Bundesministerium
für Wirtschaft
und Energie

Smart
Service
Welt

Rechtliche Heraus-forderungen bei Smart Services

Ein Leitfaden

Impressum

Herausgeber
Bundesministerium für Wirtschaft und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Text
Begleitforschung zum Technologieprogramm Smart Service Welt:
Institut für Innovation und Technik (iit) in der VDI/VDE
Innovation+Technik GmbH, Berlin
Jan-Hinrich Gieschen
Uwe Seidel
Sebastian Straub

Loesch*Hund*Liepold Kommunikation GmbH, 10827 Berlin

Stand
Mai 2019

Gestaltung
PRpetuum GmbH, 80801 München

Bildnachweis
Fotolia
Gorodenkoff / S. 8
Maximusdn / S. 13
peterschreiber.media / S. 3
Robert Kneschke / Titel

Diese und weitere Broschüren erhalten Sie bei:
Bundesministerium für Wirtschaft und Energie
Referat Öffentlichkeitsarbeit
E-Mail: publikationen@bundesregierung.de
www.bmwi.de

Zentraler Bestellservice:
Telefon: 030 182722721
Bestellfax: 030 18102722721

Inhalt

1. Einleitung: Rechtssicherheit als Erfolgsvoraussetzung

Der Austausch von Daten über Plattformen und die Vernetzung von physischen Geräten untereinander sind wesentliche Grundvoraussetzung für die Entwicklung von intelligenten Dienstleistungen, so genannten Smart Services. Plattformen ermöglichen die Kombinationen verschiedener digitaler Dienste oder cyberphysischer Systeme aus unterschiedlichen Anwendungsfeldern, deren Kombination bislang nicht oder nur sehr umständlich möglich war.

Anwender profitieren von der bequemen Nutzung dieser flexiblen Kombinationsmöglichkeiten, denn dank der Plattformen gibt es einen „einheitlichen" Anbieter, also eine zentrale Anlaufstelle, für die Nutzung unterschiedlicher Dienste. Zudem gibt es für Unternehmen und Start-ups zahlreiche Chancen für die Entwicklung neuer intelligenter Dienstleistungen. Smart Services bieten dabei nicht nur neue Möglichkeiten der Wertschöpfung, sie vereinfachen auch den Alltag – sei es in der Gesundheit, der Mobilität oder im eigenen Zuhause.

Die rechtssichere Gestaltung dieser Dienste ist dabei eine wesentliche Erfolgsvoraussetzung, da Plattformen regelmäßig als Verantwortliche für Rechtsverstöße Dritter herangezogen werden und damit einem nicht unerheblichen Haftungsrisiko ausgesetzt sind. Die rechtlichen Herausforderungen, insbesondere im Zusammenhang mit der Verwertung von Daten, sind vielschichtig. Zum einen stellen Daten einen eigenen wirtschaftlichen Wert dar, was die Frage aufwirft, wer die Rechte zur Nutzung von Daten und ihrer wirtschaftlichen Verwertung hat (Datenhoheit). Zum anderen hat die Frage des Schutzes von personenbezogenen Daten mit der EU-Datenschutzgrundverordnung und den damit einhergehenden Haftungsrisiken und möglichen Bußgeldern deutlich an Relevanz gewonnen. Der rechtskonforme Umgang mit Daten ist gleichzeitig aber auch wesentliche Voraussetzung für das Vertrauen der Anwender in einen Service oder ein Produkt.

In der Fachgruppe „Rechtliche Herausforderungen" der Begleitforschung zum Technologieprogramm Smart Service Welt wurden, z. T. in Zusammenarbeit mit der Fachgruppe „Sichere Plattformarchitekturen", in verschiedenen Workshops die unterschiedlichen Anwendungsfälle der Smart Service Welt-Projekte gemeinsam mit den Rechtsexperten der Begleitforschung und Projektpartner diskutiert. Dabei wurden rechtliche Herausforderungen analysiert und erste Lösungsansätze erarbeitet.

Der vorliegende Leitfaden, der unter Mitwirkung der externen Rechtsexperten der Begleitforschung, Prof. Dr. Jürgen Ensthaler[1] und Dr. Martin Haase von der Technischen Universität Berlin, Lehrstuhl für Wirtschafts-, Unternehmens- und Technikrecht, entstanden ist, stellt ein Ergebnis dieser Fachgruppenarbeit dar. Er beschreibt in kondensierter Form drei grundlegende rechtliche Themenbereiche und ihre Herausforderungen bei der Entwicklung von Smart Services und fasst die wesentlichen Erkenntnisse zusammen:

- Die Verarbeitung von personenbezogenen Daten.
- Datennutzungsrechte und Haftung von Plattformen.
- Die kommerzielle Verwendung von Open-Source-Komponenten.

Der Leitfaden bietet Entwicklern und Anbietern von Smart Services damit eine erste rechtliche Orientierung. Anhand von Beispielen einzelner geförderter Projekte aus der Smart Service Welt werden typische Anwendungsfälle aufgezeigt, in denen die hier behandelten rechtlichen Herausforderungen eine Rolle spielten. Die genannten Fälle stehen beispielhaft für die vielfältigen rechtlichen Herausforderungen aller Projekte aus der Smart Service Welt. Weitere Beispiele finden sich in der gemeinsamen Publikation „Sichere Plattformarchitekturen – rechtliche Herausforderungen und technische Lösungsansätze" der beiden Fachgruppen „Sichere Plattformarchitekturen" und „Rechtliche Herausforderungen". Darin stellen verschiedene Projekte, u. a. STEP und Kommunal 4.0, ausführlich ihre Ziele, die jeweiligen entwickelten technischen Ansätze sowie die spezifischen rechtlichen Herausforderungen und ihren Umgang damit vor.

1 Prof. Dr. Ensthaler ist u. a. Mit-Herausgeber des Fachperiodikums "InTeR - Zeitschrift für Innovations- und Technikrecht". Nähere Informationen finden sich unter: www.wir.tu-berlin.de/menue/inter_zeitschrift_zum_innovations_und_technikrecht

2. Verarbeitung von personenbezogenen Daten

Im Rahmen von Smart Services werden häufig Informationen verarbeitet, die Rückschlüsse auf einzelne Personen zulassen und damit Fragen der datenschutzrechtlichen Zulässigkeit aufwerfen. Mit der seit Mai 2018 geltenden EU-Datenschutzgrundverordnung (DSGVO) wurde ein in weiten Teilen einheitliches Datenschutzrecht geschaffen, das in allen Mitgliedsstaaten der Europäischen Union unmittelbar gilt.

2.1 Anwendungsbereich der DSGVO

Die DSGVO schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz ihrer personenbezogenen Daten (Art. 1 Abs. 2 DSGVO). Der sachliche Anwendungsbereich der DSGVO ist eröffnet, wenn personenbezogene Daten verarbeitet werden (Art. 2 Abs. 1 DSGVO). Daten sind personenbezogen, wenn sie sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Abs. 1 Nr. 1 DSGVO). Bei absoluter Unmöglichkeit, einen Zusammenhang zwischen einzelnen Daten und einer natürlichen Person herzustellen, ist die Identifizierbarkeit einer Person nicht gegeben. Die absolute Unmöglichkeit der Bestimmbarkeit einer Person wird jedoch durch moderne IT-Systeme und die daraus resultierenden technischen Verknüpfungsmöglichkeiten selten erreicht. Darum sind das Zusatzwissen und andere technische Mittel zur direkten oder indirekten Identifizierung für die Bewertung des Personenbezugs nur in dem Maße zu berücksichtigen, in dem sie nach „allgemeinem Ermessen wahrscheinlich genutzt werden“ (Erwägungsgrund 26 DSGVO). Die alleinige theoretische Möglichkeit der Identifizierbarkeit einer Person reicht also nicht, um den Anwendungsbereich der DSGVO zu eröffnen.

2.2 Grundsätze bei der Verarbeitung von personenbezogenen Daten

In Art. 5 Abs. 1 DSGVO werden die wesentlichen Grundsätze genannt, die im Umgang mit personenbezogenen Daten beachtet werden müssen. Hierzu gehören u.a. die Grundsätze der

- Datensparsamkeit,
- Transparenz,
- Integrität und
- Zweckbindung der Datenverarbeitung.

Die Einhaltung dieser Grundsätze muss nicht nur gewährleistet, sondern auch nachgewiesen werden können (Art. 5 Abs. 2 DSGVO). Dieser sogenannten Rechenschaftspflicht (oder accountability) kommt in der Praxis eine hohe Bedeutung zu. Die DSGVO folgt dabei einem risikobasierten Ansatz. Das bedeutet: Je höher das Risiko für die Verletzung von personenbezogenen Daten ist, desto umfangreicher sind die zu ergreifenden Schutzpflichten und damit auch die Nachweispflichten in Bezug auf die Rechtmäßigkeit der Verarbeitung. Zur Vermeidung von Bußgeldern sollte daher nicht nur eine datenschutzkonforme Verarbeitung von personenbezogenen Daten sichergestellt, sondern auch auf die Einhaltung von Dokumentations- und Organisationspflichten geachtet werden.

2.3 Beispiele aus dem Anwendungsfeld Produktion

In der Produktion werden durch moderne Assistenzsysteme oder vernetzte Fertigungsprozesse immer mehr Daten erhoben und verarbeitet. Mitunter kann der Einsatz von neuen Technologien einen rechtfertigungsbedürftigen Eingriff in die persönliche Lebenssphäre der Beschäftigten darstellen. Denn die Registrierung von Arbeitsvorgängen kann möglicherweise Hinweise auf die Produktivität oder Arbeitsweise eines Mitarbeiters geben. Werden beim Einsatz von adaptiven Assistenzsystemen wie z. B. Datenbrillen, Sensoren oder Kameras personenbezogene Daten von Beschäftigen verarbeitet, müssen die Vorgaben des Beschäftigtendatenschutzes beachtet werden. Die DSGVO selbst enthält keine speziellen Vorschriften für die Verarbeitung von Beschäftigtendaten. Sie sieht aber in Art. 88 DSGVO die Möglichkeit vor, in diesem Bereich spezifischere nationale Vorschriften zu treffen. In Deutschland hat der Gesetzgeber mit der Schaffung von § 26 Bundesdatenschutzgesetz (BDSG) von dieser Regelungsmöglichkeit Gebrauch gemacht.

Beispielprojekte: AcRoSS & Glass@Service

Augmented Reality (AR) kann in der Industrie an vielen Stellen dazu beitragen, Arbeitsprozesse effektiver und einfacher zu gestalten. Die wahrgenommene Realität des Anwenders wird über ein AR-fähiges Gerät, etwa eine Datenbrille oder ein Tablet, mit kontextspezifischen Informationen angereichert. So werden viele Informationen zu Arbeitsprozessen, aber auch z. B. von anderen Mitarbeitern in der Umgebung verarbeitet.

Ziel von AcRoSS war es, eine Plattform zu entwickeln, auf der Daten ausgetauscht werden, um unterschiedliche AR-Services bereitzustellen. Dadurch sollen sich AR-Anwendungen auch von kleineren Unternehmen leichter nutzen lassen und gleichzeitig Anbieter von AR-Software und -Hardware an der Entwicklung neuer Services mitwirken können.

Im Projekt Glass@Service wurde eine eigene Datenbrille entwickelt, die hohen Standards hinsichtlich Robustheit, Ergonomie, Arbeitsschutz und Datensicherheit entspricht. Die AR-Brille ermöglicht nicht nur größtmögliche Bewegungsfreiheit, sondern auch berührungslose Interaktion, also die Steuerung über Augenbewegungen und Gesten.

Rechtliche Herausforderungen und Lösungen der Projekte

Bei der Nutzung von AR-fähigen Geräten besteht die Möglichkeit, dass personenbezogene Daten erfasst werden, weshalb datenschutzrechtlichen Fragestellungen in beiden Projekten hohe Bedeutung haben

Im AcRoSS-Projekt wurden etwa Konzepte für die IT-Sicherheit der Plattform erarbeitet, damit ein Datenaustausch tatsächlich nur mit authentifizierten und autorisierten Systemen, Geräten und Nutzern stattfinden kann. Dies war vor dem Hintergrund der Anforderungen der DSGVO in Bezug auf die Sicherheit der Datenverarbeitung erforderlich.

Das Projekt Glass@Service hat sich intensiv mit der Datenschutzthematik im Zusammenhang mit der Nutzung von Datenbrillen auseinandergesetzt. In Ergänzung zu den Arbeiten des Projekts wurde im Auftrag der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) die Studie „Rechtliche Anforderungen an den Datenschutz bei adaptiven Arbeitsassistenzsystemen“ erstellt, in der die Zusammenhänge zwischen adaptiven Assistenzsystemen, wie AR-Brillen, und den rechtlichen Rahmenbedingungen erläutert werden. Eine Erkenntnis der Studie ist beispielsweise, dass die DSGVO den technischen Datenschutz stärkt. Das Gutachten ist in Form eines Berichts erschienen, der auf der Website der BAuA heruntergeladen werden kann.

Mehr zu AcRoSS
Mehr zu Glass@Service

Die Verarbeitung von personenbezogenen Daten von Beschäftigten ist gestattet, sofern sie zum Zwecke der Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses erforderlich ist. Rechtsgrundlage für eine Verarbeitung im Beschäftigtenkontext können aber auch eine Einwilligung oder eine Kollektivvereinbarung (z. B. eine Betriebsvereinbarung) sein (§ 26 Abs. 2, Abs. 4 BDSG). Werden durch neue Technologien im Arbeitsumfeld Beschäftigtendaten verarbeitet, ist eine Einwilligung aufgrund ihrer jederzeitigen Widerrufbarkeit kein adäquates Mittel, um eine konstante rechtssichere Basis zu schaffen. Aus diesem Grund ist eine Betriebsvereinbarung die zuverlässigere Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten. Dabei ist das Transparenzgebot zu beachten (Art. 88 Abs. 2 DSGVO): Beschäftigte müssen klar und nachvollziehbar erkennen können, zu welchem Zweck die sie betreffenden personenbezogenen Daten verarbeitet werden (Erwägungsgrund 58 DSGVO). Wird dabei Technik genutzt, die dazu bestimmt ist, das Verhalten oder die Leistung von Arbeitnehmern zu überwachen, sieht § 87 Nr. 6 Betriebsverfassungsgesetz ein Mitbestimmungsrecht des Betriebsrats vor.

2.4 Beispiele aus dem Anwendungsfeld Mobilität

Auch im Bereich der Mobilität entstehen durch die Auswertung von Fahrzeugdaten zahlreiche Anwendungsfelder für Smart Services. Durch hoch entwickelte Sensortechnik können Unmengen von Daten innerhalb und außerhalb des Fahrzeugs gesammelt werden. Diese Daten können je nach Bedarf über Apps für verschiedene Funktionen genutzt werden. Neben rein technischen Daten (wie Betriebs- und Sensordaten) werden in der Regel auch personenbezogene Daten erfasst (z. B. Standorte oder Informationen zur Fahrweise). Die Auswertung solcher Informationen ist nur zulässig, wenn sich die Datenverarbeitung auf einen in Art. 6 DSGVO genannten Erlaubnistatbestand stützen kann.

Der Smart Service-Anbieter hat unabhängig von der jeweiligen Rechtsgrundlage den Nutzer bereits vor der Verarbeitung seiner Daten über alle datenrelevanten Prozesse präzise, transparent und in leicht zugänglicher Form zu informieren (vgl. Art. 12 Abs. 1 DSGVO).

Ausgewählte Erlaubnistatbestände nach Art. 6 DSGVO

Einwilligung (Art. 6 Abs. 1 lit. a) DSGVO	
Die Verarbeitung ist rechtmäßig, wenn die betroffene Person ihre Einwilligung gegeben hat.	**Beispiel:** Der Nutzer willigt ein, dass seine Standortdaten an einen Drittanbieter zu Werbezwecken weitergegeben werden.
Vertrag oder vorvertragliche Maßnahme (Art. 6 Abs. 1 lit. b) DSGVO	
Die Verarbeitung von personenbezogenen Daten ist für die Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen erforderlich.	**Beispiel:** Die Auswertung von Standortdaten ist notwendig, um dem Nutzer einen vertraglich zugesicherten Dienst anzubieten, z. B. Routenführung zu einem bestimmten Ziel.
Interessensabwägung (Art. 6 Abs. 1 lit. f) DSGVO	
Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich.	**Beispiel:** Zur Verifizierung von Nutzerangaben werden Daten an einen externen Anbieter übertragen, der die Richtigkeit der Daten überprüft.

Beispielprojekte: CAR-BITS.de und StreetProbe

Autos sind heute fahrende Computer. Durch unzählige Sensoren werden permanent Daten erhoben. Damit können aber beispielsweise nicht nur Rückschlüsse auf das eigene Fahrverhalten, sondern auch das von anderen Verkehrsteilnehmern geschlossen werden.

Im Projekt CAR-BITS.de ist eine Cloud-Plattform für Fahrzeugdaten entwickelt worden, mit der Fahrzeugdaten sicher, datenschutzkonform und zweckgebunden für neue Dienste genutzt werden können, zum Beispiel um günstigere, individuelle Versicherungspolicen anbieten zu können.

Im StreetProbe-Projekt wird ein cloudbasiertes System zur Erfassung und Bewertung von Straßenzuständen entwickelt. Über bereits in Fahrzeugen vorhandene Sensoren soll die Beschaffenheit von Straßen erfasst und bewertet werden, um die Erkennung von Straßenschäden zu verbessern.

Rechtliche Herausforderungen und Lösungen der Projekte

Obwohl es sich in der Regel um Daten technischer Natur, wie z. B. Sensordaten, handelt, die bei der Nutzung der entwickelten Plattformen verwendet werden, besteht die Möglichkeit, dass auch Daten erfasst werden, die Rückschlüsse auf Personen zulassen und somit datenschutzrechtlich relevant sind. Die Projekte mussten daher zunächst prüfen, inwiefern personenbezogene Daten erfasst bzw. verarbeitet werden, und dafür rechtssichere Lösungen entwickeln.

So wurde beispielsweise im Projekt CAR-BITS.de die Zweckbindung der Daten durch ein individualisiertes Schlüsselmanagement technisch ermöglicht. Damit können erfasste Daten von Diensteanbietern nur für zuvor vereinbarte Zwecke genutzt werden. Fahrer, die Services der CAR-BITS.de-Plattform nutzen wollen, müssen zunächst explizit der Verwendung bestimmter eigener Fahrzeugdaten zustimmen.

Im Projekt StreetProbe werden alle relevanten Sensordaten eines Fahrzeugs zentral erfasst und anschließend mobil an eine zentrale Datenbank (Cloud) übermittelt. Am sogenannten „Entry-Point“ der Cloud, wo die gesendeten Fahrzeugdaten als erstes eintreffen, erfolgt eine automatische Datenbereinigung. Die ersten und letzten Minuten der Fahrt werden beispielsweise aus Datenschutzgründen aus den Datensätzen eliminiert.

Mehr zu CarBits.de
Mehr zu StreetProbe

2.5 Beispiele aus dem Anwendungsfeld Medizin

Auch im Bereich des Gesundheitswesens besteht ein hohes Innovationspotenzial für die Entwicklung von smarten Dienstleistungen, zum Beispiel zur Verbesserung der Patientenversorgung und der Kommunikation zwischen Ärzten und Patienten oder anderen Fachärzten. In der Regel werden dafür Gesundheitsdaten verarbeitet, also solche Daten, die sich auf die körperliche oder geistige Gesundheit einer Person beziehen und aus denen Informationen zum Gesundheitszustand hervorgehen (Art. 4 Nr. 15 DSGVO). Bei Gesundheitsdaten handelt es sich um sogenannte besondere Kategorien von personenbezogenen Daten. Die Verarbeitung von besonderen Kategorien personenbezogener Daten ist untersagt (Art. 9 Abs. 1 DSGVO). Die Verarbeitung kann aber durch die Einwilligung des Betroffenen oder einen gesetzlich normierten Ausnahmetatbestand legitimiert werden (Art. 9 Abs. 2 lit. a DSGVO). Soll die Verarbeitung durch Einwilligung des Patienten erfolgen, muss die Zustimmung ausdrücklich und freiwillig erfolgen. Darüber hinaus ist der Patient in präziser, transparenter, verständlicher und leicht zugänglicher Form über die beabsichtigte Datenverarbeitung zu informieren. Im ärztlichen Behandlungskontext ist zudem zu berücksichtigen, dass der Weitergabe von Patientendaten neben

dem Datenschutzrecht auch die ärztliche Schweigepflicht entgegenstehen kann. Sollen Patientendaten zur Weiterbearbeitung etwa an einen Dritten übermittelt werden, sollte der Patient gebeten werden, den behandelnden Arzt von seiner Schweigepflicht zu entbinden.

Beispielprojekt: MACSS

Im MACSS-Projekt wurde eine Plattform entwickelt, die den Datenaustausch und die Vernetzung zwischen Patienten und Ärzten verbessern soll. Für Patienten dient die entwickelte MACSS-App als Verbindung zu Medizinern und persönlicher Assistent. Fachärzte, Hausärzte, Kliniken, Versorgungszentren und weitere Partner können über die Plattform die Patientendaten der App, wie etwa Therapieverlauf, Vitaldaten und Patientenakten, einsehen und somit den Therapieverlauf verfolgen und mögliche Fehlentwicklungen frühzeitig erkennen.

Rechtliche Herausforderungen und Lösung des Projekts

Wesentliche Herausforderungen des Projekts lagen neben der Datenauswertung in der Gewährleistung von Sicherheit und Datenschutz insbesondere bei der Speicherung hochsensibler medizinischer und damit personenbezogener Daten. Die Verarbeitung personenbezogener Daten auf der Plattform erfolgt ausschließlich in einem geschützten Bereich innerhalb des Klinikinformationssystems. Für die Nutzung individueller Patientendaten ist ein ausgefeiltes Datenschutz- und Sicherheitskonzept erarbeitet worden, das auf Basis pseudonymisierter, verschlüsselter Daten nach Einwilligung des Patienten nur berechtigten Ärzten den Zugriff und die personenbezogene Zuordnung ermöglicht.

Um den umfangreichen datenschutzrechtlichen Anforderungen in Bezug auf medizinische Anwendungen zu begegnen, wurde im Rahmen von MACSS außerdem ein internes Datenschutzgutachten erstellt, was sich mit spezifischen Fragen des Datenschutzes im Projekt, wie etwa der Konformität mit Landesdatenschutzgesetzen und der Integration von Services Dritter, beschäftigt.

Mehr zu MACSS

3. Datennutzungsrechte und Haftung von Plattformen

In der Regel agieren Plattformen als „Mittler“ zwischen verschiedenen Diensten und Anbietern, indem sie Daten zusammenführen und eine einheitliche Datengrundlage für die Weiterverarbeitung zu verschiedenen Services zur Verfügung stellen. Im Produktionsbereich kann die Auswertung von großen Datenmengen aus unterschiedlichen Quellen zum Beispiel zu einer verbesserten Steuerung oder Planung von Herstellungsprozessen führen. Gleichzeitig können Wartungsdienste mit maschinengenerierten Produktionsdaten optimiert und entsprechend des individuellen Wartungsbedarfs der Maschine angepasst werden. Im Idealfall kann eine Wartung dann so geplant werden, dass der Produktionsprozess nur geringfügig oder gar nicht unterbrochen wird.

Beispielprojekt: STEP

Das Projekt STEP (Smarte Techniker-Einsatzplanung) hat eine Lösung entwickelt, um auf Basis des prognostizierten Instandhaltungsbedarfs von Maschinen den Einsatz von Technikern bedarfsgerecht, effizient und automatisiert zu planen. Dafür werden alle relevanten, z. T. anbieterübergreifenden Daten von Maschinen, wie prädiktive Fehlermeldungen, gesammelt. Sie werden mit Informationen zum Einsatzort und Informationen zu Service-Technikern, wie Qualifikationen und mögliche Fachgebiete, und digitalen Diensten wie Chat-Anwendungen kombiniert. Über eine Cloud-Plattform lassen sich diese Informationen zentral und datenschutzkonform bereitstellen und darauf basierend Technikeraufträge intelligent steuern.

Rechtliche Herausforderungen und Lösungen des Projekts

Bei STEP waren die rechtlichen Aspekte wie Beschäftigtendatenschutz und der Umgang mit dem Verbot der automatisierten Einzelfallentscheidung nach der DSGVO wichtig. Dies ist sowohl beim Design der Plattformarchitektur als auch für die Interaktionsstrategie zwischen dem Techniker und dem Einsatzplaner ausschlaggebend. Weiterhin spielte, aufgrund der Nutzung von Daten als Wirtschaftsgut, auch das Thema Datenhoheit eine wichtige Rolle.

Zur Wahrung der Privatsphäre der Servicetechniker werden in STEP Pseudonymisierungs- und Anonymisierungsverfahren verwendet. Außerdem werden die Standortdaten der Servicetechniker nach dem Prinzip der Datensparsamkeit nur partiell erfasst. Die finale Entscheidung über die Einsatzplanung der Servicetechniker übernimmt eine natürliche Person – der Einsatzplaner. Damit wird auch die automatisierte Einzelfallentscheidung nach der DSGVO verhindert.

Das Projekt ist durch den Konsortialpartner KIT ZAR (Zentrum für angewandte Rechtswissenschaft) juristisch begleitet worden. Das Projekt hat Beiträge zu den Themen in einer Fachzeitschrift veröffentlicht. Diese setzen sich mit den im Projekt behandelten rechtlichen Fragestellungen auseinander, wie z. B. mit automatisierten Arbeitgeberentscheidungen.

Mehr zu STEP

Die Datenauswertung zur Optimierung von kommunalen Infrastrukturen stellt einen weiteren wichtigen Anwendungsfall dar, der zeigt, wie Prozesse besser steuerbar und effizienter gestaltet werden können. Hierzu ist die Schaffung einer bereichsübergreifenden Datengrundlage notwendig. Dadurch lässt sich z. B. die Verkehrssteuerung einer Kommune mit Wetterdaten koppeln, um den Verkehrsfluss in Hinblick auf Wetterereignisse zu regeln. Die relevanten Daten, die für den Erhalt und den Betrieb kommunaler Infrastrukturen wichtig sind und die bereits an vielen Stellen innerhalb einer Kommune vorliegen, können über eine Plattform zusammengeführt werden.

Beispielprojekt: KOMMUNAL 4.0

Im Projekt Kommunal 4.0 wurde eine Plattform aufgesetzt, auf der vorhandene Daten aus Städten und Gemeinden übergreifend erfasst, mit anderen Informationen intelligent verknüpft und durch smarte Services ausgewertet und verwendet werden können. So können sie für eine effiziente und vorausschauende Betriebsführung von Kanalnetzen, Regenbecken und Kläranlagen genutzt werden.

Rechtliche Herausforderungen und Lösungen des Projekts

Bei der Entwicklung der IoT-Plattform für die städtische Wasserversorgung stand die Berücksichtigung besonderer IT-Sicherheitsanforderungen an kritische Infrastrukturen nach dem IT-Sicherheitsgesetz im Vordergrund. Einen wichtigen Aspekt stellt dabei auch der Umgang mit den erhobenen Daten und die Beschäftigung mit den aufgeworfenen juristischen Fragestellungen durch die Verwendung von Daten der öffentlichen Verwaltung dar: Denn hierbei muss auch die verwaltungsrechtliche Datenhoheit berücksichtigt werden. In Zusammenhang mit der Nutzung war darüber hinaus die Haftungsregelung zwischen dem Plattformbetreiber und dem Betreiber der kritischen Infrastruktur bei der Verwendung von Daten aus verschiedenen kommunalen Quellen wichtig.

Um den verschiedenen rechtlichen Anforderungen, wie etwa dem Datenschutz oder der Datenhoheit, zu begegnen, wurde bereits in der Anforderungsphase das Konzept der Kommunal 4.0-Plattformarchitektur nach dem „Security-by-Design"-Prinzip entworfen und dadurch die Informationssicherheit der einzelnen Plattformbereiche von Anfang an fest integriert. Als Grundlage dienten die IT-Sicherheitsstandards ISO 27001 und der branchenspezifische Sicherheitsstandard Wasser/Abwasser (B3S) des BSI. Die Haftungsaspekte wurden durch eine speziell dafür ausgelegte Vertragsgestaltung und Monitoringmaßnahmen umgesetzt.

Mehr zu KOMMUNAL 4.0

3.1 Nutzungsrechte und Datenhoheit

Bei den zur Auswertung herangezogenen Daten von Smart Services handelt es sich besonders im Produktionsbereich regelmäßig um Daten ohne Personenbezug (z. B. Daten über Maschinenstörungen, Produktionsmengen oder Produktqualität). Auch wenn diese Daten keinen Personenbezug aufweisen und damit nicht dem Datenschutzrecht unterliegen, sind sie dennoch für viele Unternehmen, aber zum Beispiel auch für Behörden, sehr sensibel. Eine Auswertung kann mitunter sehr detaillierte Rückschlüsse erlauben, etwa zu einzelnen Produktionsprozessen und damit der Leistungsfähigkeit eines Unternehmens. In diesem Zusammenhang ergeben sich somit Fragen hinsichtlich der Datenhoheit, also der Frage, wer welche Nutzungsberechtigungen an den Daten hat.

Zunächst ist festzustellen, dass es weder in Deutschland noch in der Europäischen Union eine gesetzliche Regelung gibt, die dem Datenproduzenten (z. B. dem Eigentümer einer Maschine) ein ausschließliches Verwertungsrecht an seinen Daten einräumt.

Von daher erscheint es ungefährlich, mit maschinengenerierten Daten zu arbeiten. Gleichzeitig kann ein Unternehmen, das Daten durch die Nutzung von technischen Geräten generiert, auch Verträge über die Nutzung der Daten mit Dritten schließen. Dies kann der Maschinenhersteller, der Verkäufer oder aber auch ein Wartungsunternehmen sein. Ob sich aus solchen Vereinbarungen Ansprüche der jeweils nutzungsberechtigten Akteure gegeneinander ergeben, ist juristisch ungeklärt.

Es kann davon ausgegangen werden, dass bei einer Nutzungseinräumung nur ein einfaches Nutzungsrecht besteht. Das bedeutet, dass Daten auch noch an Dritte übertragen werden dürfen. Ist aber im jeweiligen Vertrag ein Ausschließlichkeitsrecht vereinbart und wurde dieses auch noch entlohnt, etwa in Form einer finanziellen Gegenleistung, ist von einer Verarbeitung solcher Daten abzuraten.

Räumt beispielsweise ein Unternehmen dem Hersteller einer Maschine ein einfaches Nutzungsrecht an den Maschinendaten ein, kann das Unternehmen eine zusätzliche Datennutzungsvereinbarung mit einem Wartungsunternehmen schließen. Wird dem Hersteller hingegen ein ausschließliches Nutzungsrecht gewährt, könnte er bei einer weiteren Nutzungsrechtseinräumung versuchen, gegenüber dem Wartungsunternehmen Ansprüche geltend zu machen und etwa die Datennutzung untersagen.

In der Praxis lassen sich Hersteller von technischen Geräten und Maschinen häufig in den Verkaufsverträgen vom Verkäufer die Rechte an den Daten einräumen. Im Zusammenhang mit Serviceleistungen ist danach zu fragen, ob der Verkäufer von technischen Geräten oder Maschinen bereits Datenrechte an Dritte eingeräumt hat. Hierdurch entsteht bei Unternehmen, Behörden oder Kommunen oftmals eine Unsicherheit, ob die Datenweitergabe überhaupt zulässig ist.

Aus diesem Grund muss ein Unternehmen vor der Einräumung von Datenrechten immer sichergehen, dass die Daten tatsächlich selbst generiert wurden, und gewährleisten, dass nicht bereits Dritten, wie dem Hersteller, ausschließliche Nutzungsrechte übertragen wurden.

Durch die erforderlichen Nutzungsberechtigungen an Daten sowie die möglichen Haftungsrisiken für die Richtigkeit von Daten folgt: Ein Geschäftsmodell, das auf der Verarbeitung von Daten Dritter aufbaut, muss dadurch abgesichert werden, dass die Herkunft der Daten geklärt wurde. Dabei muss auch sichergestellt werden, dass es keinerlei Zweifel an der Berechtigung zur Verwendung der Daten durch die Datenlieferanten gibt.

3.2 Haftung der Plattform für fremde Daten

Plattformen sind durch die Verarbeitung von fremden Daten aus unterschiedlichen Quellen einem erhöhten Haftungsrisiko ausgesetzt. Zur Vermeidung solcher Risiken sollten alle, die Daten für die Plattform zuliefern, ausdrücklich darauf hingewiesen werden, dass nur solche Daten übermittelt werden dürfen, für die eine entsprechende Berechtigung besteht. Weiterhin sollten zumindest sporadisch Kontrollen durchgeführt werden, die dem Betreiber einer Plattform mehr Sicherheit geben. Haftungsrechtlich geht es darum, den Schuldvorwurf durch Hinweise und Kontrollen auszuräumen, auch wenn keine aktive Prüfpflicht in Bezug auf Rechtsverletzungen Dritter besteht.

Werden Daten auf eine Plattform geladen, die Nutzungsrechte Dritter verletzt haben, stellt sich aber immer die Frage, ob der Plattformbetreiber für diese Rechtsverletzungen haftet. Da der Betreiber der Plattform in der Regel keine Kenntnis von dem genauen Inhalt der hochgeladenen Daten hat, haftet er allenfalls als sogenannter Störer. Eine Störerhaftung liegt vor, wenn der Plattformbetreiber die Rechtsverletzung nicht selbst begeht oder einen anderen dabei

Haftung von Plattformbetreibern nach der EU-Urheberrechtsreform

Das Europäische Parlament, der Rat und die Kommission haben sich im April 2019 auf eine Reform des Urheberrechts geeinigt. Davon betroffen ist die Nutzung urheberrechtlich geschützter Werke auf Plattformen. Die Richtlinie über das Urheberrecht und verwandte Schutzrechte im digitalen Binnenmarkt sieht insbesondere strengere Regeln für die Haftung von Plattformbetreibern vor. Stellen diese große Mengen von urheberrechtlich geschützten Werken ihrer Nutzer öffentlich bereit, haften sie, sofern sie keine geeigneten Schutzmaßnahmen ergreifen oder eine entsprechende Lizenz erwerben. Die Mitgliedsstaaten der EU werden die Vorgaben aus der Richtlinie innerhalb von 24 Monaten in nationales Recht umsetzen.

unterstützt, aber dennoch in irgendeiner Weise an der Herbeiführung der rechtswidrigen Beeinträchtigung mitgewirkt hat. Das ist beispielsweise der Fall, wenn auf der Verkaufsplattform eines Anbieters wiederholt Produkte eingestellt werden, die Schutzrechte Dritter verletzen. Wird eine Störerhaftung bejaht, führt das allerdings nicht zum Schadensersatz, sondern zu einer Erklärung des Plattformbetreibers, künftig derart erfolgte Verletzungshandlungen besser zu kontrollieren. Allerdings muss die Erklärung strafbewehrt abgegeben werden. Das bedeutet, dass für jeden Verstoß, der danach begangen wird, ein Geldbetrag zu leisten ist.

3.3 Haftung von Plattformen für eigene und fremde Dienste

Für eine Plattform ergeben sich nicht nur Herausforderungen aus der Frage der Datenhoheit, also wem Daten „gehören“ und wer diese nutzen darf, sondern auch in Bezug auf die Qualität der Daten. Relevant wird dies vor allem dann, wenn aus der Nutzung von Services oder der Verwendung von Daten Schäden für den Anwender resultieren, also dass beispielsweise fehlerhafte Sensordaten zu einer falschen Steuerung einer Maschine führen oder eine Produktionsanlage durch ein falsches Wartungssignal gestoppt wird. Um wirtschaftliche Risiken zu minimieren, sind Plattformbetreiber bemüht, die Verantwortlichkeit für Qualitätszusagen ebenso wie die Verfügbarkeit der Produkte möglichst eindeutig zu klären. Dies gilt insbesondere, wenn an der Entstehung eines Services mehrere Partner beteiligt sind, sodass Daten aus verschiedenen Quellen genutzt und der Ursprung der Daten in Folge der Aggregation deswegen nicht mehr einem Leistungspartner eindeutig zugeordnet werden kann. Transparenz und umfassender Informationsaustausch sind bei dieser Arbeitsteilung unverzichtbar. Für die interne Kommunikation sollte idealerweise verdeutlicht werden, wer als eigentlicher Produzent anzusehen ist und im Außenfeld so wahrgenommen werden soll. Über die Verteilung vertraglicher Pflichten sollte geklärt werden, wem mögliche Fehler bei den Services zuzurechnen sind.

Um sich eindeutig und rechtssicher zu positionieren, muss jeder Plattformbetreiber entscheiden, welche Leistungen und welchen Leistungsumfang er wahrnehmbar anbieten will. Dieses Eigenverständnis ist den Plattformnutzern, also den Kunden, klar und unmissverständlich zu vermitteln. In der Kommunikation ist dabei die reine Vermittlungsfunktion (transaktionszentrierte Plattformen) und die erweiterte Positionierung als Produzent einer Leistung (datengetriebene Plattformen) zu unterscheiden. Bei transaktionszentrierten Plattformen „vermittelt“ die Plattform Angebot und Nachfrage und ermöglicht wie bei einem klassischen Marktplatz die Transaktionen. Bei datengetriebenen Plattformen steht hingegen die datenbasierte Vernetzung im Zentrum, was bedeutet, dass die Plattform den beteiligten Akteuren z. B. eine Aufbereitung und Auswertung von Daten bietet und damit für Kompatibilität und Interoperabilität zwischen Daten sorgt.[2]

3.3.1 Plattform als Anbieter

Sobald der Plattformbetreiber selbst Anbieter ist und nicht nur fremde Leistungen vermittelt, ist er für die fehlerfreie Ausführung verantwortlich. Wenn er dies nicht leistet, ist er je nach Vertragsart zur Gewährleistung verpflichtet, also zur Nachbesserung, und soweit ihm zumindest Fahrlässigkeit bei der Abwicklung zur Last gelegt werden kann, auch zum Schadensersatz für Folgeschäden. Folgeschäden sind

2 Eine ausführliche Beschreibung der unterschiedlichen Besonderheiten findet sich in der Studie „Eigenschaften und Erfolgsfaktoren digitaler Plattformen“. Darin finden sich auch Beispiele für transaktions- und datenzentrierte Plattformen (S. 21).

die Nachteile, die dem Kunden bzw. Vertragspartner aufgrund der sogenannten Schlechtleistung entstehen, also zum Beispiel ein Produktionsstillstand oder Lieferengpässe.

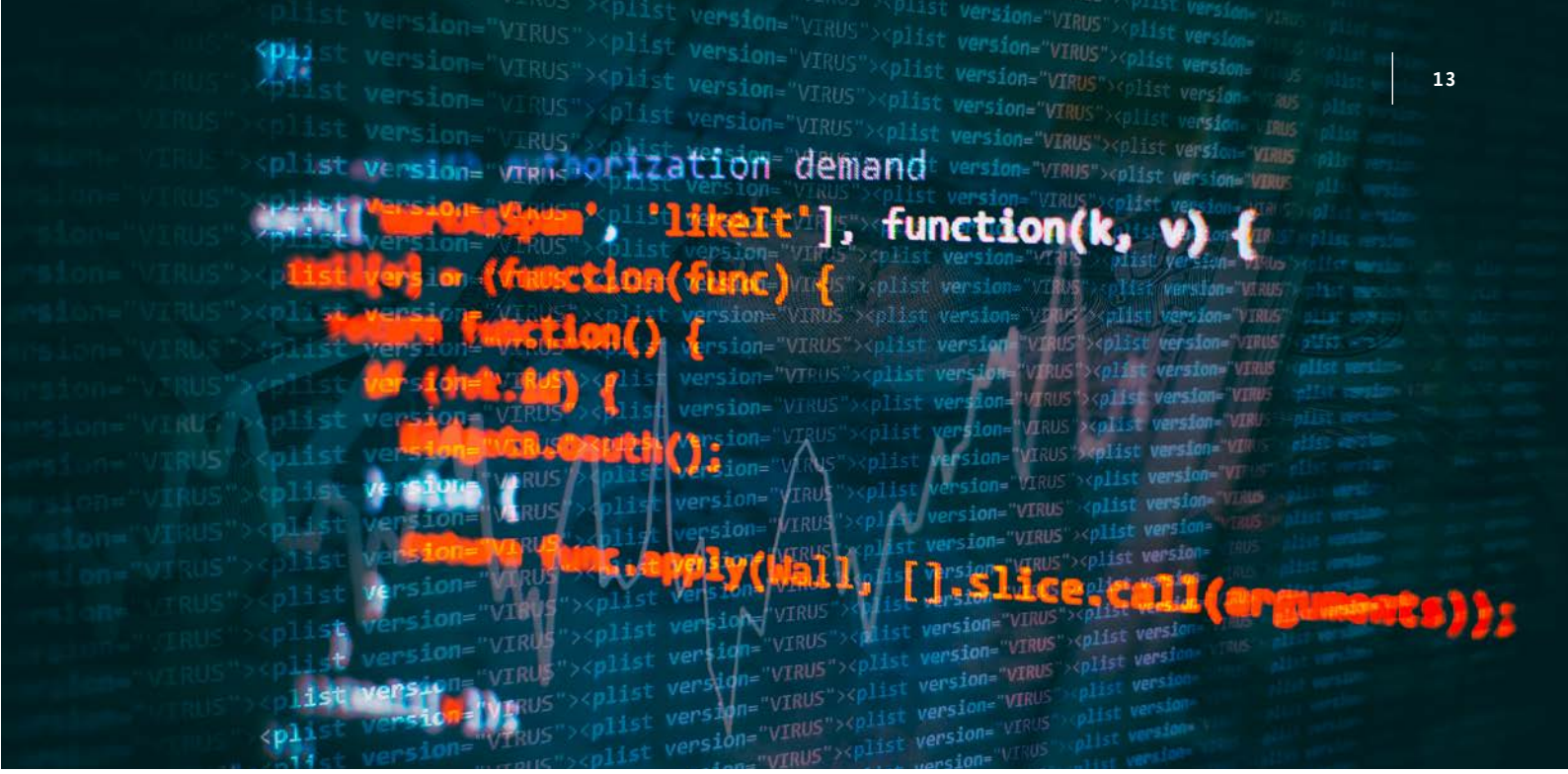
Zur Verringerung des Haftungsrisikos sollte der Plattformbetreiber in den Verträgen und auch schon in der Bewerbung des Angebots eindeutig herausstellen, unter welchen Voraussetzungen die Leistung erbracht werden kann. Soweit Risiken bestehen, dass z. B. die Verarbeitung von fehlerhaften Sensordaten zu Schäden führen kann, ist der Kunde darauf hinzuweisen. Schadensersatzansprüche für nur einfaches fahrlässiges Verhalten[3] sollten ausgeschlossen werden.

Bei solchen Haftungsausschlüssen ist darauf zu achten, dass dadurch nicht Hauptleistungspflichten wieder aufgehoben werden. Damit sind für den Vertrag wesentliche Leistungspflichten, wie z. B. die Bereitstellung eines Dienstes oder die Lieferung einer Ware, gemeint. Der Ausschluss solcher widersprüchlicher Klauseln in Verträgen wäre unwirksam.

3.3.2 Plattform als Vermittler

Als reiner Vermittler von Leistungen Dritter bewirbt ein Plattformbetreiber Produkte, bietet sie als Leistungen Dritter an, organisiert Versand und Abrechnung sowie eventuell notwendige Wartungsarbeiten. In diesem Fall schuldet der Plattformbetreiber seinen Vertragspartnern nur diese Vermittlungsleistung (also etwa die technische Bereitstellung der Plattform, Unterstützung bei der Bezahlung oder dem Versand). Eine weitergehende Verpflichtung trifft ihn nicht. Auch für Schäden, die bei Kunden infolge der vermittelten Leistung bzw. des Produkts auftreten, ist er dann nicht verantwortlich. Gewährleistungs- und Schadensersatzansprüche können sich ausschließlich an den Vertragspartner selbst richten, also denjenigen, an den die Plattform vermittelt hat.

3 Fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt (§ 276 Abs. 2 BGB).



4. Kommerzielle Verwendung von Open-Source-Komponenten

Ein wichtiger Bestandteil von Smart Services ist die zugrunde liegende Software. Bei der Entwicklung von Smart Services spielten nicht nur Eigenentwicklungen oder proprietäre Software eine Rolle, also Software, deren Möglichkeiten zur Weitergabe von der Genehmigung des Lizenzinhabers abhängen, sondern auch Open Source Software (OSS). Obwohl das Wort „Open“ suggeriert, dass eine Nutzung oder Weitergabe ohne Einschränkungen möglich ist, ist die Verwendung von OSS nicht frei von Hürden, sodass aufseiten der Projekte Klärungsbedarf hinsichtlich der Nutzung entstanden ist.

Für den Verwender von OSS ist zunächst relevant, ob die Nutzung der jeweiligen OSS an Lizenzbedingungen geknüpft ist. Oftmals sind die jeweiligen Konditionen der OSS sehr verschieden und für Anwender nicht immer sofort verständlich. Auch kann sich erst im Nachhinein herausstellen, dass bestimmte Programmteile unter einer beschränkenden Lizenz stehen. Daneben spielt die Frage der Weiterentwicklung von bestehender OSS eine wichtige Rolle. Soll eine verfügbare OSS in ein Produkt oder einen Smart Service integriert werden, muss sichergestellt werden, dass diese Nachnutzung mit den Lizenzbedingungen der ursprünglichen OSS vereinbar ist. Damit sich der Verwender von OSS nicht unnötigerweise einem Haftungsrisiko aussetzt, ist insbesondere darauf zu achten, ob die Lizenzbedingungen eine Copy-left-Klausel enthalten. Diese Klausel verlangt, dass im Falle der Bearbeitung und Weiterverbreitung der OSS-Komponenten die entstandene Software unter dieselben Bedingungen zu stellen ist wie die Ausgangssoftware. Eine Bearbeitung liegt nach herrschender Ansicht dann vor, wenn Komponenten in die eigenen oder anderen Softwareelemente eingefügt werden, also eine Vermischung stattfindet. Eine derartige Lizenzbedingung schließt demnach eine kommerzielle Verwertung nahezu aus. Daneben verpflichten nahezu alle OSS-Lizenzen dazu, den Lizenztext mitzuliefern. Das erfordert aber keinen besonderen Aufwand, weil der Text in der Regel beim Herunterladen der OSS automatisch mit heruntergeladen wird. Selbstverständlich ist, dass Copyright-Hinweise nicht gelöscht werden dürfen.

4.1 Haftung wegen Verletzung von OSS-Lizenzen

Bei der Verletzung von OSS drohen haftungsrechtliche Konsequenzen. Sanktionen sind auf der Grundlage des § 97 Abs.1 Urheberrechtsgesetz (UrhG) möglich: Diese Norm verpflichtet zum Schadensersatz, zur Unterlassung und auch zur Löschung. Die OSS-Lizenzen bestimmen, unter welchen Voraussetzungen OS-Komponenten der Allgemeinheit angeboten werden dürfen. Viele OS-Lizenzen sehen einen Wegfall der Nutzungsrechte bei einem Lizenzverstoß vor. In der Folge darf der Lizenznehmer die OSS nicht weiterverwenden und ist darüber hinaus auch nicht zur Weitergabe des Programms an Dritte berechtigt. Die Nutzung der OSS ist dann nur noch auf die Gefahr hin möglich, sich urheberrechtlichen Schadens- und Unterlassungsansprüchen auszusetzen. Neben solchen zivilrechtlichen Konsequenzen kann sich der unberechtigte OSS-Verwender unter Umständen auch strafbar machen.

4.2 Haftung bei Störungen

Daneben stellt sich die Frage, wer bei Verwendung von OSS für Störungen haftet. Beispielsweise kann die auf einer Plattform verwendete OSS fehlerhaft sein, wodurch es zu Betriebsausfällen oder Datenverlust bei Kunden der Plattform oder angeschlossenen Anbietern kommen kann. Sollte durch fehlerhafte OSS ein Schaden beim Kunden entstanden sein, haftet der Anbieter eines Services mit OSS gegenüber seinen Kunden grundsätzlich dafür genauso wie für eine fehlerhafte selbst entwickelte Software. Grundlage der Haftung ist der zwischen den Parteien geschlossene Vertrag. Ein im Vertrag möglicherweise vorgesehener Haftungsausschluss für fehlerhafte OSS scheitert regelmäßig an der Inhaltskontrolle des § 307 des Bürgerlichen Gesetzbuchs (BGB). Ein Regressanspruch gegen den Verantwortlichen der OSS, also den ursprünglichen Entwickler, kann durch die Lizenzbedingungen wirksam ausgeschlossen werden. Die Haftung des Serviceanbieters kann allerdings umgangen werden, wenn eindeutig dargestellt wird, dass nur proprietäre Software angeboten wird und der Kunde die für den Service nötige OSS selbst beziehen muss.

4.3 Vertrieb von eigener OSS an Dritte

Wird ein Plattformbetreiber selbst Anbieter von Software, die OSS-Komponenten enthält, muss geklärt werden, unter welchen Bedingungen er Dritten diese Software bereitstellen will. Bei der Weitergabe solcher Software ist darauf zu achten, dass der Bearbeiter bzw. Plattformbetreiber an seine Kunden nur Lizenzen für eigene Software oder Softwareelemente vergeben kann. Es ist deshalb darauf hinzuweisen, dass OSS-Komponenten enthalten sind.

Wichtiges im Umgang mit Open Source Software

- Bei der Verwendung von OSS sind die jeweiligen Lizenzbedingungen zu beachten.
- Die meisten OSS-Lizenzen schließen eine kommerzielle (Weiter-)Verwertung aus.
- Die Integration von bestehender OSS in Nachfolgeprodukten verpflichtet oftmals zu einer Veröffentlichung unter der Ursprungslizenz.
- Bei Verstößen gegen eine OSS-Lizenz kann der Plattformbetreiber verschuldensunabhängig auf Unterlassung, Beseitigung, Rückruf und Überlassung verpflichtet werden.

5. Ausblick: Jeder Smart Service muss individuell betrachtet werden

Bei Smart Services stehen Daten im Mittelpunkt: Maschinengenerierte Daten, Daten mit Personenbezug, Daten, die von Kunden bzw. Nutzern übermittelt werden und solche, deren Ursprung bekannt oder auch nicht bekannt ist. Ihre Nutzung, Bearbeitung und Weiterleitung erfolgen nicht im rechtsfreien Raum. Mögliche Rechtsverletzungen können zu relativ belanglosen Abmahnungen bis hin zum Zusammenbruch eines Geschäftsmodells führen. Daneben ist zur Vermeidung von haftungsrechtlichen Konsequenzen zu klären, welche Rolle eine Plattform einnimmt und welches Geschäftsmodell sie verfolgt. Die vorhergehenden Ausführungen zeigen beispielhaft die Risikobereiche auf und geben eine erste Orientierung bei der Erarbeitung von Lösungen. Die Arbeit in der Fachgruppe innerhalb des Technologieprogramms Smart Service Welt hat unterstrichen, dass die juristischen Herausforderungen immer entlang der spezifischen Risiken der individuellen Geschäftsmodelle betrachtet werden müssen. Nur so gelingt die rechtlich sichere Gestaltung neuer Smart Services.

www.bmwi.de