Bereiche umfasst.

Personalpolitisch ist die Digitalkompetenz der Mitarbeitenden der wichtigste Schlüssel zur Geschwindigkeit und Akzeptanz bei der Digitalisierung der KMU. Erfolgreiche Strategien können ein hoher Technologisierungsgrad, gepaart mit einem klaren Humanbezug der eingesetzten Technologie (Mensch steuert Maschine) und eine klare „HR 4“ Strategie (siehe hierzu der Kapitel „ Szenarien in der Gestaltung von HRM“) sein. Das heisst, dass bei hohem Technologisierungsgrad bei den Mitarbeitenden ein hohes Mass an Selbstorganisationsfreiheit und -kompetenz vorhanden sein muss.

Künftige Forschungsfragen, deren Klärung die *Digitalisierung* in der Bodenseeregion unterstützen könnten, sind u. a.:

- Welche Antworten geben Politik, Unternehmen und Forschungseinrichtungen in andere Wissens- / Technologie-Regionen?
- Wissen als Asset im Sinne von angewandter, unternehmensnaher Forschung: Wissensausbau in der Gesamtorganisation (personalpolitisch): Erkennen mangelnder Vorbereitung von Digitalisierungsmassnahmen und gelungene Kommunikation zur *Digitalisierung* in KMU.
- Datenökonomie und Ethik: Welche Herausforderungen birgt eine zunehmende Algorithmisierung und Ökonomisierung der Daten, insbesondere über Plattformen, für die Region?

Autor: Prof. Dr. Marc Strittmatter

Literaturverzeichnis

Ala-Mutka, K. (2011). Mapping digital competence: Towards a conceptual understanding. Luxembourg: Publications Office of the European Union. Abgerufen am 1. April 2019 von: https://www.dctest.org/uploads/6/8/7/0/68701431/jrc67075_tn.pdf

Auer-Reinsdorff, A. & Conrad, I. (2016). Handbuch IT- und Datenschutzrecht. Leinen: C.H.Beck.

Baden, D. & Higgs, M. (2018). Challenging the Perceived Wisdom of Management Theories and Practice. Academy of Management Learning & Education, 14/4, pp. 539-555.

Beranek Zanon, N. & De la Cruz, C. (2013). Urheberrechtliche Beurteilung von IaaS- (und XaaS)-Cloud-Diensten für die betreibliche Nutzung gemäss Art. 19 URG. Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht, p. 663.

Bitkom. (20. Februar 2018 a). Blockchain wird zu einem Top-Thema in der Digitalwirtschaft. Abgerufen am 17. 07 2019 von: https://www.bitkom.org/Presse/Presseinformation/Blockchain-wird-zu-einem-Top-Thema-in-der-Digitalwirtschaft.html

Bitkom. (9. Oktober 2018 b). Markt für IT-Sicherheit erstmals über 4 Milliarden Euro. Abgerufen am 17. 07 2019 von: https://www.bitkom.org/Presse/Presseinformation/Markt-fuer-IT-Sicherheit-erstmals-ueber-4-Milliarden-Euro.html

Böhm, M., Leimeister, S., Riedl, C. & Krcmar, H. (2009). Cloud Computing: Outsourcing 2.0 oder ein neues Geschäftsmodell zur Bereitstellung von IT-Ressourcen? Information Management & Consulting, 24(2), p. 8.

Brink, S., Dienes, C., Icks, A. & Schröder, C. (2017). Nutzung von Cloud-Computing im Verarbeitenden Gewerbe. Bonn: IfM Bonn.

Brodbeck, F. & Woschée, R. (2012). Personalentwicklung – Themen, Trends, Best Practices. Freiburg / München. 19-29). Grundlagen und Möglichkeiten eines evidenzbasierten Personalmanagements. In K. Schuchow, & J. Gutmann, Personalentwicklung 2013 – Themen, Trends, Best Practices (pp. 19-29). Freiburg / München.

Bruch, M. (2015). Forum und Meinung: Digitaler Bauplan. Versicherungswirtschaft, 7/2015, p. 87.

Bundesamt für Sicherheit in der Informationstechnik (2013). ICS-Security-Kompendium. Abgerufen am 14. Juli 2019 von: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile.

Bundesanstalt für Finanzdienstleistungsaufsicht. (11. November 2018). Merkblatt Orientierungshilfe zu Auslagerungen an Cloud-Anbieter. Abgerufen am 31. März 2019 von: https://www.bafin.de/SharedDocs/Downloads/DE/Merkblatt/BA/dl_181108_orientierungshilfe_zu_auslagerungen_an_cloud_anbieter_ba.html

Bundesgerichtshof. (2014). Urt. v. 6.2.2014– I ZR 2/11. GRUR, p. 879.

Bundeskartellamt. (2016). Arbeitspapier Marktmacht von Plattformen und Netzwerken. Bonn: Bundeskartellamt.

Bundesministerium für Bildung und Forschung. (2015). Zukunftsbild „Industrie 4.0". Abgerufen am 14. 07 2019 von: https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/zukunftsbild-industrie-4-0.pdf?__blob=publicationFile&v=4

Bundesministerium für Wirtschaft und Energie. (2017). Weissbuch Digitale Plattformen. Berlin: BMWi.

Busch, C. (2018). Fairness und Transparenz in der Plattformökonomie. Zeitschrift für Internationales Wirtschaftsrecht, p. 147.

Chirco, C. G. (2016, Januar). Industrie 4.0 in der Praxis, Die Auswirkungen der Vernetzung von Wertschöpfungsketten auf die anwaltliche Beratung. Zeitschrift zum Innovations- und Technikrecht, p. 11.

Cording, S. G. (2018). Der CLOUD Act aus europäischer Sicht. Computer und Recht, p. 636.

Daugherty, P., Wilson, J. & Chowdhury, R. (21. November 2018). Using Artificial Intelligence to Promote Diversity. MIT Sloan Management Review. Abgerufen am 1. April 2019 von: https://sloanreview.mit.edu/article/using-artificial-intelligence-to-promote-diversity/

Davies, Anna, Filder, D. & Gorbis, M. (2011). Future Work Skills 2020. Palo Alto: Institute for the Future for University of Phoenix Research Institute. Abgerufen am 05. April 2019 von: http://www.iftf.org/uploads/media/SR-1382A_UPRI_future_work_skills_sm.pdf

De la Cruz, C. (2013). Cloud Computing: Alter Wein in neuen Schläuchen? Jusletter IT, p. 212.

Deutsche Telekom / T-Systems. (2014). Cyber Security Report 2014 – Ergebnisse einer repräsentativen Befragung von Abgeordneten sowie Top-Führungskräften in mittleren und großen Unternehmen. Abgerufen am 14. Juli 2019 von: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjkvOW8IPbkAhWFKVAKHRmtDD0QFjAAegQIBBAC&url=https%3A%2F%2Fwww.telekom.com%2Fresource%2Fblob%2F314252%2F9d0217701b1a46319b80ee7cf8865c99%2Fdl-cyber-security-report-2014-data.pdf&usg=AOvVaw1lyq-sqElgRfjhD2A25bDs

Deutscher Bundestag. (2016). Drucksache 18 / 10207. Entwurf eines Neunten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen.

Dovas, M. (2016). Joint Controllership – Möglichkeiten oder Risiken der Datennutzung? Zeitschrift für Datenschutz, p. 512.

Ehlen, T. & Brandt, E. (2016). Die Schutzfähigkeit von Daten – Herausforderungen und Chancen für Big Data Anwender. Computer Und Recht, 32(9).

Eidgenossenschaft, K. P.–S. (7. November 2018). In diesen KMU nimmt die Industrie 4.0 Form an. Von https://www.kmu.admin.ch/kmu/de/home/aktuell/monatsthema/2018/in-diesen-kmu-nimmt-die-industrie-4-0-form-an.html

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter. (31. Oktober 2018). Erläuterungen zu Cloud Computing, o.D. Abgerufen am 17. 07 2019 von: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/cloud-computing/erlaeuterungen-zu-cloud-computing.html

Engert, A. (2018). Digitale Plattformen. Archiv für die civilistische Praxis, 218, pp. 304 – 376.

Ensthaler, J. (2016). Industrie 4.0 und die Berechtigung an Daten. Neue Juristische Wochenschrift, 48, p. 3473.

Europäische Kommission. (2017). Commission staff working document on the free flow of data and emerging issues of the European data economy. Abgerufen am 28. Mai 2018 von: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017SC0002

Europäische Kommission. (12. September 2018). Die Cybersicherheit in Europa wirksam erhöhen. Brussels. Von: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-cybersecurity_de.pdf

Eurostat. (2018). Cloud computing – statistics on the use by enterprises. Von: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises abgerufen

Frenzel, M. (2018). In B. P. Paal, & D. A. Pauly, Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO BDSG. C.H.Beck.

Garbers-von Boehm, K., Haas, P., Helwig, B., Hullen, N., Schweinoch, M., Vogel, O., ... Ziegelmayer, D. (2016). Rechtliche Aspekte von Industrie 4.0. Berlin: Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Geissbauer, R., Schrauf, S., Berttram, P. & Cheraghi, F. (2017). Digital Factories 2020 Shaping the future of manufacturing. PricewaterhouseCoopers GmbH. Abgerufen am 28. Mai 2018 von: https://www.pwc.de/de/digitale-transformation/digital-factories-2020-shaping-the-future-of-manufacturing.pdf

gfs.zürich Markt- und Sozialforschung. (2017). Cyberrisiken in Schweizer KMUs - Befragung von GeschäftsführerInnen, S. 8. Zürich: gfs.zürich Markt- und Sozialforschung. Abgerufen am 14. Juli 2019 von: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwj10Pa2k_bkAhWQLFAKHT1hDWkQFjABegQIAhAC&url=https%3A%2F%2Fwww.isb.admin.ch%2Fdam%2Fisb%2Fde%2Fdokumente%2Fthemen%2Fncs%2FSchlussbericht_CyberriskKMU_04122017.pdf.download.pdf%2FSchlussbericht_CyberriskKMU_04122017.pdf&usg=AOvVaw3F4XCpZ5NQyNcsIDhQRw1m

Giermindl, L., Christ, O. & Redzepi, A. (5. März 2019). HR Analytics. Workshop der FHS St.Gallen und HR Campus, St.Gallen.

Groß, J. (2018). AGB 4.0: Allgemeine Geschäftsbedingungen im Rahmen autonomer Vertragsschlüsse. Zeitschrift zum Innovations- und Technikrecht, 1(18), p. 4.

Grüneberg, C. (2019). § 311 Rn. 26. In G. Brüdermüller, J. Ellenberger, I. Götz, C. Grüneberg, S. Herrler, H. Sprau, . . . H. Wicke, Bürgerliches Gesetzbuch: BGB (78. ed.). C.H.Beck.

Grünwald, A. & Nüßing, C. (2015). Machine To Machine (M2M)-Kommunikation: Regulatorische Fragen bei der Kommunikation im Internet der Dinge. Multimedia und Recht, p. 378.

Hahn, C. (2016). Digitalisierung der IT-Indrustrie mit Cloud Plattformen – Implikationen für Entwickler und Anwender. HMD Praxis der Wirtschaftsinformatik , p. 595.

Hauck, R. & Blaut, H. (2018). Die (quasi-)vertragliche Haftung von Plattformbetreibern. Neue Juristische Wochenschrift, p. 1425.

Heuer-James, J. U., Chibanguza, K. J. & Stücker, B. (2018). Industrie 4.0 – vertrags- und haftungsrechtliche Fragestellungen. Betriebsberater, 48, pp. 2818-2832.

Heymann, T. (2016). Rechte an Daten. Computer und Recht, pp. 650-657.

Horner, S. & Kaulartz, M. (2016). Haftung 4.0 Rechtliche Herausforderungen im Kontext der Industrie 4.0. Zeitschrift zum Innovations- und Technikrecht(01), p. 22.

Hürlimann, D. & Zech, H. (2016). Rechte an Daten. sui-generis, pp. 89-95.

IFLA. (18. August 2017). Statement on Digital Literacy. International Federation of Library Associations and Institutions. Abgerufen am 01. Mai 2018 von: https://www.ifla.org/publications/node/11586

Institut der Wirtschaftsprüfer. (11. März 2011). IDW PS 980, Grundsätze ordnungsmäßiger Prüfung von *Compliance* Management Systemen. Retrieved Juli 19, 2019, from: https://www.idw.de/idw/verlautbarungen/idw-ps-980/43124

Institute for Digital Business. (2018). Digital Switzerland. Abgerufen am 30. Mai 2019 von: https://www.digital-switzerland.ch/digital-switzerland-2018

Jochmann, W. & Belch, T. (2016). Eine ernüchternde Zwischenbilanz. Personalführung, 5, S. 58-63. Abgerufen am 1. April 2019

Klabunde, A. (2018). Art. 4 Rn. 19. In E. Ehmann, & M. Selmayr, Datenschutz-Grundverordnung: DS-GVO, DS-GVO. Leinen: C.H. Beck.

Kluge, V. & Müller, A.-K. (2017). Autonome Systeme – Überlegungen zur Forderung nach einer „Roboterhaftung". Zeitschrift zum Innovations- und Technikrecht, p. 24.

Köhler, C., Olbert-Bock, S. & Strittmatter, M. (2018). Grünbuch Digitale Agenda Bodensee – Eine Bestandsaufnahme zum Potential der Digitalisierung innerhalb KMU in der Bodenseeregion.

Kramer, P. (2018). Cloud Computing unter der DSGVO – erleichtert oder erschwert? Datenschutz-Berater 2018, p. 54.

Langer, C. (2016). Digitalisierung und M2M Kommunikation. Zeitschrift zum Innovations- und Technikrecht, 1(16), p. 28.

Lehmann, M. & Giedke, A. (2013). Cloud Computing - technische Hintergründe für die territorial gebundene rechtliche Analyse. Computer und Recht, p. 608.

Mäder, L. (13. März 2018). Nationalrat sagt Nein zu mehr IT-Sicherheit – wegen der Kosten. Neue Züricher Zeitung Online. Von: https://www.nzz.ch/schweiz/nationalrat-sagt-nein-zu-mehr-it-sicherheit-wegen-der-kosten-ld.1365453 abgerufen

Markendorf, M. (2018). Recht an Daten in der deutschen Rechtsordnung. Zeitschrift für Datenschutz, p. 409.

Müller, T., Käser, H., Gübell, R. & Klaus, R. (2009). Technische Informatik - Grundlagen der Informatik und Assembler-programmierung (2. ed.). Zürich: vdf Hochschulverlag.

Nägele, T. & Jacobs, S. (2010). Rechtsfragen des Cloud Computing. Zeitschrift für Urheber- und Medienrecht, p. 281.

Neuenschwander, E. (2014). Cloud Computing – Eine rechtliche Gewitterwolke? Von: https://www.swico.ch/media/filer_public/0b/1b/0b1b7e8b-38bc-4043-9c75-cbecbbe31a55/masterarbeit_cloud_computing_eric_p_neuenschwander.pdf abgerufen

Olbert-Bock, S. & Lévy-Tödter, M. (2017). Human Resources Leadership – Gestaltung der digitalen Transformation unter dem Fokus der Nachhaltigkeit. St.Gallen / Hamburg.

Olbert-Bock, S. & Lévy-Tödter, M. (2019). Sustainable Resources Leadership – Gestaltung der Digitalisierung unter dem Fokus der Nachhaltigkeit. In A. Ternès, Integriertes Nachhaltigkeitsmanagement. Wiesbaden: Springer Verlag.

Otto, B., Jürjens, J., Schon, J., Auer, S., Menz, N., Wenzel, S. & Cirullies, J. (2016). Whitepaper: Industrial Data Space – digitale Souveränität über Daten. München: Fraunhofer-Gesellschaft. Abgerufen am 14. Juli 2019 von: https://www.fraunhofer.de/content/dam/zv/de/Forschungsfelder/industrial-data-space/Industrial-Data-Space_whitepaper.pdf

Peitz, M., & Schweitzer, H. (2018). Ein europäischer Ordnungsrahmen für Datenmärkte? Neue Juristische Wochenschrift , p. 275.

Peschel, C. & Rockstroh, S. (2014). Big Data in der Industrie - Chancen und Risiken neuer datenbasierter Dienste. MultiMedia und Recht, p. 571.

Pieper, F.-U. (2016). Die Vernetzung autonomer Systeme im Kontext von Vertrag und Haftung. Zeitschrift zum Innovations- und Technikrecht, p. 188.

Porter, M. & Happelmann, J. (2015). How Smart, Connected Products are Transforming Competition. Harvard Business Review, 11(10/15), p. 3.

Rempe, C. (2016). Smart Products in Haftung und Regress. Zeitschrift zum Innovations- und Technikrecht(01), p. 17.

Rockstroh, S. & Kunkel, H. (2017). IT-Sicherheit in Produktionsumgebungen - Verantwortlichkeit von Herstellern für Schwachstellen in ihren Industriekomponenten. MultiMedia und Recht, p. 77.

Roßnagel, A. (2017). Rechtsfragen eines Smart Data-Austauschs. Neue Juristische Wochenschrift(01), p. 10.

Sassenberg, T. & Kiparski, T. (2017). Teil 2 Abschnitt D Rz. 7, 18. In T. Sassenberg & T. Faber, Rechtshandbuch Industrie 4.0 und Internet of Things. Leinen: C.H. Beck.

Sattler, C.-M. (2017). Rn. 7. In T. Sassenberg & F. T., Rechtshandbuch Industrie 4.0 und Internet of Things. Leinen: C.H.Beck.

Schäfer, F. (2014). Kap. 6 Rn. 47. In F. Niemann & P. J.-A., Praxishandbuch Rechtsfragen des Cloud Computing. Leinen: C.H.Beck.

Schlinkert, H.-J. (2017). Industrie 4.0 – wie das Recht Schritt hält. Zeitschrift für Rechtspolitik, p. 222

Schmidt, A., Schmidt, K.-J. & Zech, H. (2018). Rechte an Daten – zum Stand der Diskussion. Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht, p. 627.

Schneider, J. (2019). Datenschutz nach der EU-Datenschutz-Grundverordnung (2. ed.). Leinen: C.H.Beck.

Schweitzer, H. (2017). Neue Machtlagen in der digitalen Welt? Das Beispiel unentgeltlicher Leistungen. In T. Körber & J. Kühling, Regulierung – Wettbewerb – Innovation (pp. 269-306). Baden-Baden: Nomos Verlagsgesellschaft.

Schweizerische Bundesamt für Justiz. (2019). Stärkung des Datenschutzes. Abgerufen am 17. Juli 2019 von https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html

Seufert, S., Guggemos, J., Meier, C. & Helfritz, K. (2018). Digitale Kompetenzen von Personalentwicklern. SCIL Trendstudie. St.Gallen.

Stender-Vorwachs, J. & Steege, H. (2018). Wem gehören unsere Daten? Zivilrechtliche Analyse zur Notwendigkeit eines dinglichen Eigentums an Daten, der Datenzuordnung und des Datenzugangs. Neue Juristische Online-Zeitschrift, p. 1362.

Stieper, M. (2019). Urheberrecht in der Cloud. Zeitschrift für Urheber- und Medienrecht, p. 1.

Stögerer, C. (2013). Ein bewölkter Himmel für Urheber? Cloud Computing – ausgewählte zivilrechtliche und urheberrechtliche Fragen.
Von http://othes.univie.ac.at/27395/1/2013-03-07_0400508.pdf abgerufen

Strittmatter, M. (2016). § 22 Rn. p. 59 f. In A. Auer-Reinsdorff, & I. Conrad, Handbuch IT- und Datenschutzrecht. Leinen: C.H.Beck.

Sura, M. (2017). Rn. 27. In T. Sassenberg, & T. Faber, Rechtshandbuch Industrie 4.0 und Internet of Things (p. 194). Leinen: C.H.Beck.

Sydow, G. (2018). Europäische Datenschutzgrundverordnung, DSGVO (2. ed.). Baden-Baden: Nomos Verlagsgesellschaft.

Voigt, P. (2018). IT-Sicherheitsrecht - Pflichten und Haftung im Unternehmen. Köln: Dr. Otto Schmidt.

Vuorikari, R., Punie, Y., Carretero Gomez, S. & Ven den Brande, G. (2016). DigCompt 2.0: the digital competence framework for citizens. Brussels: Publications Office of the European Union.

Weck, A. (26. März 2018). Lebenslanges Lernen: Die Halbwertzeit von Wissen sinkt wahnsinnig. Abgerufen am 19. Mai 2019 von: https://t3n.de/news/lebenslanges-lernen-wissen-999367/

Wicker, M. (2014). Haftet der Cloud-Anbieter für Schäden beim Cloud-Nutzer? – Relevante Haftungsfragen in der Cloud. MultiMedia und Recht, p. 715.

Wilson, H., Daugherty, P. & Morini-Bianzino, P. (2017). The Jobs That Intelligence Will Create. MIT Sloan Management Review, 58/4, S. 13-16.

World Economic Forum. (2018). The future of jobs report. Geneva: World Economic Forum.

Żdanowiecki, K. (November 2015). Recht an den Daten. In P. Bräutigam & T. Klindt, Digitalisierte Wirtschaft/Industrie 4.0 (S. 19-29). Von:
https://bdi.eu/media/themenfelder/digitalisierung/downloads/20151117_Digitalisierte_Wirtschaft_Industrie_40_Gutachten_der_Noerr_LLP.pdf abgerufen

Glossar

Bodenseeregion
Als Datenbasis für die Bodenseeregion werden für diese Publikation die Länder Deutschland, Österreich und Schweiz mit den sechs Teilregionen Untersee & Hegau, Überlinger See und Linzgau, Obersee, Oberschwaben & Allgäu, Vorarlberg sowie Ostschweiz herangezogen. Geographisch setzt sich die Bodenseeregion aus den vier Ländern Deutschland, Österreich, Schweiz und dem Fürstentum Liechtenstein zusammen und wird somit als Vierländerregion Bodensee bezeichnet.

Compliance
Compliance ist die Gesamtheit aller Massnahmen, die das rechtmässige (Legal Compliance) und ethisch vertretbare (Moral Compliance) Verhalten der Organe und Mitarbeitenden eines Unternehmens im Hinblick auf gesetzliche und unternehmensinterne Regelungen sicherstellen sollen.

Digitale Agenda
Eine digitale Agenda ist ein Programm von überstaatlichen Organisationen (z. B. der EU), Staaten (z. B. Deutschland), Landesteilen (z. B. Baden-Württemberg), Städten und / oder Kommunen zur Informations- und Kommunikationstechnik. Innerhalb dieser Digitalen Agenden werden Rahmenbedingungen, Massnahmen und Ziele in Bezug auf verschiedene Bereiche der Digitalisierung wie z. B. Infrastruktur und Bildung festgelegt.

Digitalisierung
Digitalisierung innerhalb eines Unternehmens meint die Verwendung digitaler Technologien und Daten zur Generierung von Umsatz und zur Verbesserung der Unternehmensperformance in verschiedenen Bereichen.

Kleine und mittlere Unternehmen (KMU)
Kleine und mittlere Unternehmen besitzen weniger als 250 Mitarbeitende und der Umsatz pro Jahr liegt unter 50 Millionen Euro. Diese Definition der EU unterteilt KMU in Kleinstunternehmen, kleine- und mittlere Unternehmen. Kleinstunternehmen besitzen weniger als 10 Mitarbeitenden und der Umsatz pro Jahr liegt unter 2 Millionen Euro. Kleine Unternehmen besitzen weniger als 50 Mitarbeitenden und einen Umsatz kleiner als 10 Millionen Euro. In der Schweiz und in Liechtenstein besteht lediglich die Mitarbeiterabgrenzung und keine Abgrenzung über den Umsatz.

Maschinendaten
Maschinendaten sind Daten, die von Maschinen ohne menschliches Zutun generiert werden. Als Beispiele für Maschinendaten können Sensor-, Betriebs- und Nutzungsdaten angeführt werden.

Personalpolitik
Die Personalpolitik beschreibt die formale / intendierte und informelle / beiläufige Steuerung von Human- und Sozialkapital bzw. Menschen und Zusammenarbeit in Unternehmen. Gerade auch ihre impliziten Anteile unterscheiden die Personalpolitik von der Personalstrategie.

Personenbezogene Daten
Gemäss Art. 4 Abs.1 DSGVO sind „personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann. Diese Kennung ist Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person.

Politische Rahmenbedingungen
Politische Rahmenbedingungen sind von politischen Akteuren (z. B. Bundesregierung, Landesregierung, Bürgermeister) festgelegte Bestimmungen, Gesetze, Willensbekundungen und / oder formelle / informelle Grundlagen. Sie sollen dazu dienen, einen vorteilhaften Zustand und / oder Handlungsrahmen für eine gewisse Gruppe von Akteuren bereitzustellen. In diesem Fall bedeutet dies, vorteilhafte Rahmenbedingungen für KMU im Bereich der Digitalisierung zu schaffen u. a. über Gesetze, Fördermassnahmen oder Netzwerkveranstaltungen.

Impressum

An diesem Projekt beteiligte IBH-Hochschulen
Zeppelin Universität Friedrichshafen, FHS St.Gallen Hochschule für Angewandte Wissenschaften,
Hochschule Konstanz Technik Wirtschaft und Gestaltung (HTWG)

Herausgeberinnen und Herausgeber
Christopher Köhler, Prof. Dr. Sibylle Olbert-Bock, Prof. Dr. Marc Strittmatter
(Auflistung in alphabetischer Reihenfolge)

Redaktion
Frederic Denker, Miriam Ebinger, Laura Heintz, Thilo Jansch, Christopher Köhler, Philipp Kopka, Dr. Dennis Lichtenstein, Nicole Neubrander, Prof. Dr. Sibylle Olbert-Bock, Claire Perrot-Minot, Abdullah Redzepi, Prof. Dr. Michael Scharkow, Malcolm Schmidt, Prof. Dr. Marc Strittmatter, Manuel Treiterer

Lektorat
Kerstin Nebel / Konvena UG

Konzeption und Gestaltung
PIKOLIN Kommunikations-Design, www.pikolin.de

Fotografie
Seite 01: Ulrike Sommer, www.schattenlichtfarbe.de; Seite 02: Rainer M. Hohnhaus
Alle anderen Fotos: Hannes Thalmann, www.hannes-thalmann.ch

Druck
www.flyeralarm.com

IBH-Lab KMUdigital
c/o Zeppelin Universität
Zentrum für Politische Kommunikation
Am Seemooser Horn 20
88045 Friedrichshafen
Telefon: +49 7541 6009-1300
E-Mail: zpk@zu.de

www.kmu-digital.eu

www.bodenseehochschule.org

Europäische Union
Europäischer Fonds für regionale Entwicklung
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
interreg
Internationale Bodensee Konferenz
VIER LÄNDER REGION BODENSEE®