DIV | Deutschland intelligent vernetzt

Digital Gipfel

Sichere Smart City-Plattformen

Positionspapier der Expertengruppe Sichere IKT-Plattformen für Intelligente Netze

Digital-Gipfel
Plattform Innovative Digitalisierung der Wirtschaft
Fokusgruppe Intelligente Vernetzung

www.deutschland-intelligent-vernetzt.org

Inhalt

1. Einleitung und Motivation

Vor dem Hintergrund einer weltweit zunehmenden Urbanisierung, Digitalisierung und Vernetzung stehen deutsche Städte und Kommunen heute vor großen Herausforderungen bei der Bewältigung des gesellschaftlichen, demografischen, klimatischen und digitalen Wandels. Finanzielle, administrative, regulatorische und technologische Unsicherheiten beeinflussen nachhaltige Entwicklungen in Kommunen. Städte und Kommunen wollen in Zeiten von Veränderungen und Umbruch das direkte Umfeld ihrer Bürgerinnen und Bürger miteinander gestalten und so das Fundament für eine funktionierende Gesellschaft bilden / legen. Sie berufen sich hierbei auf die Smart City Charta und die New Urban Agenda der Vereinten Nationen, die Städte als intelligente, zukunftsorientierte aber auch komplexe Systeme beschreiben.[1]

Die Rolle der Kommune als Initiator und Akteur der Digitalisierung bei gleichzeitiger Einbindung und Akzeptanz der Bürger ist dabei unerlässlich. Ausgangspunkt der Digitalen Transformation von Kommunen ist oft eine verbesserte Effektivität kommunaler Prozesse und die Initiierung von Veränderungsprozessen auf der strukturellen Ebene der Stadtentwicklung. Sie erstreckt sich in der Folge jedoch über das gesamte Spektrum sowohl ökologischer, soziologischer als auch wirtschaftlicher Frage und Zielsetzungen aus Sicht der Kommune.

Die Digitale Transformation ist durch umfängliche und disruptive Veränderungen geprägt, bei denen moderne Technologien als Enabler eingesetzt werden.[2]

Smart City und Smart Regions sind die international verwendeten Begriffe für die Vision einer digital vernetzten Stadt oder Region. Sie bezeichnen damit Siedlungsräume, in denen die regelmäßige Nutzung im Dreiklang ökologisch, ökonomisch und sozial nachhaltiger Produkte, Dienstleistungen, Technologien, Prozesse und Infrastrukturen durch eine hochintegrierte Vernetzung mittels Informations- und Kommunikationstechnologien (IKT) systematisch ermöglicht und unterstützt wird.[3] „Smart City“ fungiert zudem oftmals als Sammelbegriff für alle digitalen Anwendungen, die Daten intelligent verknüpfen, um urbane Prozesse, Anwendungen und Geschäftsmodelle mittels IKT effizient, technologisch fortschrittlicher und nachhaltiger zu gestalten. Neueste IKT kommt so zum Einsatz, Ressourcen geschont, die Lebensqualität für alle Bewohner bessert sich und die Wettbewerbsfähigkeit der Stadt und der ansässigen Wirtschaft steigt.

Für Smart Cities existieren eine Vielzahl möglicher Anwendungsbereiche.

1 Vgl. Bundesinstitut für Bau-, Stadt- und Raumforschung (BBSR) im Bundesamt für Bauwesen und Raumordnung (BBR) / Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMUB), 2017 sowie Deutscher Städtetag, 2019

2 Vgl. Computerwoche, 2019

3 Zu weiteren Details hinsichtlich Definition und Grundlagen von Smart Cities und zugehörigen Datenplattformen vgl. Whitepaper „Smart City-Datenplattformen“ der Fokusgruppe Intelligente Vernetzung des Nationalen Digital-Gipfels (Veröffentlichung geplant für Dezember 2019, dann abrufbar unter deutschland-intelligent-vernetzt.org/downloads/)

Dabei zielen die Konzepte auf wirtschaftliche und gesellschaftliche Innovationen unter anderem in den Bereichen Verwaltung, Gebäude, Energie und Umwelt, Mobilität, Gesundheit, Bildung und Infrastruktur. In Abhängigkeit von der konkreten Anwendung interagieren Verwaltung, Unternehmen, Versorgungseinrichtungen und Bürger in unterschiedlichen Konstellationen.

Als Grundlage einer nachhaltigen Konzeption und Umsetzung von Smart Cities bieten sich offene, flexible digitale Plattformen unter Verwendung offener Standards an. Sie stellen die technischen Funktionalitäten zur Verfügung, die eine digitale Gesellschaft und Smart Cities als Infrastruktur einer Intelligenten Vernetzung brauchen, bilden die Grundlage für Innovation aus Daten und Vernetzung und sind entscheidend für die ökonomische Zukunftsfähigkeit.

Die Fokusgruppe Intelligente Vernetzung des Nationalen Digital-Gipfels hat vor diesem Hintergrund für 2019 das Jahresthema „Smart City Datenplattformen – Anforderungen, Ansätze und Herausforderungen für intelligent vernetzte Städte und Regionen“ definiert und geht der Leitfrage nach, wie Deutschland nachhaltige Plattform-Infrastrukturen sowie Informations- und Innovations-Ökosysteme schaffen kann. Dies zum Anlass nehmend, will die Expertengruppe „Sichere IKT-Plattformen für Intelligente Netze“ (EG SIKT) kommunalen Entscheidungsträgern Orientierung und Unterstützung auf dem Weg in die Plattformökonomie geben. Anhand ausgewählter Anwendungsfälle richtet die EG ihr Augenmerk dabei insbesondere auf die Aspekte Datenschutz und Sicherheit.

Bausteine der Smart City
Digitalisierung in allen Bereichen einer Stadt

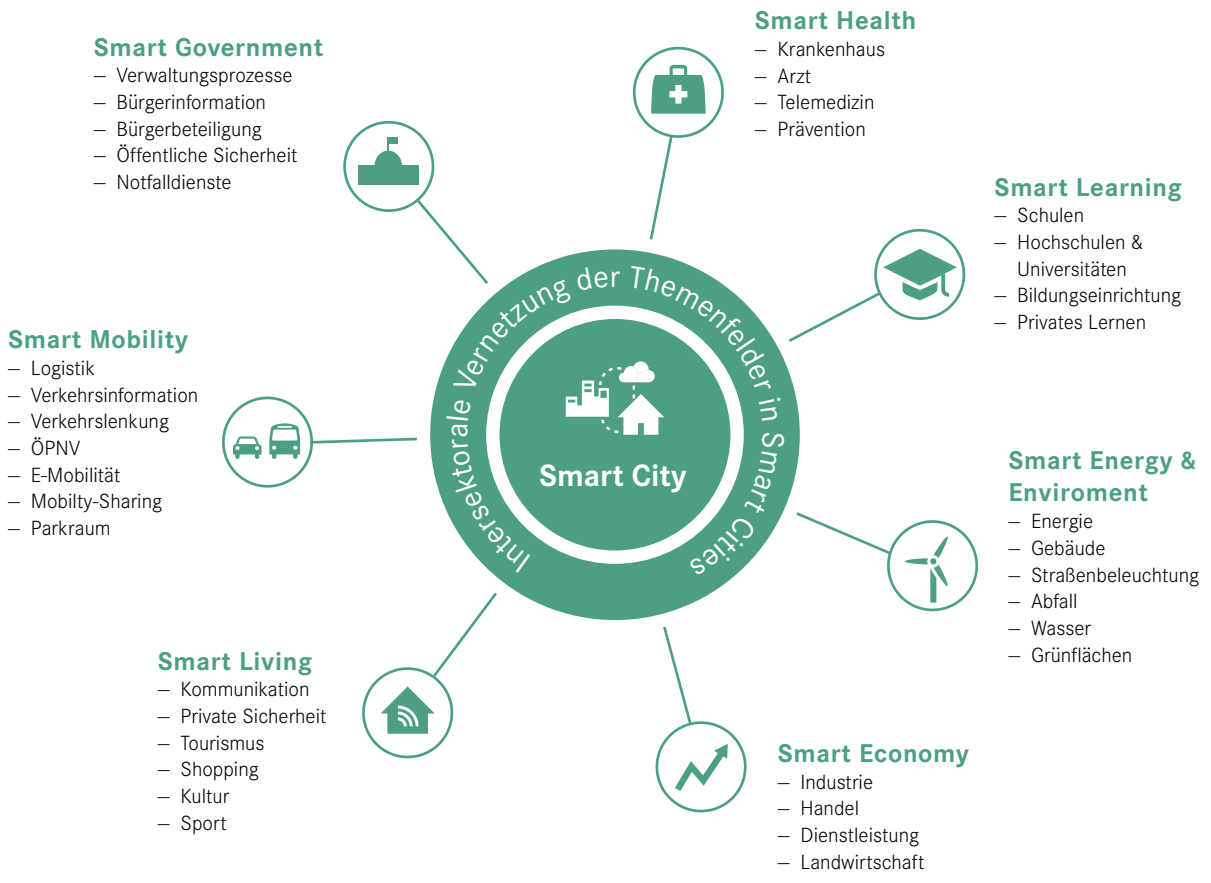

Abbildung 1: Überblick der Themenfelder und Anwendungen von Smart Cities (Quelle: Expertengruppe Smart Cities / Smart Regions der Fokusgruppe Intelligente Vernetzung des Nationalen Digital-Gipfels, 2015)

2. Smart City-Datenplattformen: Übersichtsmodell und ausgewählte Anwendungsfälle

2.1 Smart City-Datenplattform

Für Betrachtungen zu IKT-Plattformen und insbesondere zu Sicherheitsmechanismen ist ein grundsätzliches Verständnis der technischen Grundlagen von Smart-City-Plattformen hilfreich.

Mit einem Übersichtsmodell können die verschiedenen Komponenten einer digitalen Infrastruktur der Smart City verortet und ihre jeweilige Funktion erläutert werden. Insbesondere für Betrachtungen von Sicherheitsaspekten ist die Wahl einer angemessenen Komplexitätsstufe sehr wichtig, um ein möglichst gutes Verständnis zum Schutz vor potentiellen Angriffen (in Hinblick auf IT-Sicherheit) und für die Konsequenzen des Betriebs der Infrastruktur (in Hinblick auf funktionale Sicherheit) zu entwickeln. Daher sollen nachfolgend die technischen Systeme auf verschiedenen Abstraktionsstufen beschrieben werden.

Abbildung 2 zeigt die grundsätzliche Verortung von IoT-Komponenten in der Smart City. Der Schwerpunkt der Darstellung liegt auf dem Datenfluss, von der Entstehung der Daten bis hin zu ihrer Nutzung, also eine Ende-zu-Ende-Betrachtung. Bei unseren Überlegungen entstehen Daten vor allem durch den Einsatz von **Sensoren**. Beispielsweise können Sensoren Wetterbedingungen oder Luftverschmutzung erfassen, den derzeitigen Ort von Fahrzeugen öffentlicher Verkehrsmittel oder den Belegungszustand von Parkplätzen ermitteln und vieles mehr. Ziel ist in jedem Fall, dass die Sensoren ein Abbild von physischen Zuständen in der Smart City erfassen, um sie digitalen Prozessen zugänglich zu machen.

Neben den Sensoren sind in der Smart City auch **Aktoren** im Einsatz, die auf die physische Umwelt einwirken und damit eine Steuerung beispielsweise für Heizungsanlagen oder dynamische Verkehrszeichen erlauben. Zur Vereinfachung beschränken wir unsere Darstellungen weitgehend auf Sensoren und den Datenfluss vom Sensor zur Nutzung der Daten.

Die Sensoren sind über **Zugangsnetze** angebunden, in vielen Fällen drahtlos. Bei der mobilen Nutzung von Sensoren sind Funknetze eine Voraussetzung, aber auch stationäre Sensoren können in eine vorhandene Netzinfrastruktur mit geringem Aufwand eingebunden werden. Die Daten fließen von den Sensoren über das Zugangsnetz weiter zu den IKT-Plattformen. **IoT-Plattformen** kümmern sich insbesondere um die Verwaltung der verteilten Sensoren. **Datenplattformen** führen Datenströme und damit Informationen aus verschiedenen Quellen zusammen, die für eine spezielle Anwendung gebraucht werden. Es ist ein ganz wesentlicher Aspekt bei Smart City Anwendungen (wie auch generell bei der Digitalisierung), dass Daten aus unterschiedlichen Quellen zusammengeführt werden. Am Ende werden die Daten in verschiedenen **Smart City-Anwendungen**

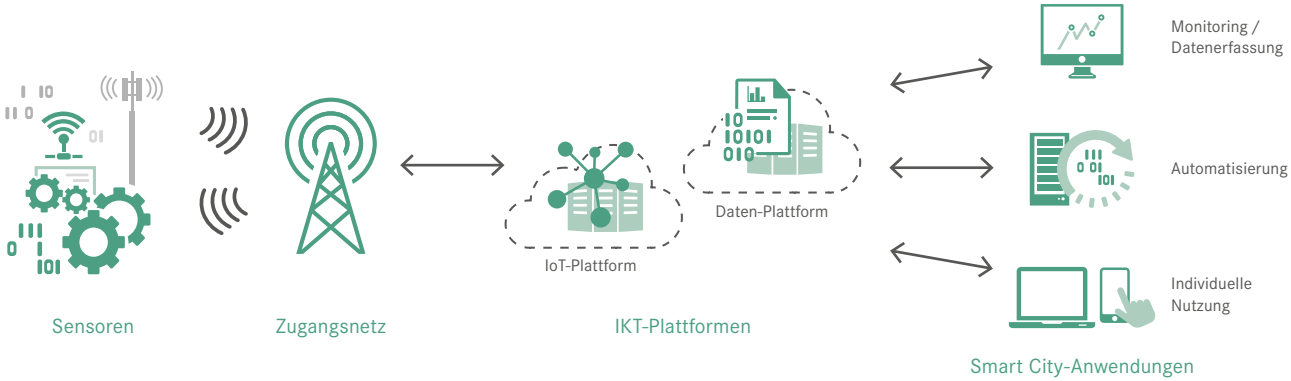

Abbildung 2: Schematische Darstellung von Smart City-Komponenten

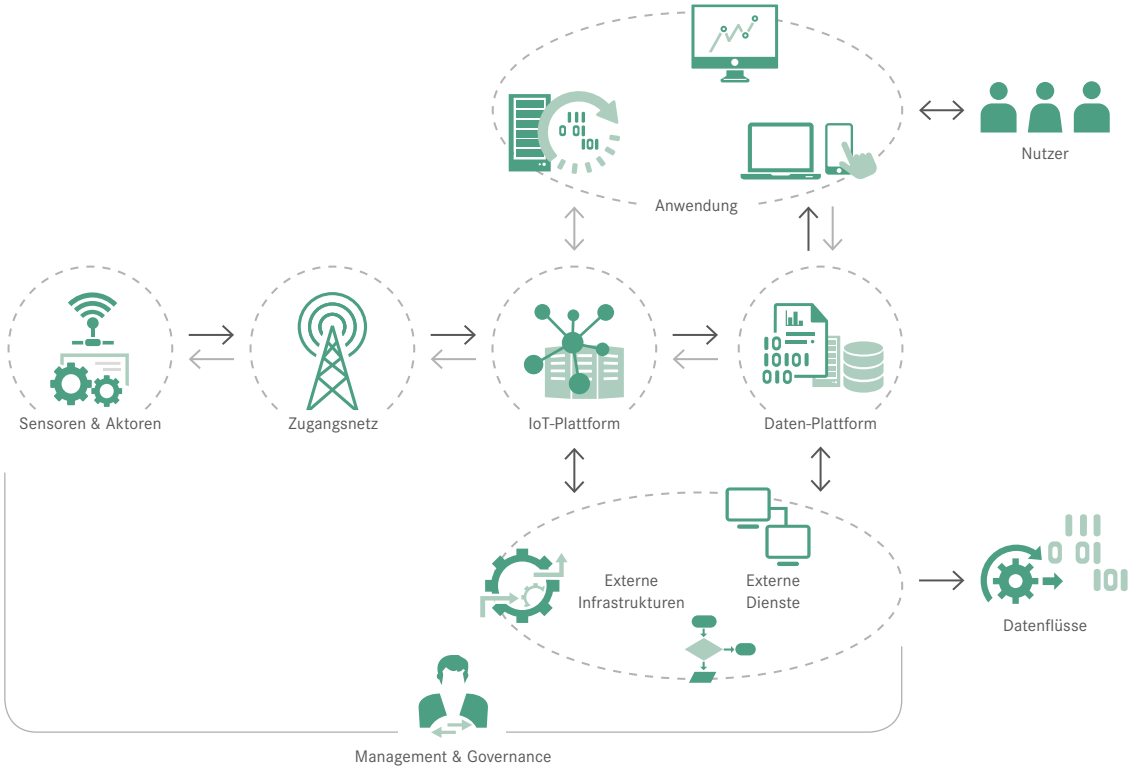

Abbildung 3: Abstraktes Übersichtsmodell

genutzt, die in der Abbildung nur exemplarisch klassifiziert dargestellt sind: Die Daten können ausgewertet und / oder gespeichert werden, um Zustände in der Smart City zu überwachen, Entscheidungen zu treffen und (automatisierte) Prozesse aufzusetzen. Eine weitere Möglichkeit ist die Nutzung der Daten in Apps. Hier soll besonders hervorgehoben werden, dass die Daten nicht nur durch die Kommune selbst, sondern auch durch Dritte genutzt werden können, sowohl in kommerziellen Produkten als auch in gemeinwohlorientierten Anwendungen. Im Sinne von Open Data ermöglichen also einzelne verfügbare Datensätze neuartige Anwendungen oder verbessern bestehende Angebote.

Abbildung 3 zeigt eine abstrakte Sicht auf das Gesamtsystem, in der sich die bereits benannten Teile wiederfinden. Auch bei dieser Darstellung des Übersichtsmodells stehen die Datenflüsse im Mittelpunkt, in der Mitte ist der Ende-zu-Ende-Datenfluss von den Sensoren in Richtung Datenplattform erkennbar. Im Modell baut die eigentliche Anwendung auf den IoT-Plattformen oder Datenplattformen auf, d. h. sie nutzt diese Plattformen als Grundlage für die Bereitstellung ihrer Funktionen. Aber auch die IoT- und Daten-Plattformen basieren auf weiteren Infrastrukturen, bspw. eigenen Cloud-Infrastrukturen oder entsprechenden Infrastrukturen von Drittanbietern. Hinzu kommt die Nutzung von externen Daten oder Diensten von Dritten.

Die Bereiche des Übersichtsmodells dienen nicht nur der Strukturierung der technischen Funktionen, sondern sind zugleich häufig Grenzen zwischen verschiedenen Betreibern oder bilden zumindest interne administrative Grenzen: Zur Anbindung von Sensoren können öffentliche Zugangsnetze genutzt werden, um Daten in die IoT-Plattform zu befördern. Alternativ kann der Betreiber einer IoT-Plattform kommerzielle Cloud-Dienste zur Realisierung seines Angebots nutzen, beispielsweise beim Gebrauch von Schnittstellen zum Datenaustausch. Diese Schnittstellen sind wichtig für Betrachtungen von Sicherheitsaspekten wichtig und stellen Punkte dar, an denen Regeln zum Betrieb des Gesamtsystems erzwungen werden können. Dies ist im Übersichtsmodell mit der übergreifenden Aufgabe von Management & Governance gekennzeichnet, die sich letztlich über alle Komponenten erstreckt, beispielsweise über eine direkte Kontrolle von Komponenten oder über vertragliche Regelungen mit Dritten.

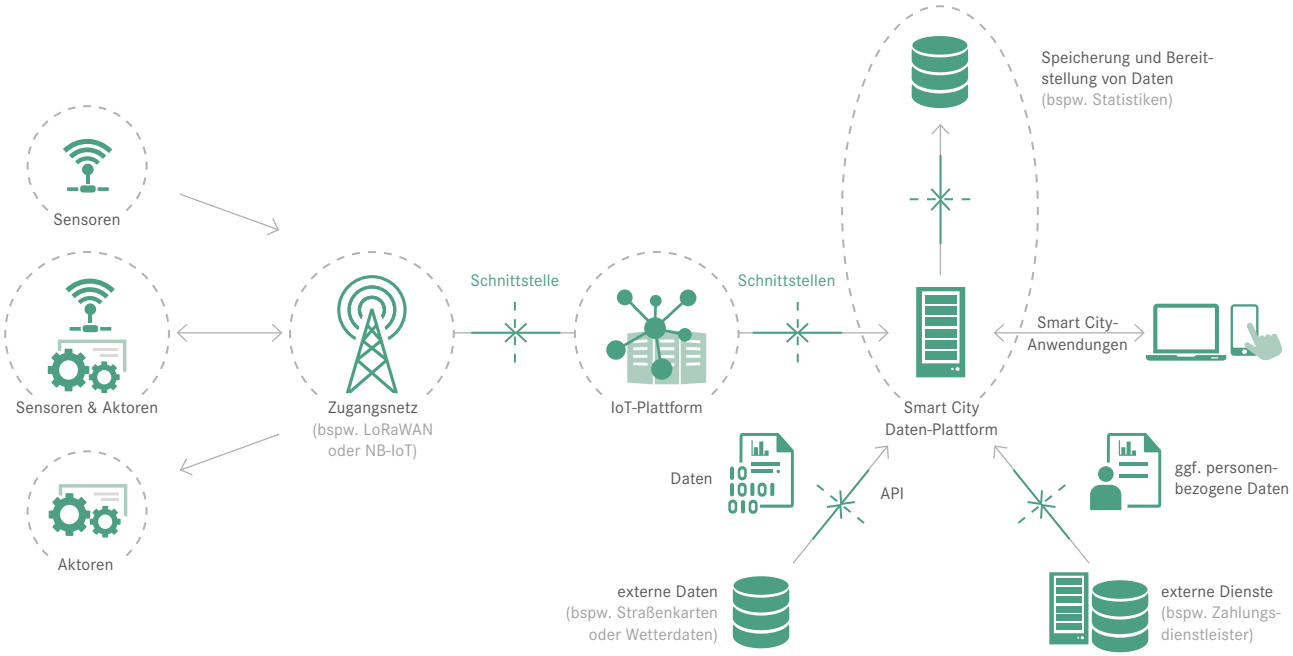

Abbildung 4: Technische Komponenten des Übersichtsmodells

Abbildung 4 zeigt das Übersichtsmodell auf einer technischen Ebene, die Netzverbindungen und Schnittstellen sowie einzelne Komponenten zur Verarbeitung oder Speicherung von Daten sichtbar macht. Es gilt zu beachten, dass in der Praxis die vorgestellten Elemente auf verschiedene Art realisiert (verwendete Technologien, Protokolle, Software) und betrieben (Betreibermodelle, gleichzeitige Nutzung verschiedener Teilsysteme, Datenquellen, externe Dienste) werden können.

Das Zugangsnetz wird auch hier als abstraktes Teilsystem dargestellt, das je nach verwendeter Technik bestimmte Eigenschaften aufweist. In den letzten Jahren ist eine neue Klasse von speziellen IoT-Funknetzen verfügbar geworden, sogenannte Low Power Wide Area Networks (LPWAN, konkrete und breit verfügbare Techniken sind bspw. NB-IoT und LoRaWAN). Diese Netze verfügen über eine hohe Reichweite oder gute Durchdringung von Gebäuden und benötigen nur wenig Energie für die meist kurzen und nur gelegentlich versendeten Sensordatensätze. Gerade im Bereich LPWAN gibt es verschiedene Betreibermodelle. Neben dem Betrieb eines eigenen Netzes und der Nutzung einer kommerziellen Infrastruktur gibt es auch einen Community-basierten Ansatz. Selbstverständlich können auch herkömmliche Netze die IoT-Daten transportieren. Allerdings erweitern LPWAN-Angebote die Möglichkeiten der Vernetzung sowohl in technischer und wirtschaftlicher Hinsicht.

Für den Transport von IoT-Daten haben sich eine Reihe spezieller Kommunikationsprotokolle etabliert, die insbesondere geringe Anforderungen an Ressourcen von Sensoren stellen und für die typischen Arten der Kommunikation im Internet der Dinge besonders geeignet sind. Neben der Weiterleitung von Daten haben IoT-Plattformen vor allem die Aufgabe, die „Dinge“ zu verwalten und entsprechend auf derem Lebenszyklus zu begleiten: Neue Sensoren müssen registriert sowie sichere Kommunikationsbeziehungen aufgebaut und der Zustand von Sensoren überwacht werden. IoT-Plattformen sollen automatisch auf Mängel und Probleme aufmerksam machen, indem sie bspw. einen niedrigen Batteriestand oder defekte Sensoren erkennen.

Die Hauptaufgabe der Smart City-Datenplattform ist die Bereitstellung der Daten für die eigentliche Smart City-Anwendung. Darüber hinaus können Daten natürlich auch für verwandte Anwendungen aus dem gleichen Anwendungsbereich genutzt werden, bspw. kann eine Anwendung freie, aktuell nutzbare Parkplätze anzeigen, und eine Auswertung der Daten über einen längeren Zeitraum kann für Zwecke der Stadtplanung genutzt werden. Besonders wirksam wird eine Smart

City-Datenplattform dadurch, dass ihre Daten mit anderen Daten kombiniert werden, beziehungsweise dass eine ihrer Anwendungen als Baustein für ganz andere Anwendungen genutzt werden können.

Einfache Anwendungen können direkt auf einer IoT-Plattform basieren, leistungsfähigere Anwendungen werden allerdings vernetzt sein und damit auf verschiedenen Datensätzen aus mehreren Datenquellen beruhen sowie auch weitere Dienste von Dritten nutzen. Das können bspw. Kartendaten aus einer freien Quelle oder auch Wetterdaten eines kommerziellen Angebots sein. Daneben können auch komplexere Dienste genutzt werden, wie die Einbindung eines Bezahldienstleisters. Die Beispiele verdeutlichen, dass in einem Fall auf nicht-personalisierte (Massen-)Daten zugegriffen wird, und im anderen Fall für die Dienstnutzung eine individuelle Authentifizierung durchgereicht werden muss, wobei während der Nutzung des Dienstes personenbezogene Daten anfallen können. Der Austausch von Daten bzw. der Zugriff auf Dienste erfolgt meist über Web-basierte Kommunikationsprotokolle und die jeweilige API (Application Programming Interface), die den technischen Zugriff auf Teilsysteme erlauben und ggf. auch administrative Grenzen darstellen. Auch die Anwendung selbst kann wieder als Ausgangspunkt für weitere Anwendungen dienen und als Datenquelle fungieren, bspw. indem sie Nutzungsstatistiken bereitstellt und damit wichtige Informationen für langfristige Gestaltungs- und Steuerungsaufgaben bereithält.

2.2 Smart City-Anwendungsfälle

Für ein besseres Verständnis wird das in Kapitel 2.1 beschriebene Übersichtsmodell im Folgenden beispielhaft an den drei Anwendungsfällen

- Parkraummanagement,
- Mobilitäts-Hub und
- Energetisches Quartiersmanagement

erprobt und praxisnah beschrieben.

2.2.1 Anwendungsfall „Parkraummanagement“

Im Folgenden wird beispielsweise der Anwendungsfall „Parkraummanagement“ beschrieben und sowohl Ziele als auch praktische Umsetzungsvarianten dargestellt.

2.2.1.1 Beschreibung Anwendungsfall

Ausgehend von einer Prozesssicht sind die folgenden Aufgabenstellungen für die Bewirtschaftung von Parkraum zu unterscheiden:

- Das **Finden** eines freien Parkplatzes
- Das **Navigieren** zum freien Parkplatz
- Das **Bezahlen** des (gebührenpflichtigen) Parkplatzes

Die Diskussionen über technische Lösungen zur Parkraumbewirtschaftung sind bereits zahlreich geführt worden genauso wie die Einführung von Telematik-Lösungen. Die Herausforderung beim Parken besteht im ganzheitlichen Ansatz der Parkplatzdetektion. Die Technologien zur Detektion freien Parkraums müssen verbunden werden, um auch kostenoptimal eine hohe Genauigkeit zu erreichen. Bei einem solchen integrierten Marktplatz für Parkplätze, Autofahrer, Parkplatzbetreiber und Kommunen können Verkehrsteilnehmer Informationen über freie Parkplätze abrufen und buchen. Parkplatzsuchende erhalten aus einer Hand Informationen über freie Parkplätze im öffentlichen Raum und auf privaten Flächen. Das Finden, Navigieren sowie die integrierte Bezahlung vermittelt das beste Parkerlebnis (siehe z. B. park and joy[4]). Auch andere Ansätze setzen auf die Integration lokaler Infrastrukturen (wie beispielsweise Buchungssäulen) und mobile Kommunikation, zum Beispiel über Smart Devices (siehe Mobiles Parken).

Aufgrund des hohen Potentials hinsichtlich Profilbildung und der Verarbeitung personenbezogener Daten gilt dabei der besondere Augenmerk den Datenschutzbestimmungen, die mit Inkrafttreten der Datenschutz-Grundverordnung (DSGVO)[5] ihren Stellenwert insbesondere aus Haftungsgründen jedoch deutlich erhöht haben.

4 www.parkandjoy.de/

5 ec.europa.eu/info/law/law-topic/data-protection/reform_de

Finden eines freien Parkplatzes
Beim Parken in Parkhäusern und auf abgeschlossenen Parkflächen (off-street Parken) werden die tatsächlich verfügbaren Parkplätze mittels Sensoren ermittelt und angezeigt. Diese Sensoren zählen den Zu- und Abgang zum Parkraum oder ermitteln freien bzw. markieren besetzten oder reservierten Parkraums mittels stellplatzgebundener Technik. Die Datenhaltung und Datenverfügbarkeit liegt dabei bei den Parkraumanbietern. Der Datenzugang für den Parkplatzsuchenden erfolgt in der Regel über Serviceplattformen oder kommunale Plattformen. Die Daten sind aktuell proprietär.

Im öffentlichen Parkraum, d. h. beim Parken im öffentlichen Verkehrsraum (on-street Parken), kann die Verfügbarkeit sehr viel schneller wechseln, eine Reservierung ist gem. StVO nicht möglich. Der Einsatz von Sensoren steckt nach heutigem Stand heute noch in der Evolution. Üblicherweise wird die Verfügbarkeit heuristisch auf Basis von Erfahrungswerten ermittelt. Mit der Evolution der Technik ergeben sich jedoch auch sensorbasierende Daten wie z. B. durch Sensoren auf der Stellfläche oder durch Kameras und Bildanalyse. Darüber hinaus werden Daten über On-Board Telematik-Systeme oder Smart Device-basierte Lösungen aus dem Bewegungsprofil von KFZ oder anderen Transportmitteln gewonnen. Die Datenhaltung und Datenverfügbarkeit liegt dabei bei den Telematik-Anbietern bzw. Serviceanbietern. Der Datenzugang für den Parkplatzsuchenden erfolgt dabei über Telematik-Systeme oder Apps der Serviceanbieter. Auch diese Daten sind aktuell proprietär.

Navigieren zum freien Parkplatz
Bereits 2009 hat der BITKOM festgehalten: „Mobile Navigation existiert in Deutschland seit Mitte der 1990er Jahre, und auf dem ITS-Weltkongress 1997 in Berlin wurden von Bosch marktreife Systeme mit detaillierten Karten (z. B. auch für Sondernutzungen wie Golfplätze etc.) angeboten. Eine große Marktdurchdringung aber wurde erst mit den nomadic devices, also kabellosen mobilen Geräten wie PDAs und Smartphones erreicht.“[6] Heute verfügt jedes Fahrzeug über eine festverbaute Navigationslösung. Apps mit einer entsprechenden Funktionalität stehen zur Verfügung.

Bezahlen des (gebührenpflichtigen) Parkplatzes
Für den letzten Prozessschritt ist die Bezahlung der Dienstleistung Parken entscheidend. Wurden und werden herkömmlich solche Parkplätze an Automaten oder an Kassen mittels Bargeldes oder Karten bezahlt, so setzen sich auch beim Parken neue digitale Zahlungsmöglichkeiten vermehrt durch.

Beim **off-street** Parken sind dies vor allem Transponder im Kraftfahrzeug, die bei der Einfahrt und der Ausfahrt Schranken öffnen und eine Abrechnung durch eine Betreibergesellschaft oder einen Dienstleister ermöglichen.

Beim **on-street** Parken sind die Betreibermodelle zu unterscheiden. Bei einem singulären Betreiber in einer Kommune steht dem Nutzer nur ein Betreiber zur Bezahlung des Parkplatzes zur Verfügung. Die Datenhaltung und Datenverfügbarkeit liegt dabei beim Betreiber bzw. seinem Serviceanbieter. Der Zahlungsvorgang schließt dabei alle möglichen Zahlungsarten ein. Die Daten sind aktuell proprietär.

Bei einer so genannten Multibetreiber-Plattform für Smart Parking stehen dem Nutzer mehrere Betreiber zur Bezahlung zur Verfügung. Diese Plattformen nutzen zum Datenaustausch und zur Verwaltung Software auf Basis einer gemeinsamen Governance bezgl. Daten, Zertifizierung und Kontrolle.

Die Datenhaltung und Datenverfügbarkeit obliegt dabei beim Plattformbetreiber für die Middleware bzw. den angeschlossenen Parkservice Plattformen. Der Zahlungsvorgang schließ dabei alle möglichen Zahlungsarten ein. Die Daten innerhalb dieser Multibetreiber Netzwerkes sind aktuell proprietär.

2.2.1.2 Herausforderungen für Kommunen

Parkraum ist nicht nur in städtischen Regionen knapp geworden, auch entlang der intermodalen Reise- und Transportkette ist der Stellplatz für Kraftfahrzeuge

6 Vgl. Bitkom, 2009: Telematik & Navigation – Anwendungen und Mehrwertnutzen, Schriftreihe Politik, Berlin, www.dlr.de/rd/Portaldata/28/Resources/dokumente/rn/satnav/Telematik_und_Navigation_web_BITKOM.pdf

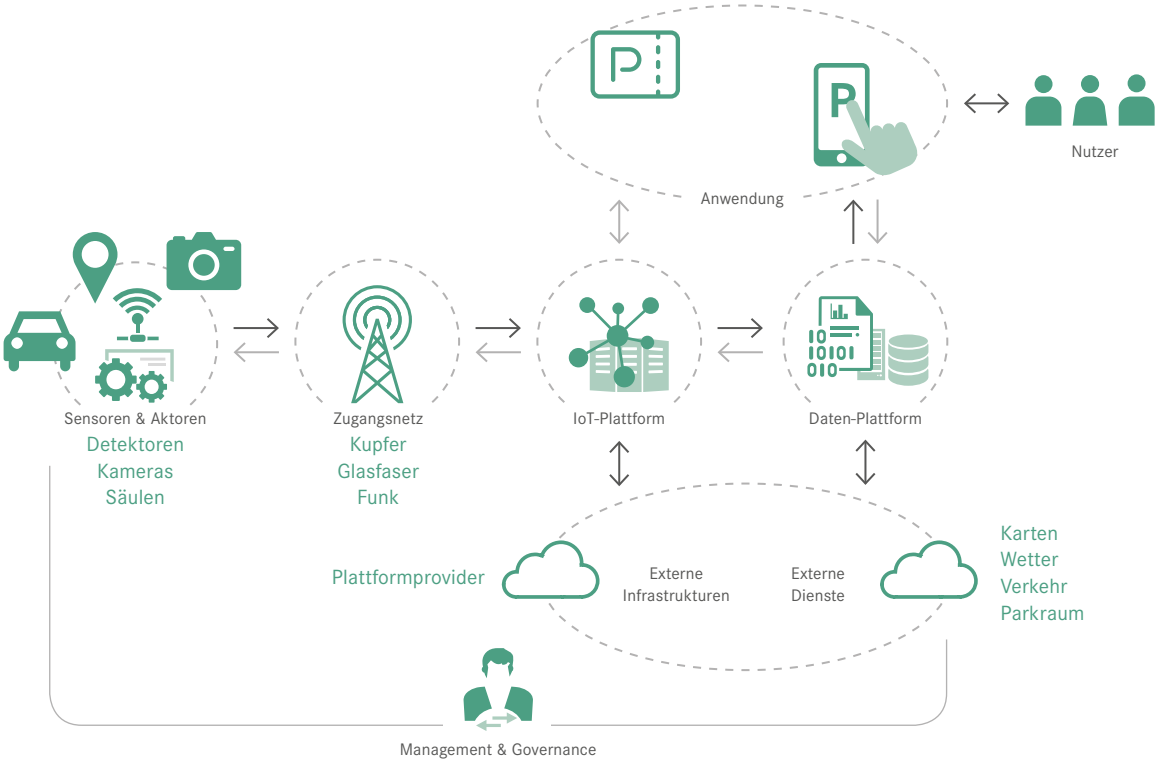

Abbildung 5: Anwendungsfall Parkraummanagement

mancherorts sehr begrenzt. Die Parkraumbewirtschaftung zielt im urbanen Raum auf Faktoren wie z. B.:

- auf die Steuerung des innerstädtischen Verkehrs,
- die Reduzierung des innerstädtischen Parksuchverkehrs,
- die Stauminderung und Verbesserung des städtischen Parkservices,
- Parkraummanagement mit ausgelasteten Parkflächen,
- die Reduktion von Schadstoffemissionen und
- dem Beitrag zur Nachhaltigkeit.

2.2.1.3 Anwendung auf das Übersichtsmodell

Reflektiert man den Anwendungsfall auf das Übersichtmodell, kommt man zu folgender Darstellung (Abbildung 5).

Als Zugangsnetze stehen alle heute bekannten Technologien zur Verfügung: Kupfer, Glasfaser und Funk (Mobilfunk, Narrowband, LoRaWAN etc.).
Für die Anwendungen wurden beispielhaft Handyparken oder Park and Joy bereits erwähnt, dazu gehören aber auch klassische Lösungen wir die Zugangssysteme in Parkhäusern.

Als Sensoren & Aktoren können Bodendetektoren, Kameras, Buchungssäulen, Schranken aber auch Bluetooth oder Nahbereichskommunikationstechnologien aufgeführt werden.

Betrachtet man die Datenebene in einem Gesamtszenario, so ist für ein effizientes Parkraummanagement die Verknüpfung von Daten aus den reinen Parkraumbewirtschaftungslösungen mit weiteren Daten, beispielsweise aus den Bereichen Wetter oder Verkehr, sinnvoll. All diese Daten können dann den Anwendungsfall Parkraumbewirtschaftung als auch andere Anwendungsfälle wie z. B. Verkehrslage, Stadtplanung, Management von Großveranstaltungen als Dritten über Schnittstelle zur Verfügung gestellt werden.

IoT-Plattformen und Datenplattformen stellen dabei das Bindeglied zwischen den Daten, Diensten und Anwendungen dar.

Mit der Erfassung von Daten über Sensoren wie Kameras oder Smart Devices, mit und ohne Verbindung zu anderen Sensoren (Boden, Säule), sind die Datenschutzbestimmungen (Stichwort DSVGO) auch im Anwendungsfall Parkraummanagement relevant und bedürfen bezgl. Datenerhebung, Datennutzung und Anwendungen einer besonderen Überprüfung.

2.2.2 Anwendungsfall „Urbaner Mobilitätshub“

Im Folgenden wird der Anwendungsfall „Parkraummanagement“ beispielhaft beschrieben, und es werden sowohl Ziele als auch praktische Umsetzungsvarianten dargestellt. Als Weiterentwicklung des Anwendungsfalls „Parkraummanagement“ kann der „Urbane Mobilitätshub“ angesehen werden.

2.2.2.1 Beschreibung Anwendungsfall

Der „Urbane Mobilitätshub“ beschreibt eine Vielzahl von Anwendungen auf einer Smart-City-Datenplattform, die folgende Grundfunktionen für die Bürger einer Stadt, deren Mobilitätsanbieter und ihrer IT / Verwaltung anbietet:

- Portal der Verkehrs- bzw. Mobilitätsangebote (Transport & Infrastruktur)
- Bürgerfunktionen der Plattform (Planung, Buchung, Abrechnung)
- Mehrwertdienste / Zusatzangebote (B2x), Onboarding und Stadt-Kennzahlen (KPI)

Im Zuge der fortschreitenden Digitalisierung entwickelt sich aus kommunaler Sicht ein ständig wachsender urbaner Datenraum, der der aus unterschiedlichsten Anwendungen gespeist wird. Viele dieser Anwendungen sind heute in sich abgeschlossen und erlauben keinen Datenübergang in parallele oder höhergestellte Anwendungssysteme, so dass Synergiepotenziale nur bedingt gehoben werden können und ein zentrales Datenmanagement schwierig ist.

2.2.2.2 Herausforderungen für Kommunen

Der **Urbane Mobilitätshub** ist eine **Chance für die Kommunen und Regionen**, die Digitalisierung für ihre Bürger erlebbar zu machen und gleichzeitig ihre eigene Attraktivität zu steigern. Ein großer Schwerpunkt liegt dabei in der umfassenden Zugänglichkeit von Personentransport- und Infrastrukturkomponenten. Während die allseits bekannte „Bahn-App“ mittlerweile zu den meistgenutzten Mobilitäts-Apps gehört, geht der **Urbane Mobilitätshub** eine Stufe weiter, denn er ermöglicht den digitalen Zugang auf alle verfügbaren Anbieter (Personentransport) und Ressourcen der Infrastruktur (Parkraum/Ladesäulen) gleichzeitig. Intelligente Verknüpfungen (Routing) werden möglich und erforderliche Buchungs-/Bezahlvorgänge werden reduziert.

Entlang der gesamten Prozesskette ist die Erhebung und Verarbeitung von **Daten** erforderlich (prozessbegleitender Datenfluss). Diese lassen sich grob in **statische und dynamische Daten** aufteilen. Außerdem ist es sicherlich von Bedeutung, ob **personenbezogene Daten** vorliegen. Eine gute und sehr detaillierte Übersicht der möglichen Datenkategorien bietet die Verordnung (EU) 2017 / 1926.[7]

2.2.2.3 Anwendung auf das Übersichtsmodell

Alle in dieser Beschreibung aufgezählten Funktionen und Dienste lassen sich im vorliegenden Übersichtsmodell und im Dokument „Smart City Data-Plattformen“ der EG beschreiben und abbilden.

Sensoren / Aktoren

Damit die für die Steuerung erforderlichen Daten auf einer Smart City-Datenplattform erhoben und zusammengeführt werden können, ist es notwendig, die entsprechenden Mobilitätskomponenten (wie etwa Transportmittel, Parkplätze und Ladesäulen) mit geeigneten **Sensoren und Aktoren** auszustatten. Erst diese ermöglichen die Erfassung entsprechender Daten und die Steuerung der einzelnen Komponenten im Rahmen des Internet der Dinge.

7 Vgl. Europäische Union (EU), 2017: Delegierte Verordnung (EU) 2017/1926 der Kommission vom 31. Mai 2017 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter multimodaler Reiseinformationsdienste, Brüssel, eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32017R1926&from=EN, im Anhang ab Seite 11

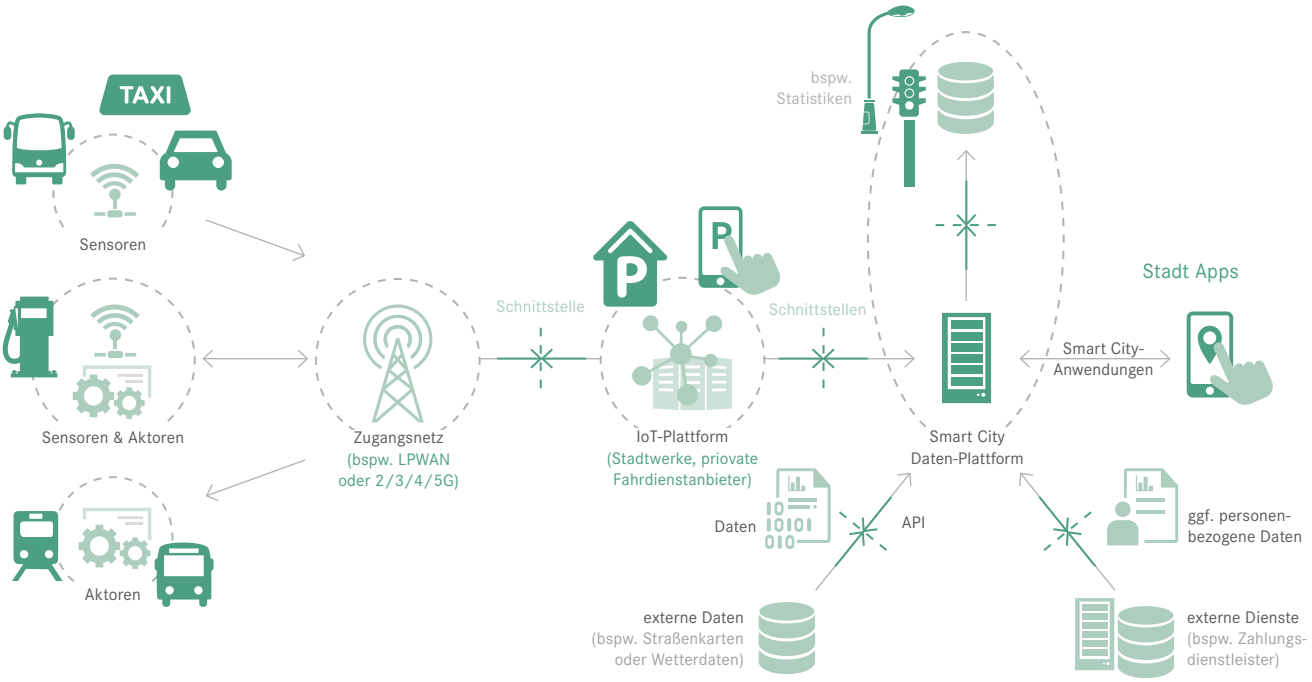

Abbildung 6: Urbaner Mobility-Hub

Zugangsnetze

Als Zugangsnetze kommen alle öffentlichen und privaten Mobilfunk- und Festnetze in Betracht. (2G–5G, LPWAN, WLAN / BLE / Zigbee, Kupfer / Glas, etc.). Die Anforderungen an die Netzinfrastruktur können über die Breite der Anwendungen höchst unterschiedlich ausfallen. Mal reicht ein batteriebetriebener Sensor, der den Zustandswechsel von Parkplätzen (belegt / frei) vor Ladesäulen über ein LPWAN Netz (z. B. NB-IoT) meldet, mal werden Meta-Daten eines Transportmittels (aktueller Ort, Auslastung) von der Onboard-Unit über 4G-Funk an den Mobilitätsanbieter gemeldet, der sie dann per API an die Smart City-Datenplattform weiterleitet.

IoT-Plattform

Eine zentrale Rolle bei der Umsetzung des Urbanen Mobilitätshubs spielt die verwendete IoT-Plattform. Da Sensoren / Aktoren über unterschiedlichste Zugangsnetze angebunden sind, liegt die wesentliche Stärke einer IoT-Plattform darin, die unterschiedlichsten Zugangsprotokolle zu unterstützen (mit und ohne eigene IP-Adresse der Sensoren / Aktoren). Ein weiteres wichtiges Merkmal ist die Flexibilität in der Provisionierung, damit unterschiedlichste Sensoren / Aktoren möglichst schnell im System angemeldet und administriert werden können. Aus betrieblicher Sicht werden die aktuellen Zustandsdaten aller aktiven Sensoren / Aktoren über sogenannte Dashboards visualisiert. Die IoT-Plattform erkennt Anomalien bzw. Fehlerzustände und kann diese zur Behebung weiterleiten. Zudem hält sie alle Konfigurationsdaten und Firmware-Versionen nach und kann diese auch bei Bedarf ändern / updaten (Over The Air – OTA). Da in einer Kommune / Region sehr viele Sensoren / Aktoren verortet sind, viele davon auch mehrfach-Parameter bereitstellen, und darüber hinaus die eben angesprochenen Konfigurationsdaten und Firmwarestände zu administrieren sind, sollte die IoT-Plattform sehr skalierbar sein und zudem auch eine Zwischenspeicherung von Daten für ca. 3 Monate erlauben (IoT-Data-Lake).

Die IoT-Plattform kann sich aus verschiedenen Instanzen zusammensetzen. Ist ein Zugangsnetzbetreiber involviert, wird er für die Sensoren / Aktoren im eigenen

Zugangsnetz eine eigene IoT-Plattform betreiben. Sollte ein Systemintegrator unterschiedlichste Zugangsnetze konsolidieren, wird auch dieser eine eigene IoT-Plattform betreiben. Legt die Kommune / Region großen Wert darauf, eigene Sensorik unkompliziert administrieren zu können, so sollte ebenfalls über den Einsatz einer eigenen IoT-Plattform nachgedacht werden. Die Zusammenschaltung der IoT-Instanzen per API ist unproblematisch, sollte aber die gängigen Datensicherheitskriterien erfüllen. Je nach gewähltem Konstrukt kommen dann Private / Public / Hybrid-Cloud Betriebsumgebungen für die unterschiedlichen IoT-Plattform Instanzen in Betracht.

Smart City-Datenplattform (Big Data-Analytics)
In der Ende-zu-Ende-Betrachtung nimmt die Smart City-Datenplattform die eigentliche Schlüsselfunktion ein und sollte sich in der Hoheit der betroffene Kommune / Region befinden. Sie zeichnet sich dadurch aus,

- dass sie das Urbane Datenmodell abbildet (Vorgabe für alle Mobilitätsanbieter),
- die eigentlichen Portale und Anwendungen der Kommune beherbergt,
- dass sie massenhaft Sensor / Aktor-Daten über einen langen Zeitraum speichern kann,
- höchste Datensicherheitsanforderungen erfüllt und
- große Datenmengen innerhalb kürzester Zeit verarbeiten, auswerten und visualisieren kann.

Insbesondere für den Einsatz von KI-Techniken sollte diese Plattform mit einer entsprechenden Rechenleistung ausgestattet sein. Für den Betrieb dieser Plattform kommen IoT-Systemintegratoren oder die IT-Dienstleister der jeweiligen Kommune / Region in Frage. Als Betriebsmodell bietet sich eine Private / Hybrid Cloud Umgebung an.

2.2.2.4 Ausblick eines möglichen Portal- & Diensteangebotes des „Urbanen Mobilitätshub“

Portal der Mobilitätsangebote (Transport & Infrastruktur)
Die Portalfunktion des Mobility-Hubs bietet den Bürgern der jeweiligen Stadt / Kommune einen digitalen Zugang zu allen nutzbaren Transportmitteln wie z. B. ÖPNV, Asset-Sharing (Car, Bike, Scooter, etc.), Private-Sharing (Ride, Peer-2-Peer, etc.), Taxi (Klassisch, Neue Angebote) und Fernbusse.

Gleichzeitig bietet dieses Portal auch den digitalen Zugang auf die gesamte nutzbare Infrastruktur der jeweiligen Stadt / Kommune. Dazu gehören die verschiedenen Parkräume im öffentlichen und privaten Bereich (z. B. P&R, städtische / private Parkhäuser, städtische / private Parkplätze) sowie Ladesäulen im privaten und öffentlichen Raum.

Vergleichbar mit der bekannten Bahn-App lassen sich nun sämtliche Transportmittel und Infrastrukturen in die individuelle Reiseplanung einbeziehen und können anschließend aus einer Hand gebucht und abgerechnet werden.

Folgende Unterfunktionen können damit abgedeckt werden:

Information
- vor der Reise: Plandaten / Routen, Verfügbarkeiten / Dashboard oder Tarife, Reservierung;
- während der Reise: Navigation, Verspätungen, Alternativrouten, Parkplätze, Anschlüsse oder Barrierefreiheit

Buchung
- ÖPNV-Fahrscheine, Taxis, Mitfahrgelegenheiten oder AssetSharing

Bezahlung
- Zahlungsoptionen, wie Lastschrift, Kreditkarte oder Bezahldienste

Zugang
- Check-In / Check Out, Be In / Be Out, Fahrzeugzugang etc.)

Abrechnung
- Gesamtabrechnung oder Einzelabrechnung, ggfs. Verrechnung zwischen den Mobilitätsdienstleistern

Mehrwertdienste / Zusatzangebote (B2x), Onboarding und Stadt-KPI's
Der entstandene Datenraum der Smart City lässt sich nun durch die Big / Smart Data Analytics Funktion auf neuartige Mehrwertdienste im Sinne der Bürger und Verwaltung anwenden. Diese Mehrwertdienste sind dann direkt für die Bürger / innen nutzbar oder aber dienen der besseren Kooperation der beteiligten Mobilitätsanbieter zur Unterstützung / Verbesserung Ihres Angebotes. Folgende Mehrwertdienste / Zusatzangebote der Stadt sind denkbar:

(Big / Smart) Data-Analytics
- Erkenntnisse aus Bewegungsdaten (Mobilfunk, Google, Stadt-eigene Sensorik)
- Effiziente Verkehrssteuerung
- Angepasste Straßenbeleuchtung
- Eventbasierte Transportmittelbereitstellung
- Parkraumbewirtschaftung
- Ladesäulenplanung
- Erkennung von Anomalien und Optimierungsspielräumen
- Definition urbaner Datenraum

Einbindung kommunaler Angebote
- Tourismus, Events

Durch- / Umsetzung gesetzlicher Vorgaben
- Umweltzonen
- Messung der individuellen Feinstaubbelastung

Info-Portal
- WLAN Hotspots
- Ladesäule @ Home

Onboarding neuer Mobilitätsanbieter
Um der Dynamik einer sich ständig verändernden Smart City gerecht zu werden, bietet der Mobility-Hub ein sogenannte „Onboarding" Möglichkeit, über die sich neue Mobilitätsanbieter registrieren und sich damit in das Portalkonzept einbinden lassen. Gleichzeitig ist aber auch ein geordneter Abmeldeprozess enthalten, falls ein Anbieter sich entschlossen hat, sein Dienstangebot einzustellen bzw. zu verändern.

Aufbau eines urbanen Datenmodells (IT-Plattformarchitektur)
Eine große Aufgabe kommt auf das Stadt-eigene IT-Management zu. Die vorab erwähnten Anwendungsfälle sind individuell und vielschichtig, so dass ein zentrales Datenmodell einen großen Beitrag zur Datenhomogenität leisten kann. So lassen sich Prozesse vereinfachen und neue Anbieter in kürzester Zeit hinzufügen. Das zentrale Datenmodell wird damit zum Kernstück einer jeden Ausschreibung für neue Anwendungsfälle.

Vermarktung von Teilen des urbanen Datenraumes an Dritte
Der Datenraum einer Stadt ist natürlich auch für externe Dienstleister von höchstem Interesse. So beschäftigt z. B. der Mobilitätsanbieter HERE ein großes Team von Data-Scouts, die damit beauftragt sind, wichtige und interessanten Datenräume entstehen zu lassen, um diese im Rahmen eigener Dienstleistungen (zum Beispiel für intelligente Navigationssysteme) einzusetzen. Je strukturierter sich dieser Stadt-eigene Datenraum also präsentiert (zentrales Datenmodell!), desto wertvoller lassen sich die Daten anschließend kommerziell vermarkten.

2.2.3 Anwendungsfall „Energetisches Quartiersmanagement / Energetische Quartierskonzepte"

„Energetische Quartierskonzepte" werden als Instrument zur Planung und Umsetzung energetischer Quartierssanierungen eingesetzt und schaffen die Möglichkeit eines integrierten **„Energetischen Quartiersmanagements"**, das grundsätzlich mittels digital, vernetzter Lösungen umgesetzt werden kann.

2.2.3.1 Beschreibung Anwendungsfall
Die Umsetzung des Energetischen Quartiersmanagements kann maßgeblich dazu beitragen, den **Energieverbrauch im Quartier zu senken** und die **Energieeffizienz zu erhöhen**. Dabei werden immer seltener einzelne Gebäude, als vielmehr energetische Sanierungskonzepte ganzer Quartiere berücksichtigt.

Im Fokus stehen hierbei:

- Energetische Modernisierung von Gebäuden
- Energetische Optimierung der Wärmeversorgung
- Gewinnung und Nutzung regenerativer Energien
- Energieeffiziente Stromnutzung / Einsatz stromsparender Haushaltsgeräte
- Vernetzte, umweltfreundliche Mobilität
- Klimabewusstes Verbraucherverhalten
- Bürgerpartizipation

Erste Umsetzungsschritte finden sich beispielsweise in Köln (GrowSmarter, RheinEnergie AG), Jena (Smartes Quartier Lobeda, Stadtwerke Jena) und Oldenburg (Energetisches Nachbarschaftsquartier, Stadt Oldenburg u. a.).[8]

2.2.3.2 Herausforderungen für Kommunen

Klimafreundliches Bauen und Wohnen ist eine zentrale Säule der aktuellen **Energie- und Klimaschutzpolitik**. Die Bundesregierung hat das Ziel ausgegeben, dass bis zum Jahr 2050 ein nahezu klimaneutraler Gebäudebestand in Deutschland realisiert werden soll. Um dieses Ziel zu erreichen, sind höhere Anteile erneuerbarer Energien am Wärmeverbrauch und energieeffizientere Gebäude notwendig.[9] Ein wichtiger Hebel kann demnach auch die energetische Sanierung bestehender Gebäude und ihr energetisches Management sein. Für Kommunen ergibt sich hieraus eine der großen **Herausforderungen der Energiewende**.

Im Rahmen einer energetischen Modernisierung der Gebäude bzw. der Quartiersanlagen wird die Möglichkeit geschaffen, **energiespezifische und weitere Daten** im Quartier zu erheben. Diese können im Rahmen des Energetischen Quartiersmanagements genutzt werden, um auf Basis einer **vernetzten Plattformlösung** die energiespezifischen Anlagen (Strom und Wärme) intelligent und bedarfsgerecht zu steuern, neue energiebezogene Geschäftsmodelle zu entwickeln sowie weitere Dienste, etwa in den Bereichen der Elektromobilität oder der Bürgerpartizipation, im Quartier anzubieten. Wird das Quartiersmanagement um eine **Mobilitätslösung** erweitert, können die verstärkte Nutzung von E-Mobilität sowie die angestrebte Reduzierung des motorisierten Individualverkehrs (CarSharing) dazu führen, dass zusätzlich **lokale und globale Emissionen** (Lärm, Feinstaub und CO_2) **eingespart** werden.

In Abhängigkeit der Ausgestaltung des Quartierskonzepts und der damit zugrundliegenden **Daten**, ergeben sich mitunter umfassende **Herausforderungen** für die handelnden Akteure. Beispielsweise erlaubt die massenhafte Erfassung, Verknüpfung und Auswertung von Daten immer detailliertere Einblicke in das Verhalten, die Gewohnheiten und die Präferenzen von Verbrauchern. Deshalb erhalten die Themen **Datenschutz, Verbraucherschutz und Datensicherheit** auch in der Energiewirtschaft eine immer größere Bedeutung.[10]

Dies gilt insbesondere für die Erhebung und Verarbeitung **personenbezogener Daten** (vgl. vor allem DSGVO) und die wachsende Bedeutung des **Schutzes von IT-Systemen**. Im Energiesektor sind in diesem Zusammenhang die Vorgaben des IT-Sicherheitsgesetzes, das Betreibern kritischer Infrastrukturen die Einhaltung bestimmter Mindeststandards im Bereich der IT-Sicherheit auferlegt, von grundlegender Bedeutung (vgl. bspw. BSI-KritisV[11]).

2.2.3.3 Anwendung auf das Übersichtsmodell

Sensoren/Aktoren

Damit die für die Steuerung erforderlichen Daten auf einer Smart City Plattform erhoben und zusammengeführt werden können, ist es notwendig, die entsprechenden energiespezifischen Anlagen, Geräte und sonstigen Gegenstände (wie etwa Ladesäulen und Fahrzeuge) mit geeigneten **Sensoren und Aktoren** auszustatten. Erst diese ermöglichen die Erfassung entsprechender Daten und die Steuerung der einzelnen Komponenten im Rahmen des Internet der Dinge.

Eine Installation oder Nachrüstung von Sensoren und Aktoren bietet sich beispielsweise für folgende

8 Vgl. Bitkom, 2019

9 Vgl. Bundesministerium für Wirtschaft und Energie (BMWi), 2015: Energieeffizienzstrategie Gebäude, Berlin, www.bmwi.de/Redaktion/DE/Publikationen/Energie/energieeffizienzstrategie-gebaeude.html

10 Vgl. Bundesnetzagentur, 2017

11 Vgl. BSI, 2016

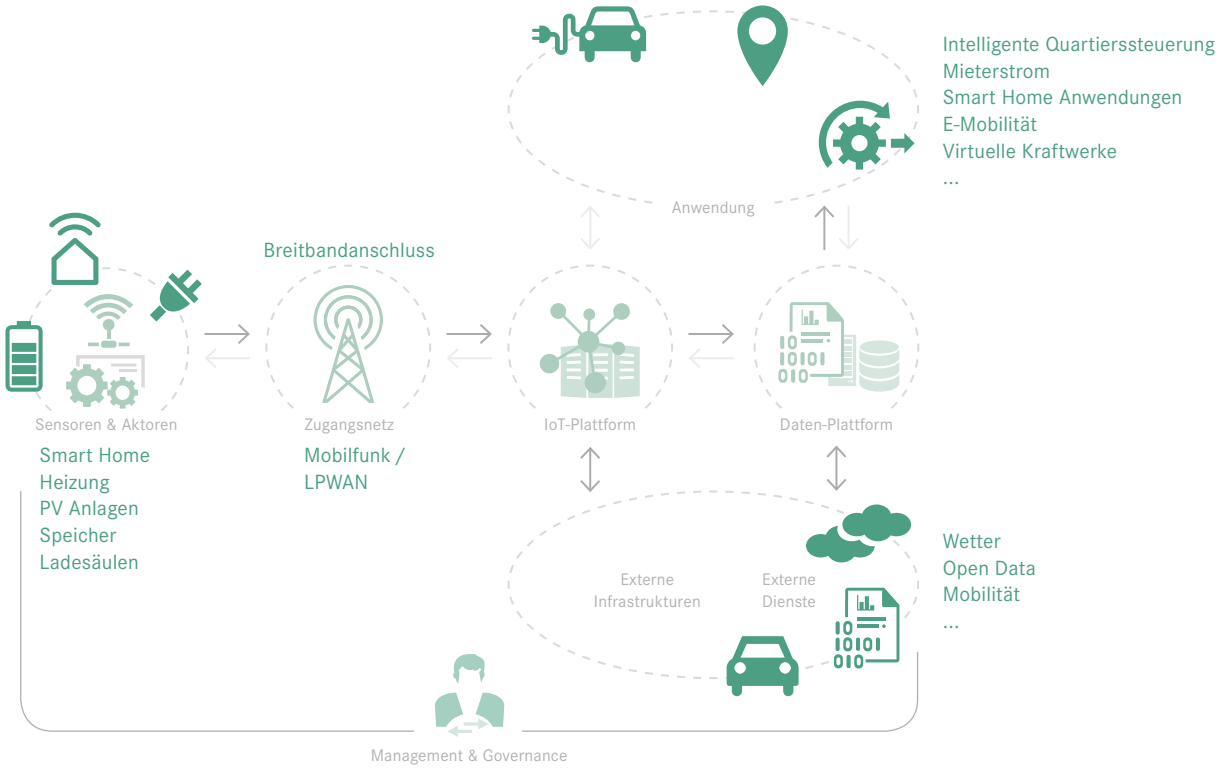

Abbildung 7: Smart City-Plattform: Energetisches Quartiersmanagement

Infrastrukturkomponenten an:

- Photovoltaik Anlagen (PV-Anlagen)
- Batteriespeicher
- Wärmepumpen
- Heizungsanlagen
- Smart Home Geräte
- Ladesäulen
- CarSharing Systeme
- etc.

Zugangsnetze

In den Fokus von Vernetzungsprozessen, wie sie im Rahmen von Smart City Lösungen umgesetzt werden, rückt vor allem die **Qualität der Übertragungstechnologien**. Neben der flächendeckenden Verfügbarkeit sind weitere Qualitätsmerkmale wie eine hohe Datenübertragungsrate, kurze **Latenzzeiten, Zuverlässigkeit, Sicherheit** sowie **Flexibilität** von hoher Relevanz. **Die erforderlichen Qualitäten werden dabei durch den jeweiligen Anwendungsfall bestimmt.** Während einige Anwendungen hohe Datenübertragungsraten erfordern, ist für andere Anwendungen beispielweise eine möglichst geringe Latenz oder eine hohe Zuverlässigkeit zentral. Die Anforderungen an die Netzinfrastruktur können über die Breite der Anwendungen somit höchst unterschiedlich ausfallen.

Grundsätzlich kommen für die Umsetzung des Energetischen Quartiersmanagements sowohl kabelgebundene als auch kabellose Datenübertragungstechnologien in Frage. Gängige Sensorlösungen nutzen als Netzzugang bspw. WLAN, Bluetooth oder Zigbee, deren Reichweite allerdings eingeschränkt ist. Um ein Quartier vollständig einbinden zu können eignen sich eher Technologien mit höherer Reichweite, wie NB-IoT, Sigfox oder LoRaWAN, die speziell für Internet of Things (IoT)-Anwendungen entwickelt wurden.

IoT-Plattform

Eine zentrale Rolle bei der Umsetzung des Energetischen Quartiersmanagements spielt die verwendete IoT-Plattform. Sie ermöglicht die Vernetzung zwischen den einzelnen Geräten, also etwa Sensoren, und den entsprechenden Systemen, die **IoT-Daten speichern,**

verarbeiten und auswerten. Hinzu kommen Funktionen für die **Steuerung und die Analyse von Daten**, das Management von IoT-Anwendungen und das Reporting. Auch erweiterte, KI-basierte, Analysemethoden werden immer öfter angeboten, wie etwa maschinelles Lernen.

Welche Plattform im **Einzelfall** am geeignetsten ist, kann nicht pauschal angenommen werden, da in der Praxis unterschiedliche Lösungen mit unterschiedlichen Schwerpunkten existieren. Dazu zählen bspw. Cloud-Services, Datenanalyse-Plattformen oder Plattformen mit einem Schwerpunkt auf der Verwaltung von IoT-Geräten.

Bei der Auswahl der jeweiligen IoT-Plattform sollten Kommunen bzw. Unternehmen neben den konkreten **aktuellen Anforderungen** auch immer **den Aspekt der Skalierbarkeit** mit einbeziehen. Demnach bestimmen die geplanten Anwendungen maßgeblich die Ausgestaltung der entsprechenden Plattform.

Anwendungen
Die Möglichkeiten der Datenerfassung, -speicherung, -auswertung und -übermittlung sind grundsätzlich vielfältig und eine wichtige Voraussetzung für die Realisierung von **Effizienzpotenzialen** und die Entwicklung **innovativer Dienstleistungen und Produkte**.

Im Bereich des Energetischen Quartiersmanagement sind exemplarisch folgende Anwendungsfälle denkbar.

Energiemanagement: Ein Anwendungsfeld ist das intelligente Energiemanagement für die Bewohner von Quartieren (bspw. automatisierte Steuerung von Heizung, Lüftung und Licht). Voraussetzung dafür ist die Erfassung und Verarbeitung von Daten aus dem Quartier, mit dem Ziel, passgenaue Prognosen für den Energiebedarf (Strom, Wärme oder Ladesäulen) erstellen zu können. Überschüssig erzeugte Energie des Quartiers kann so entweder in Wärme umgewandelt, gespeichert oder ins öffentliche Stromnetz eingespeist werden. Fehlende Energiemengen können entsprechend aus den Speichern oder dem öffentlichen Stromnetz bezogen werden.

Energiehandel: Im Quartier erzeugte Energie kann als Mieterstrom angeboten werden. Als Mieterstrom wird der Strom bezeichnet, der in einem Blockheizkraftwerk oder in einer Photovoltaik-Anlage auf dem Dach eines Wohngebäudes erzeugt und an Letztverbraucher geliefert wird. Außerdem kann im Quartier erzeugte Energie über die Einbindung in ein virtuelles Kraftwerk vermarktet werden und perspektivisch möglicherweise auch (zum Beispiel auf Basis der Blockchain-Technologie) direkt mit Nachbarn gehandelt werden. Auf diese Weise ist die Umsetzung einer nutzerfreundlichen, individuellen Lösung möglich, die es erlaubt, Energie zu beziehen oder überschüssige Energie zu verkaufen.

Weitere Anwendungen: Des Weiteren ist die Umsetzung von Geschäftsmodellen aus dem **Mobilitätssektor** denkbar, die auf Basis der erhobenen Daten und der IoT-Plattform entwickelt werden. Das gilt beispielsweise für Anwendungen aus den Bereichen E-Mobilität oder CarSharing. Ebenfalls denkbar ist die Einrichtung eines plattformbasierten **Bürgerportals**, das genutzt werden kann, um die Quartiersbewohner zu informieren und untereinander zu vernetzen. Im Fokus könnten hierbei energiespezifische Themen (etwa Einsparpotenziale) oder auch allgemeinere kommunale Themen (bspw. Bürgerservices oder regionale Veranstaltungen) stehen.

3. Datenschutz und Sicherheitsanforderungen

Mit der Digitalisierung und damit der Vernetzung entstehen sowohl neue Möglichkeiten für das urbane Leben als auch neue Risiken. Ob das selbstfahrende Auto, der mobilen Service Roboter oder die effiziente Energiesteuerung: dem wichtigen Schutz vor Verletzungen und Beschädigung (Safety-funktionale Sicherheit) muss die Sicherheit der Daten und IT-Systeme insgesamt vor Manipulation und Ausspähungen (Security-Informationssicherheit)[12] und die Verteidigung der Privatsphäre (Datenschutz) an die Seite gestellt sein. Ganzheitlich gedachte Sicherheitskonzeptionen, die alle Aspekte abdecken, sind dafür unabdingbar. Wichtig dabei sind Lösungen, die offenen Standards folgen, herstellerübergreifend stets die neusten Entwicklungen und ‚Security by design' aufgreifen. Ein weiterer zentraler Aspekt ist ein eindeutiger und sicherer Identitätsnachweis für Produkte, Prozesse und Lösungen sowie ein ausreichend abgesicherter Kommunikations- und Informationsaustausch. Ein ebenfalls nicht zu unterschätzender Faktor ist die Nutzerfreundlichkeit. Maßnahmen und Einrichtungen für Safety, Security und Datenschutz müssen sich an den Bedürfnissen der Nutzer orientieren. Wenn diese von Anfang an bei der Erstellung von Sicherheitskonzeptionen mit einbezogen werden, stößt das Sicherheitskonzept auf Akzeptanz und wird dadurch auch eingehalten. Sicherheit hat mit Verlässlichkeit und Vertrauen zu tun. Da sind das Wissen sowie das Verständnis für die Sicherheit und des Datenschutzes wesentliche Faktoren.

Die folgende Beschreibung von Anforderungen an Sicherheit und Datenschutz ist essentiell, aber auch eine nicht-exklusive Darstellung:

- Daten- und Privatsphärenschutz
- Verschlüsselung und Schlüsselmanagement
- Authentifizierung und Identitätsmanagement
- Autorisierung und Zugriffskontrolle.

Wichtig zu erwähnen ist, dass wegen der vielfältigen Bereiche und möglicher Anwendungen einer Smart City-Datenplattform entsprechende Monitoring Sensoren eingerichtet werden, um die Plattform zu überwachen. Mit Hilfe des Monitorings können sowohl betriebsrelevante Parameter wie Latenz und Verbindungsabbrüche erfasst, als auch sicherheitsspezifische Logs (z. B. Login Versuche) aufgezeichnet werden. Diverse Lösungen zur Konsolidierung dieser Logs sind für diesen Zweck auf dem Markt verfügbar.

Qualitätssicherung kann als Sicherstellung der Effektivität der gewählten Maßnahmen aufgefasst werden. Die Sicherung der Qualität ist für alle Phasen bei der Gestaltung von Smart City-Anwendungen und den nötigen Sicherheitsmechanismen wesentlich und sollte deshalb als Prozess integraler Bestandteil der Entwicklung und Implementierung sein.

Die genannten Anforderungen an Sicherheit und Datenschutz fußen dabei auf existierenden Standards wie ISO 27001 und der BSI Standardreihe 200-x mit dem BSI Grundschutz-Kompendium. Dabei wird gezeigt, welche Aspekte bei der Umsetzung des jeweiligen Themas für eine Smart City-Plattform beachtet werden sollten.

3.1 Daten- und Privatsphärenschutz

Daten- und Privatsphärenschutz ist die Voraussetzung für die informationelle Selbstbestimmung eines jeden Nutzers einer Smart City-Anwendung. Das Recht auf informationelle Selbstbestimmung wird als eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) verstanden. Es bezeichnet das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. In Bezug auf das Internet der Dinge bestehen im Hinblick auf die Verwendung personenbezogener

12 Vgl. VDE, 2019, www.vde.com/tic-de/dienstleistungen/informationssicherheit

Daten unterschiedliche Anknüpfungspunkte, bei denen u. a. die Vorgaben der Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) berücksichtigt werden müssen.

Entscheidend ist hier die Aufstellung einer Risikoanalyse und eine Datenschutz-Folgenabschätzung, um eine Übersicht zu erhalten, welche Daten wo erhoben, gespeichert und ausgewertet werden und wer auf welche Daten Zugriff hat. Datenschutzfolgeabschätzungen beantworten die Frage des möglichen Schadens für ein Individuum bei Kompromittierung eines Datenschutzziels. In Bezug auf IoT kann diese Kompromittierung insbesondere durch die Kombination zuvor nicht verketteter Datenquellen erfolgen. Neben den Datenschutzzielen kommt daher der Nicht-Verkettbarkeit eine tragende Rolle zu. Darüber hinaus ist darauf zu achten, dass die eingesetzte Technik auch perspektivisch einsetzbar ist, was das Schließen von Sicherheitslücken und die Update-Fähigkeit der Hardware anbelangt, um die Datenschutz- und Privatsphäre-Vorgaben auch in Zukunft einzuhalten. Die risikoorientierte Maßnahmenwahl und der Nachweis einer adäquaten, risikoorientierten Absicherung sind grundlegende Forderungen der Datenschutzgrundverordnung.

Sensoren & Aktoren

In Abhängigkeit der Daten, die erhoben werden sollen, ergeben sich unterschiedliche Anforderungen. Grundsätzlich sollten nur solche personenbezogenen Daten erhoben werden, die für die Umsetzung einer konkreten Anwendung benötigt werden („Datensparsamkeit“). Sofern perspektivisch der Einsatzbereich einer Anwendung erweitert werden soll, ist dies rechtzeitig einzuplanen. Falls personenbezogene Daten erhoben werden sollen, ist hierfür eine Rechtsgrundlage erforderlich oder die Einwilligung der Betroffenen einzuholen.

Zugangsnetze

Je nach eingesetzter Art der Zugangstechnologie ergeben sich gesonderte Aspekte, die berücksichtigt werden müssen. Sofern der Zugang über öffentlich verfügbare Telekommunikationsnetze erfolgt, werden durch den Telekommunikationsnetzbetreiber z. B. für Abrechnungszwecke meist personenbezogene Daten (beispielsweise Bestandsdaten) erhoben. Der Telekommunikationsnetzbetreiber unterliegt hierfür den strengen Vorgaben des Telekommunikationsgesetzes. Erfolgt der Zugang über „private“ (nicht-öffentliche) Zugangstechnologien, werden möglicherweise keine personenbezogenen Daten erhoben. Sollten doch personenbezogene Daten für den Zugang erhoben werden (vgl. Identitätsmanagement), sind hierfür die jeweiligen Einwilligungen einzuholen und die weiteren Vorgaben von DSGVO und BDSG zu beachten. In jedem Fall bietet sich der Einsatz einer Transport- oder Ende-zu-Ende-Verschlüsselung an, um den Zugriff von unberechtigten Dritten auf die Datenflüsse zu unterbinden.

IoT- und Big Data-Plattform

Für die IoT-Plattform ergeben sich neben den Vorgaben zur IT-Sicherheit, die oben bereits erläutert wurden, vielschichtige Anforderungen in Abhängigkeit der verarbeiteten Daten, da auf der IoT-Plattform sowohl nicht-personenbezogene Daten als auch personenbezogene Daten gespeichert werden können. Dabei sollte das berechtigte Interesse, sowie die Zweckbindung (vgl. Identitätsmanagement, Risikoanalyse und Datenschutz-Folgeabschätzung) für die Ableitung der Anforderungen berücksichtigt werden. Ggf. bietet sich auch eine Verschlüsselung der gespeicherten Daten an.

Smart City-Anwendung

Der Smart City-Anwendung als Schnittstelle der Nutzer zur IoT- und Big Data-Plattform kommt insbesondere im Bereich der Nutzerverwaltung (vgl. Identitätsmanagement) eine hohe Bedeutung zu. Aber auch die durch die Smart City-Anwendung selbst erhobenen Daten (beispielsweise Daten, die durch eine App-Nutzung generiert werden) müssen in Risikoanalysen und Datenschutz-Folgeabschätzungen bedacht und entsprechend der Vorgaben von DSGVO und BDSG berücksichtigt werden. Die Transport- oder Ende-zu-Ende-Verschlüsselung betrifft somit auch die Smart City-Anwendung.

Im Gesamtsystem sind für die Umsetzung von Datenschutz und Datensicherheit folgende Aktivitäten in Abhängigkeit vom Anwendungsfall zu berücksichtigen:

Risikoanalyse
Die Risikoorientierte Maßnahmenwahl und der Nachweis einer adäquaten, risikoorientierten Absicherung sind grundlegende Forderungen der DSGVO. Die Nachvollziehbarkeit der Risikobewertung und der Wahl der Maßnahmen ist entsprechend zu berücksichtigen. Datenschutzfolgenabschätzungen können aus Risikoanalysen abgeleitet werden.

Privacy Impact Analysen (PIA) und Datenschutzfolgeabschätzungen (DSFA)
Privacy Impact Analysen beantworten die Frage des möglichen Schadens für ein Individuum bei Kompromittierung eines Datenschutzziels. In Bezug auf Smart Cities kann diese Kompromittierung insbesondere durch die Kombination zuvor nicht verketteter Datenquellen erfolgen. Eine PIA kann sowohl für eine Risikoanalyse als auch eine Business Impact Analyse genutzt werden, um eine datenschutzkonforme Maßnahmenwahl zu erreichen. Datenschutzfolgenabschätzungen können aus Risikoanalysen abgeleitet werden.

Business Impact Analysen (BIA)
Business Impact Analysen ermöglichen die wirtschaftliche Wahl von Maßnahmen zur Wiederherstellung der Geschäftsfähigkeit nach einem Ausfall. Gerade bei Smart Cities kann die Verfügbarkeit eine zentrale Rolle spielen. Je nach Höhe des zu erwartenden Schadens über einem Zeitraum ist daher die jeweils sinnvolle Wiederherstellungsstrategie zu wählen. Dabei sind neben Ausfällen von beispielsweise Zahlungsdiensten auch im Sinne der EU-DSGVO die Konsequenzen der Nicht-Verfügbarkeit personenbezogener Daten für das Individuum zu berücksichtigen.

3.2 Verschlüsselung und Schlüsselmanagement

Verschlüsselung ist ein grundlegendes Werkzeug zur Wahrung der Vertraulichkeits- und Integritätsziele. So kann, je nach Vertraulichkeits- und Integritätsanforderung, Verschlüsselung eine entscheidende Rolle für Netzwerke, Kommunikation und Anwendungen sämtlicher Anwendungsfälle spielen. Dies sollte jeweils bei der technischen Konzeption der Komponenten berücksichtigt werden.

Sensoren, Aktoren und Zugangsnetze
Diese können häufig auf stark integrierten und miniaturisierten Systemen vorgefunden werden. Es können Anforderungen an die Vertraulichkeit oder Integrität bestehen. Beispielsweise durch entsprechende Kritikalität der erfassten personenbezogenen Daten, hohem Schadenspotential ausgeführter Aktionen, oder der davon abzuratenden, jedoch nach wie vor häufig vorgefundenen Verwendung hartkodierter Informationen im weiteren Sicherheitssystem der Smart City. Bestehen solche Anforderungen, sollte ausreichend Performanz und Speicher für Verschlüsselungsfunktionen und die Aufbewahrung entsprechender Schlüssel vorgesehen werden.

Weiterhin ist auf das Schlüsselmanagement zu achten. So bestehen nur wenige am Markt verfügbare Ansätze für eine effiziente Schlüsselverwaltung von zahlreichen, miniaturisierten und nicht, oder kaum zugänglichen Systemen, die über eine PKI hinausgehen. Daher muss ggf. der Betrieb einer PKI vorgesehen werden.

IoT-Plattform, Smart City-Anwendung und Big Data-Plattform
Die Vertraulichkeitsgewährleistung, die durch Verschlüsselung entsteht, kann zu einer mandantenartigen Zugriffskontrolle herangezogen werden. So ist beispielsweise bei der Verarbeitung personenbezogener Daten, deren verschlüsselte Vorhaltung zu empfehlen. Selbst bei getrennter Verarbeitung verschiedener Daten einer Person kann der unberechtigte Zugriff auf die vereinzelten Datenverarbeitungen zur Profilbildung und somit zur Gefährdung der informationellen Selbstbestimmung der Person führen. In diesem Fall sollte ein

Schlüsselmanagement, personenspezifische Trennungen berücksichtigen und Rechtekonsolidierungen durch Unbefugte vorbeugen.

3.3 Authentifizierung

Authentifizierung ist die Prüfung der vom Nutzer behaupteten Identität. Die Bestätigung der Authentifizierung wird als Autorisierung bezeichnet. Die Authentisierung (Nachweisen der eigenen Identität) kann auf drei verschiedenen Wegen erreicht werden:

- Wissen
- Besitz
- Sein

Die Wahl der Authentifizierungsmethoden führt je nach Anwendungsfall zu Vor- und Nachteilen bei der Praktikabilität für den Nutzer und Sicherheitsbedarf der zu schützenden Information. Prinzipiell gilt: eine Risikoanalyse und die entsprechende Wahl der Authentifizierungsmöglichkeit ermöglicht hierbei passgenaue effektive Entscheidungen.

Sensoren & Aktoren
Da Sensoren & Aktoren sind häufig miniaturisiert, stark integriert und vor allem ohne grundlegende Sicherheitsanforderungen entwickelt worden sind. Es finden sich in diesen teilweise keine oder sehr schwache Authentifizierungsmöglichkeiten. So nutzen viele Sensoren hartkodierte Passwörter oder fälschbare Eigenschaften wie die MAC Adresse zur Authentifizierung. Daher sollte, sofern möglich und sinnvoll, die Auswahl der Sensoren & Aktoren die Verwendung widerrufbarer und fälschungserschwerter Authentifizierungsmerkmale, wie beispielsweise durch Nutzung von Public Key Zertifikaten, berücksichtigen.

Eine Authentifizierung vieler Sensoren und Aktoren in einer Stadt bringen hohe Aufwände an Registrierung, Überwachung und Deregistrierung dieser Sensoren mit sich. Schwächen in dem hierzu notwendigen Identitätsmanagement können auch eine starke Authentifizierung angreifbar machen.

Daher sollte das Risiko, das mit der Authentifizierung einhergeht, betrachtet werden. Dies kann maßnahmenorientiert durch diverse Authentication Assurance Level (Vgl. ISO/IEC 29115:2013[13]) erreicht werden. Aufgrund der Tragweite über die Datensicherheit hinaus und in den Datenschutz hinein, kann jedoch eine risikoorientierte Abwägung der Authentifizierungsstärke sinnvoll sein.

Zugangsnetze
Angriffe auf Mobilfunknetze haben deutlich die Bedeutung der Authentifizierung für Zugangsnetze gezeigt. Insbesondere, wenn die kommunizierenden Sensoren & Aktoren schwache Attribute zur Authentifizierung nutzen, ist die Vertraulichkeit deren Kommunikation von hoher Bedeutung für die Sicherheit des Gesamtsystems. Diese kann jedoch leicht durch Kompromittierung der Empfänger- oder Senderauthentizität gefährdet werden. Daher müssen Zugangsnetze zwischen IoT-Plattform und den Sensoren, bzw. Aktoren, starke Authentifizierungsmerkmale verwenden.

Dies bedeutet, dass die verwendeten Authentifizierungssysteme auf mehreren Faktoren, auf Vertrauenswürdigkeit überprüfbare Zertifikatsketten mit nationalen und glaubwürdigen Zertifikatswurzeln, sowie überprüfbaren Widerrufslisten aufbauen sollten. Dies ist in der Regel bei modernen Netzwerken, wie 4G – 5G gewährleistet.

Dabei müssen jedoch auch Angriffsmöglichkeiten durch Blockieren (Jamming) der entsprechenden Frequenzen berücksichtigt werden. So nutzt beispielsweise GSM ein auf Geheimnissen beruhendes und somit inhärent unsicheres Authentifizierungs- und Verschlüsselungssystem. Angriffe auf moderne Zugangsnetze wirken daher zunächst durch das aktive Blockieren der entsprechenden Frequenzen, auf eine Nicht-Verfügbarkeit der moderneren Netze hin. Dies führt bei den entsprechenden Endgeräten jedoch zur Nutzung des älteren und weitaus schwächeren GSM Standards und somit zur Verwendung eines unsicheren Authentifizierungssystems.

13 Vgl. ISO, 2013: ISO/IEC 29115:2013 Information technology – Security techniques – Entity authentication assurance framework, www.iso.org/standard/45138.html

Daher ist die Stärke des Authentifizierungssystems im Zugangsnetz auch unter Berücksichtigung des möglichst schwächsten Szenarios zu überprüfen. Entsprechende Schwächen sollten in der Gestaltung der Sensoren & Aktoren, sowie der IoT-Plattform Berücksichtigung finden.

IoT-Plattform

Authentifizierung und Authentisierung umfassen bei IoT-Plattformen jeweils häufig nicht nur Sensoren & Aktoren, sondern auch unterschiedliche Nutzergruppen. Gerade Letztere können dabei Endkunden, Geschäftskunden, Mitarbeiter und Administratoren der IoT-Plattform darstellen. Hierbei ist jeweils die Sensitivität der Zugänge zu überprüfen. So kann der Missbrauch eines Endkunden Accounts, Ausgangspunkt für Angriffe auf Administratoren-Accounts, Sensoren, Aktoren, oder die gesamte Smart City-Anwendung sein.

Werden von der IoT-Plattform personenbezogene Daten verarbeitet, so ist der Zugriff auf diese mit entsprechend starker Authentifizierung zu sichern. Dies kann beispielsweise durch die Verwendung von Smart Cards oder 2 Faktor Authentifizierung ermöglicht werden. Solche Systeme können in der Regel mit geringem Aufwand in bestehende Identitätsdateninfrastrukturen (beispielsweise Active Directory) integriert werden.

Bei der Verwendung eines zweiten Faktors ist dabei jedoch auf die Widerrufbarkeit und die Authentizität, Vertraulichkeit und Integrität sämtlicher Möglichkeiten neben der technischen Implementierung (Seitenkanäle) eines Faktors zu achten. Mögliche Seitenkanalangriffe können dabei im Abfangen versendeter zweiter Faktoren, der Selbstvergabe eines zweiten Faktors und der missbräuchlichen Verwendung eines zweiten Faktors liegen. Entsprechende Maßnahmen gegen Seitenkanalangriffe auf Authentifizierungsfaktoren können dabei in internationalen Standards wie der ISO / IEC 29115:2013 gefunden werden.

Unter Einbeziehung mehrerer Organisationen in der IoT-Plattform, kann die Verwendung eines übergreifenden Identitätsmanagements sinnvoll sein. Hierdurch können potentiell Kosten gespart und bereits bestehende Accounts wiederverwendet werden. Somit werden auch Anreize für die Wahl schwacher Authentifizierungsgeheimnisse oder jene zur Wiederverwendung von Authentifizierungsgeheimnissen reduziert.

Solche übergreifenden Identitätsmanagementsysteme bestehen bereits durch föderierte Identitätsmanagementsysteme. Beispielsweise auf der Basis von SAML oder OAuth können hiermit verschiedene Identitätsdateninfrastrukturen gemeinsam kommunizieren. Dabei sollte jedoch auch hier auf die Qualität der jeweiligen Authentifizierung geachtet werden. So kann die Föderation der Authentifizierung zwischen Organisationen, die eine 2-Faktor Authentifizierung nutzen, und jenen, die lediglich einen Faktor verwenden, das Sicherheitsniveau des Gesamtsystems auf das der Authentifizierung mit einem Faktor reduzieren. Auch ein unzuverlässiges Identitätsmanagement einer Organisation und somit beispielsweise das Vorhandensein ungenutzter, jedoch aktiver Accounts, kann in einer anderen teilnehmenden Organisation mit föderierten Identitätsmanagement zu Seitenkanalangriffen führen.

Daher ist bei dieser Art des Identitätsmanagements auf mögliche notwendige Vertrauensstellungen zwischen den Organisationen zu achten. Dabei sollte erörtert werden, ob das Identitätsmanagement der teilnehmenden Organisationen in der Lage ist Identitäten nur für tatsächlich autorisierte Personen einzuräumen, diese in einem angemessenen Zeitraum zu widerrufen, ob Nutzer von Identitäten, diese auch sinngemäß verwenden (bspw. durch die Wahl starker Passwörter), und ob dies auch in angemessenen Zeitabständen von der teilnehmenden Organisationen überprüft wird.

Dies muss jedoch vor dem Hintergrund der entsprechenden Authentifizierungsrisiken betrachtet werden.

Andere Ansätze des verteilten Identitätsmanagements finden sich häufig in dezentralen Identitätsmanagementsystemen, die auf der Grundlage von Blockchain die verteilte Verwaltung von Identitäten ermöglichen. Allerdings reduzieren diese Ansätze häufig das Management der Identitäten und fokussieren sich ausschließlich auf die Speicherung der Identitäten. Bei solchen Ansätzen sollte daher kritisch auf den exakten Registrierungs- Widerrufs- und Auditierungsprozess eingegangen werden. Hierdurch können versteckte Prozesskosten

vorab erkannt und die Vorteile dieser Technologie für die IoT-Plattform besser eingeschätzt werden.

Die Komplexität verteilter Ansätze, wie föderiertes und dezentrales Identitätsmanagement, führt daher in der Praxis häufig dazu, dass weiterhin ein monolithisches Identitätsmanagementsystem einer Organisation verwendet wird. Dies kann auch durchaus die wirtschaftlichste Option sein, da bestehende Workflows des Identitätsmanagements in der Organisation wiederverwertet werden können. Dies kann jedoch den Anreiz zur Wiederverwendung von Faktoren (bspw. PINs) oder der Wahl schwacher Faktoren (bspw. schwache Passwörter) bieten. Die Wahl entsprechender Authentifizierungsfaktoren, die geringere Anreize für diese Probleme bieten, sowie die Gestaltung entsprechender Überprüfungsprozesse kann dies jedoch einschränken.

Je nach Schadenspotential kann die Integration der IoT-Plattform in das bestehende, organisationseigene Identitätsmanagementsystem jedoch zur Steigerung der Risiken für die IoT-Plattform, oder die Organisation beitragen. In einem solchen Fall kann aus Gründen der Kostenersparnis das technische Identitätsmanagement getrennt, jedoch Teile der Workflows des organisationseigenen Identitätsmanagements wiederverwendet werden. Unabhängig von der Gestaltung eines Identitätsmanagements mit mehreren Organisationen sind entsprechende Sicherheitsgarantien in Bezug auf die Authentifizierung bei und von Drittparteien spätestens dann einzufordern, wenn die IoT-Plattform personenbezogene Daten verarbeitet. Diese Sicherheitsgarantien beispielsweise in Bezug auf den Umgang mit Faktoren, die Gestaltung des eigenen Identitätsmanagement, oder der Verwendung einer Mehr-Faktor Authentifizierung kann als Grundlage für Auftragsverarbeitungsbeziehungen genutzt werden und für die legale und einem Stand der Technik entsprechenden Adressierung von Authentifizierungsrisiken notwendig sein.

Privilegierter Accounts der IoT-Plattform können zum Zugriff auf Mandantengetrennte Daten, zur kurzfristigen Kompromittierung von Verfügbarkeit, Integrität und Vertraulichkeit und sogar als Teil komplexerer Angriffe genutzt werden. Dabei kann sowohl der privilegierte Nutzer selbst als auch Schwächen in der Verwendung der Authentifizierungsfaktoren zur Zugriffserlangung auf den privilegierten Account durch Dritte führen. Entsprechend sind privilegierte Accounts in jedem Fall als besonders schützenswertes Objekt zu betrachten.

Dies muss sich dabei ebenfalls in der Authentifizierung wiederspiegeln. So kann gerade für privilegierte Nutzer die Verwendung einer Mehr-Faktoren Authentifizierung sinnvoll sein. Weiterhin bieten privilegierte Identitätsmanagementsysteme die Personalisierung generischer Systemaccounts, Logging von Aktivitäten und entsprechende Verwaltungsmöglichkeiten von Zugangsdaten an.

Smart City-Anwendung
Während eine IoT-Plattform auf Sensoren, Aktoren und Nutzer einer Organisation beschränkt sein kann, zeigen die Beispiele, dass sich eine Smart City-Anwendung über mehrere verschiedene Organisationen, Identitätsmanagementsystem und Nutzerkreise erstrecken kann. Daher sind für Smart City-Anwendungen insbesondere die Handreichungen zum organisationsübergreifenden Identitätsmanagement einer IoT-Plattform zu berücksichtigen.

Big Data-Plattform
Eine Big Data-Plattform kann sowohl Nutzer, als auch Dienstleister für die Smart City-Anwendung sein. Im Rahmen eines möglichen übergreifenden Identitätsmanagements sind daher ggf. notwendige Vertrauensstellungen zwischen der Smart City-Anwendung und der Big Data-Plattform zu berücksichtigen. Auch hier gelten sämtliche Handreichungen zum organisationsübergreifenden Identitätsmanagement einer IoT-Plattform.

3.4 Autorisierung

Autorisierung bezeichnet die Funktion der Zuteilung von Berechtigungen und Privilegien für den Zugriff auf Ressourcen. Die Autorisierung baut im Regelfall auf der oben erläuterten Authentifizierung auf: Nachdem im ersten Schritt der Authentifizierung die Identität einer Einheit zweifelsfrei festgestellt wurde, kann im zweiten Schritt der Autorisierung festgelegt werden, welche Berechtigungen diese Einheit erhält. Dies betrifft beispielsweise Entscheidungen, welche Ressourcen die Einheit nutzen darf, welche Zugriffsrechte für diese Einheit bestehen oder welche Dienste und Anwendungen der Einheit bereitgestellt werden.

Sensoren & Aktoren
Zunächst sind Sensoren und Aktoren vor fremdem Zugriff zu schützen, indem auch hier, wie oben beschrieben, ein Identitätsmanagement angewendet wird und nur Nutzer, die Zugriff auf einzelne Sensoren benötigen, diesen auch erhalten. Darüber hinaus ist darauf zu achten, dass IoT-Geräte selbst auch nur begrenzten Zugriff auf andere Netzwerkressourcen erhalten, damit im Falle der Manipulation einzelner Einheiten weder Schaden an anderen Netzelementen erzeugt wird, noch die von dieser Einheit generierten Daten oder Befehle die anderen Anwendungen stören oder beeinflussen können.

Entsprechende Zugriffskontrollmodelle müssen Konfliktfreiheit aufweisen. Diese kann durch Rechtekonsolidierungen gegeben sein. Daher müssen diese Modelle ständig (oder zumindest in regelmäßigen Abständen) den aktuellen Veränderungen des Systems entsprechend angepasst und aktualisiert werden. Somit spielen im Rahmen der Autorisierung sowohl die Prozesse zur Berechtigungsvergabe als auch zur Auditierung eine tragende Rolle.

Weiterhin ist hinsichtlich der maschinellen Nutzer darauf zu achten, dass diese ein, entsprechend der angedachten Autorisierung, angebrachtes Sicherheitsniveau aufweisen. Insbesondere bei der Verarbeitung von personenbezogenen Daten ist dieser Aspekt wichtig. Denn die Schaffung eines hohen Sicherheitsniveaus im Vorhinein führt dazu, dass eine Einzelbetrachtung von Sensoren & Aktoren im Nachgang nicht mehr zwingend notwendig ist. Somit kann ein besonders hoher Aufwand in der Abschätzung von Folgen und Risiken eines Vorfalls vermieden werden.

Zugangsnetze
Die Anforderungen hinsichtlich der Autorisierung im Bereich der Zugangsnetze ergeben sich aus der Anwendung sowie aus der Art der genutzten Netzzugangstechnologie. Wird auf ein kommerziell verfügbares Kommunikationsnetz als Zugangsnetz zurückgegriffen, erfolgen die Autorisierung und Authentifizierung durch den Netzbetreiber, beispielsweise durch die Ausgabe von SIM-Karten. Wird eine im lizenzfreien Frequenzspektrum verfügbare Zugangstechnologie verwendet, sollte ebenfalls ein Netzbetreiber die Administration und damit auch die Autorisierung vornehmen. Hier kann für die Autorisierung beispielsweise auf das Identitätsmanagement (s. Kapitel Authentifizierung) und für den jeweiligen Anwendungsfall geeigneten Transport oder Ende-zu-Ende-Verschlüsselung zurückgegriffen werden.

IoT- und Big Data-Plattform
Da die IoT-Plattform als zentrale „Datendrehscheibe“ fungiert, stehen hier die Zugriffsrechte der Administratoren, Nutzer und Anwendungen auf diese Datenbank im Vordergrund. Je nach Anwendungsfall können auch Zugriffsrechte von Externen (beispielsweise Infrastrukturbetreibern oder Diensteanbietern) von Bedeutung sein. Solche Zugriffe müssen im Rahmen einer entsprechenden Risikoanalyse im Bereich des Identitätsmanagements (s. Kap. Authentifizierung) Berücksichtigung finden.

Smart City-Anwendung
Die eigentliche Anwendung ist oftmals die Schnittstelle zu den Nutzern, daher sollten die Berechtigungen der Nutzer nur soweit notwendig vergeben werden. Dies sollte entsprechend – wie bei der IoT-Plattform – im Identitätsmanagement berücksichtigt werden.

Im Umgang mit **personenbezogenen Daten** ist eine personenfeine (und konfliktfreie) Rollenzuweisung im Identitätsmanagement zu empfehlen. Die Zugriffe sind entsprechend zu protokollieren. Eine verteilte Zugriffskontrolle kann über Protokolle wie XACML realisiert werden.

Diese vier Sicherheitsanforderungen, begleitet von einem permanenten Monitoring und einer durchgängigen Qualitätssicherung über alle Komponenten und Entwicklungs- / Implementierungs- / Betriebszyklen hinweg, bilden aus Sicht der EG SIKT eine gute Grundlage, um das nötige Vertrauen und die Akzeptanz bei den Bürgern und Gemeindevertretern zum Umsetzen von Smart City-Initiativen zu erreichen. Ferner sind diese Anforderungen auch geeignet, denjenigen das Vertrauen in die Verlässlichkeit der Systeme und Verantwortung zu geben, die diese Plattformen bereitstellen und betreiben, denn ihr Verhalten trägt wesentlich dazu bei, Sicherheit herzustellen oder auch zu gefährden.

4. Zusammenfassung und Empfehlung

Eine erfolgversprechende Investition in Informations- und Kommunikationstechnologien (IKT) im städtischen Kontext ist dann gegeben, wenn ein intelligentes Wechselspiel von Sensorik, Datenraum und Anwendung realisiert wird, bei dem Prozesse effizienter, technologisch fortschrittlicher und nachhaltiger gestaltet werden. Sichere und vertrauenswürdige Datenplattformen nehmen in diesem Setting eine zentrale Rolle ein. Die digitale Transformation von Kommunen zu Smart Cities und Smart Regions schreitet durch den Einsatz von Plattformen weiter voran. Kommunale Smart City-Plattformen können zum einen dem Nutzer einen erheblichen Mehrgewinn bieten. Praxisrelevante Beispiele ergeben sich für die Bürgerinnen und Bürger beispielsweise im Rahmen der dargestellten Anwendungsfälle, sei es die Suche nach dem Parkplatz oder die Nutzung einer umfassenden Mobilitätsplattform. Zum anderen können Smart City-Plattformen bei der Verwaltung und Steuerung der städtischen Infrastruktur einen erheblichen Beitrag leisten. Ein interessantes Beispiel ist das für den Energiesektor dargestellte energetische Quartierskonzept.

Dies hat die EG Sichere IKT-Plattformen bewogen, die vorliegende Handreichung zu erstellen. Im Fokus stehen dabei mit Blick auf sichere Plattformen **Datenschutz und Sicherheitsanforderungen**, die nach einer abstrakten Darstellung bezogen auf drei Anwendungsfälle konkret dargestellt wurden. Für Aufbau und anschließende Nutzung von Smart City-Datenplattformen ist die **Einhaltung von Rahmenbedingungen** essentiell. Dies betrifft zum einen rechtliche Vorgaben, aber auch die Berücksichtigung sonstiger Aspekte, die eine Akzeptanzschwelle für die Nutzung von Datenplattformen darstellen können. Nicht minder wichtig ist die **Einhaltung nationaler und europäischer Sicherheits- und Wertestandards**. Smart City-Plattformen erheben, speichern und verarbeiten oftmals sensible persönliche Daten des Einzelnen mit lokalem Bezug. Sie stellen die Basiskomponenten für die kritischen Infrastrukturen von morgen dar. Smart City-Plattformen müssen daher **höchste Datensicherheit gewährleisten**. Die Diskussion um Wertestandards wird aktuell geführt. Zwingend einzuhalten sind gesetzliche Vorgaben, wie sie die Datenschutzgrundverordnung und das Bundesdatenschutzgesetz für die Verarbeitung personenbezogener Daten vorsieht. Zu wahren sind darüber hinaus die digitale Souveränität der Bürgerinnen und Bürger sowie des Staates. Aus technologischer Hinsicht sind bei der Implementierung von Smart City-Plattformen weitere Aspekte zu berücksichtigen:

Die **Interoperabilität** von Smart City-Plattformen ist zur **Vermeidung von Insellösungen** zu gewährleisten. Diese müssen mit anderen Plattformen oder Systemen ohne Einschränkungen hinsichtlich des Zugriffes oder Implementierung zusammenarbeiten bzw. interagieren können. Voraussetzung dafür sind **standardisierte Schnittstellen**. Die **Offenheit von Standards** ist in diesem Zusammenhang wesentlich, um eine heterogene Software-Landschaft zu unterstützen, freie Innovation zu fördern und die wirtschaftlichen Hürden des Zugangs zu verringern. Sowohl Offenheit gegenüber bestehenden Teillösungen als auch Datensicherheit und Interoperabilität über Domänen hinweg sollten **bereits bei der Planung berücksichtigt werden**, um Akzeptanz bei Bürgern und kommunalen Entscheidungsträgern gleichermaßen sicherzustellen. IKT-Plattformen müssen in der Regel auf die schnelle Verarbeitung hoher Datenmengen und die Verknüpfung einer hohen Anzahl an Subsystemen ausgelegt sein. Um nachhaltig eingesetzt zu werden, müssen sie **Skalierbarkeit bei wachsender Systemgröße oder verarbeitetem Datenvolumen gewährleisten**.

Datenbereitstellung und Datennutzung können mit abgestufter Berechtigung gewährt werden. Dies ermöglicht unter Wahrung rechtlicher Vorgaben und Berücksichtigung von Wertestandards eine wirtschaftliche Nutzung der Daten. Insgesamt sind Smart City-Datenplattformen so zu gestalten, dass sie die Anforderungen an Datensouveränität, Datensicherheit und Interoperabilität im Kontext des Systems der Systeme erfüllen. Die Umsetzung souveräner Plattforminfrastrukturen für Smart Cities und Smart Regions erfordert den Schulterschluss aller Akteure! Kommunen haben auf dem Weg zur Smart City noch einen Weg vor sich. Diese Handreichung versucht, den Weg der Kommunen praktisch zu unterstützen.

5. Anhang

Glossar

Eine Erläuterung von Sicherheitsbegriffen des Papiers (z. B. Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Funktionale Sicherheit) ist verfügbar im Rahmen des Glossars Digitale Vernetzung (it-gipfelglossar.hpi-web.de/).

Literatur

Bitkom, 2019: Smart-City-Atlas – Die kommunale digitale Transformation in Deutschland, Berlin, www.bitkom.org/sites/default/files/2019-03/190318-Smart-City-Atlas.pdf

BSI, 2016: Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz, Bonn, www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html

Bundesinstitut für Bau-, Stadt- und Raumforschung (BBSR) im Bundesamt für Bauwesen und Raumordnung (BBR) / Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMUB), 2017: Smart City Charta – Digitale Transformation in den Kommunen nachhaltig gestalten, Bonn / Berlin, www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/bauen/wohnen/smart-city-charta-kurzfassung-de-und-en.pdf?__blob=publicationFile&v=4

Bundesnetzagentur, 2017: Digitale Transformation in den Netzsektoren, Bonn, www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Digitalisierung/Grundsatzpapier/Digitalisierung.pdf?__blob=publicationFile&v=3

Computerwoche, 2019: Disruption pur – Digitalisierung ist keine Digitale Transformation (Autor: Freddy Staudt), München, 21.05.2019, www.computerwoche.de/a/digitalisierung-ist-keine-digitale-transformation,3546992

Deutscher Städtetag, 2019: Städtetag aktuell 5 / 2019, Berlin / Köln, ISSN 2193-5491, www.staedtetag.de/imperia/md/content/dst/veroeffentlichungen/dst_aktuell/2019/staedtetag_aktuell_5_2019.pdf

Deutsches Institut für Normung e. V. (DIN), 2017: DIN SPEC 91357 – Referenzarchitekturmodell Offene Urbane Plattform (OUP), Berlin, www.beuth.de/de/technische-regel/din-spec-91357/281077528

Deutsches Institut für Normung e. V. (DIN), 2019: DIN SPEC 27072 – Informationstechnik – IoT-fähige Geräte – Mindestanforderungen zur Informationssicherheit, Berlin, www.beuth.de/de/technische-regel/din-spec-27072/30346357

ENISA, 2017: Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, ISBN: 978-92-9204-236-3, doi: 10.2824/03228, www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

Expertengruppe Smart Cities / Smart Regions der Fokusgruppe Intelligente Vernetzung des Nationalen Digital-Gipfels, 2015: Intelligente Städte und Regionen in Deutschland – Aufruf zur digitalen Transformation, div-konferenz.de/app/uploads/2015/12/151109_FG2_014_PG_Smart_City_Positionspapier_Ansicht.pdf

Expertengruppe Smart Cities / Smart Regions der Fokusgruppe Intelligente Vernetzung des Nationalen Digital-Gipfels, 2017: Intelligente Städte und Regionen in Deutschland – Handreichung zur Umsetzung der digitalen Transformation, deutschland-intelligent-vernetzt.org/app/uploads/2017/07/20170612_DIV-Handreichung-Intelligente-Staedte-und-Regionen.pdf

FIWARE Foundation: FIWARE Overview, Berlin, www.fiware.org/developers/

Fokusgruppe Intelligente Vernetzung des Nationalen Digital-Gipfels, 2017: Zukunft wird vor Ort gemacht – Aufruf zur Legislaturperiode 2017–2021, deutschland-intelligent-vernetzt.org/app/uploads/2017/07/20170609_DIV-Aufruf-Legislatur-2017-2021.pdf

Matthias Flügge, Jens Fromm (Hg.), 2016: Public IoT – Das Internet der Dinge im öffentlichen Raum, FraunhoferInstitut FOKUS, www.fokus.fraunhofer.de/news/public_iot_5_2016

Fraunhofer-Institute FOKUS, IAIS & IML, 2018: Urbane Datenräume – Möglichkeiten von Datenaustausch und Zusammenarbeit im urbanen Raum, Studie im Auftrag des Bundesministerium für Bildung und Forschung, Berlin, www.fokus.fraunhofer.de/de/fokus/projekte/urbane_datenraeume

Jens Tiemann, Fabian Manzke et al., 2019: Funkende Dinge, In: Mike Weber (Hg.), 2016: ÖFIT-Trendschau: Öffentliche Informationstechnologie in der digitalisierten Gesellschaft. Berlin: Kompetenzzentrum Öffentliche IT, www.oeffentliche-it.de/-/funkende-dinge

Videos

FIWARE – Open Source Platform for our Smart Digital Future www.youtube.com/watch?v=7VH3wJmMdPU
Introduction to FIWARE www.youtube.com/watch?v=97JsnnpPLrA

Autoren

Baumgarten, Patrick: Bundesnetzagentur
Diederichs, Jörg: Huawei Technologies Düsseldorf GmbH
Gille, Daniel: T-Systems International GmbH
Grigutsch, Ralf: T-Systems GmbH
Gross, Christian: VDE e. V.
Grün, Philipp: Bundesministerium für Wirtschaft und Energie
Kurowski, Sebastian: Fraunhofer IAO
Mühlner, Jens: T-Systems International GmbH
Neufert, Caroline: BearingPoint GmbH
Tiemann, Jens: Fraunhofer FOKUS, Kompetenzzentrum Öffentliche IT

Abbildungsverzeichnis

Expertengruppe Sichere IKT-Plattformen für intelligente Netze

Vorsitz

Caroline Neufert
BearingPoint GmbH
caroline.neufert@bearingpoint.com

Mitwirkende

Dr. Dirk Achenbach
FZI Forschungszentrum Informatik

Dr. Ingmar Baumgart
FZI Forschungszentrum Informatik

Patrick Baumgarten
Bundesnetzagentur

Thorsten Behrens
CIB software Gmbh

Jörg Diederichs
Huawei Technologies Düsseldorf GmbH

Peter Ganten
Open Source Business Alliance e. V.

Sven Gelzhäuser
1&1 De-Mail GmbH

Doris Gemeinhardt-Brenk
Bundesnetzagentur

Ralf Grigutsch
T-Systems GEI GmbH

Dr. Christian Groß
VDE e. V.

Dr. Ulli Jamitzky
Roland Berger GmbH

Christoph Kaesberger
Bitkom e. V.

Markus Klein
Bundesnetzagentur

Andreas Kleinert
NUIX Ireland Ltd.

Sebastian Kurowski
Fraunhofer IAO

Dr. Alexander Lenk
BMW Group

Jens Mühlner
T-Systems International GmbH

Dr. Ulf Narloch
Initiative Stadt.Land.Digital

Marie Nietan
Bitkom e. V.

Percy Ott
Cisco Deutschland

Leslie Romeo
1&1 De-Mail GmbH

Dr. Volker Schanz
VDE Verband Der Elektrotechnik Elektronik Informationstechnik e. V.

Jens Tiemann
Fraunhofer FOKUS

Markus Wartha
Power Providing GmbH

Tobias Wernado
Bundesnetzagentur

Udo Zaudig
Stadt Köln

Vertiefende Informationen und Veröffentlichungen zum Download:
deutschland-intelligent-vernetzt.org/expertengruppen/expertengruppe-sichere-ikt-plattformen-fuer-intelligente-netze/

Alle Dokumente
und Publikationen
kostenlos zum Download:

www.deutschland-intelligent-vernetzt.org

Digital Gipfel

Positionspapier der Expertengruppe
Sichere IKT-Plattformen für intelligente Netze
Fokusgruppe Intelligente Vernetzung

Oktober 2019

Herausgeber
Digital-Gipfel
Plattform Innovative Digitalisierung der Wirtschaft

Ansprechpartner

Caroline Neufert
BearingPoint GmbH
caroline.neufert@bearingpoint.com

www.deutschland-intelligent-vernetzt.org