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 Mobilfunknetzen 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, 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).

[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.

[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 wettbewerbsrechlichen 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 Zugang 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

[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.

[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