ARTIKEL-29-DATENSCHUTZGRUPPE

1471/14/DE
WP 223

Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge

angenommen am 16. September 2014

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

eingesetzt durch Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf Artikel 29 und Artikel 30 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

ZUSAMMENFASSUNG

Das „Internet der Dinge“ (Internet of Things, IoT) befindet sich an der Schwelle zur Integration in das Leben der EU-Bürger. Zwar muss die Durchführbarkeit vieler Projekte im Internet der Dinge erst noch bestätigt werden, doch bereits heute werden „intelligente Objekte“ zur Verfügung gestellt, die unsere Wohnung, das Auto, den Arbeitsplatz und sportliche Aktivitäten überwachen und mit ihnen kommunizieren. Schon heute werden vernetzte Geräte dem Bedarf der EU-Bürger auf den großen Märkten des *Quantified Self* und der Domotik gerecht. Somit bietet das Internet der Dinge für eine Vielzahl kleiner wie großer innovativer und kreativer EU-Unternehmen, die auf diesen Märkten tätig sind, bedeutende Wachstumsaussichten.

Die Artikel-29-Datenschutzgruppe möchte, dass diese Erwartungen sowohl im Interesse der Bürger als auch der EU-Wirtschaft erfüllt werden. Im Zusammenhang mit den erwarteten Vorteilen müssen jedoch auch die vielen Herausforderungen bezüglich des Schutzes der Privatsphäre und der Sicherheit, die mit dem IoT verknüpft sein können, berücksichtigt werden. Über die Anfälligkeit dieser Geräte, die oftmals außerhalb herkömmlicher IT-Strukturen eingesetzt werden und in die häufig keine ausreichenden Sicherheitsmerkmale eingebaut sind, erheben sich viele Fragen. Datenverluste, Infektionen durch Schadprogramme, aber auch unberechtigter Zugang zu personenbezogenen Daten, in die Privatsphäre eingreifende Verwendung tragbarer Geräte oder unzulässige Überwachung sind Risiken, die die Akteure im IoT angehen müssen, um ihre Produkte oder Dienstleistungen für potenzielle Endnutzer attraktiv zu machen.

Über die rechtliche und technische Konformität hinaus geht es hier um die Auswirkungen auf die Gesellschaft insgesamt. Organisationen, die bei der Produktentwicklung ihren Schwerpunkt auf den Schutz der Privatsphäre und den Datenschutz legen, werden gewährleisten können, dass ihre Waren und Dienstleistungen dem Grundsatz des eingebauten Datenschutzes („Privacy by Design“) gerecht werden und über die von den EU-Bürgern erwarteten datenschutzfreundlichen Standardeinstellungen verfügen.

Bisher wurde dieses Thema nur sehr allgemein von einigen Regulierungsbehörden und Akteuren in und außerhalb der EU angesprochen. Die Artikel-29-Datenschutzgruppe hat beschlossen, sich mit diesem Thema näher zu befassen und zu diesem Zweck die vorliegende Stellungnahme angenommen. Sie will damit zur einheitlichen Anwendung des Rechtsrahmens für den Datenschutz im Internet der Dinge sowie zur Entwicklung eines hohen Schutzniveaus für personenbezogene Daten in der EU beitragen. Die Einhaltung dieses Rahmens ist von entscheidender Bedeutung sowohl für die Bewältigung der rechtlichen und technischen Herausforderungen als auch für die Bewältigung der genannten gesellschaftlichen Herausforderungen, da er auf der Einstufung des Schutzes personenbezogener Daten als Grundrecht basiert.

Daher werden in der vorliegenden Stellungnahme die wichtigsten Datenschutzrisiken im Ökosystem des Internet der Dinge aufgezeigt und anschließend Leitlinien für die Anwendung des Rechtsrahmens der EU in diesem Kontext gegeben. Die Arbeitsgruppe spricht sich dafür aus, dass die zuständigen Akteure die höchstmöglichen Garantien für den einzelnen Nutzer zu einem wesentlichen Aspekt ihrer Projekte erheben sollten. Insbesondere müssen die Nutzer über die gesamte Lebensdauer eines Produktes die vollständige Kontrolle über ihre personenbezogenen Daten behalten, und wenn Organisationen Daten auf der Grundlage einer Einwilligung verarbeiten, muss diese Einwilligung ohne Zwang, für den konkreten Einzelfall und in Kenntnis der Sachlage erfolgen. Um sie dabei zu unterstützen, hat die Arbeitsgruppe eine umfassende Reihe praktischer Empfehlungen für die verschiedenen Akteure (Hersteller von Endgeräten, Anwendungsentwickler, soziale Plattformen,

weitere Empfänger von Daten, Datenplattformen und Normungsgremien) entwickelt, die ihnen helfen sollen, den Datenschutz und den Schutz der Privatsphäre in ihren Produkten und Dienstleistungen umzusetzen.

Der Schlüssel zu Vertrauen und Innovation und somit zum Erfolg auf diesen Märkten besteht darin, den Einzelnen zu stärken, indem man ihn informiert und dafür sorgt, dass er frei und sicher bleibt. Die Arbeitsgruppe ist fest davon überzeugt, dass Akteure, die diese Erwartungen erfüllen, einen außergewöhnlichen Wettbewerbsvorteil gegenüber anderen Akteuren haben, deren Geschäftsmodelle darauf beruhen, dass ihre Kunden in ihrem Ökosystem eingeschlossen und in Unkenntnis darüber gelassen werden, in welchem Umfang ihre Daten verarbeitet und weitergegeben werden.

In Anbetracht der vom IoT aufgeworfenen wichtigen Herausforderungen in Bezug auf den Datenschutz wird die Artikel-29-Datenschutzgruppe dessen Entwicklung weiterhin überwachen. Sie bleibt offen sowohl für eine Zusammenarbeit mit anderen internationalen Regulierungsbehörden und Gesetzgebern in Bezug auf diese Themen als auch für Diskussionen mit Vertretern der Zivilgesellschaft sowie der entsprechenden Branchen - insbesondere wenn diese Akteure als für die Verarbeitung Verantwortliche und Auftragsverarbeiter in der EU tätig sind.

EINLEITUNG

Unter dem Begriff „Internet der Dinge“ versteht man eine Infrastruktur, in der Milliarden von in gewöhnlichen, alltäglichen Geräten („Dinge“ als solche oder Dinge, die mit anderen Objekten oder Personen verbunden sind) eingebetteten Sensoren Daten erheben, verarbeiten, speichern, weiterleiten und - da ihnen eindeutige Kennungen zugeordnet sind - sich über Netzwerkfunktionen mit anderen Geräten oder Systemen verbinden und austauschen können. Da das Internet der Dinge auf dem Grundsatz einer umfassenden Datenverarbeitung durch diese für eine unauffällige Kommunikation und einen nahtlosen Datenaustausch konzipierten Sensoren aufbaut, wird es mit den Begriffen „allgegenwärtig“ und „omnipräsent“ verknüpft.

Akteure des Internets der Dinge wollen neue Anwendungen und Dienstleistungen anbieten, indem sie Daten über Personen sammeln und neu miteinander kombinieren, sei es „nur“, um die umweltspezifischen Daten eines Nutzers zu erheben oder aber, um gezielt dessen Gewohnheiten zu überwachen und auszuwerten. Mit anderen Worten: Das Internet der Dinge bringt in der Regel mit sich, dass Daten verarbeitet werden, die bestimmte oder bestimmbare natürliche Personen betreffen und somit als personenbezogene Daten im Sinne von Artikel 2 der EU-Datenschutzrichtlinie gelten.

Die Datenverarbeitung erfordert hierbei ein koordiniertes Eingreifen einer Vielzahl von Akteuren (Gerätehersteller, die teilweise auch als Datenplattformen, Datenaggregatoren oder -vermittler agieren, Anwendungsentwickler, soziale Plattformen, Geräteverleiher oder -vermieter usw.). Die Rollen dieser Akteure werden in dieser Stellungnahme eingehender betrachtet. Die verschiedenen Akteure können aus diversen Gründen beteiligt sein, beispielsweise um zusätzliche Funktionen oder leichter nutzbare Schnittstellen anzubieten, die die Handhabung der technischen und Privatsphäre-Einstellungen ermöglichen, oder da ein Nutzer häufig über eine bestimmte Internetschnittstelle Zugang zu den eigenen Daten erhält. Darüber hinaus können die Daten, sobald sie extern gespeichert wurden, mit anderen Parteien geteilt werden, wessen sich der betroffene Nutzer zuweilen nicht bewusst ist[1]. In diesen Fällen wird die Weiterübertragung der Daten dem Nutzer aufgezwungen, der sie nicht verhindern kann, ohne die meisten Funktionen des Gerätes zu deaktivieren. Infolge dieser

[1] http://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf

Handlungskette kann das Internet der Dinge die Gerätehersteller und deren Geschäftspartner in die Lage versetzen, sehr detaillierte Nutzerprofile erstellen oder auf diese zugreifen zu können.

Angesichts dessen bringt das IoT eindeutig neue und bedeutende Herausforderungen in Bezug auf den Datenschutz und den Schutz der Privatsphäre mit sich.[2] Einige Entwicklungen des IoT können, wenn sie nicht kontrolliert werden, sogar eine nach EU-Recht unzulässige Form der Überwachung von natürlichen Personen entstehen lassen. Das IoT wirft darüber hinaus wichtige Sicherheitsfragen auf, da Sicherheitsverstöße für Personen, deren Daten in diesem Kontext verarbeitet werden, große Risiken in Bezug auf den Datenschutz mit sich bringen können.

Die Artikel-29-Datenschutzgruppe hat daher beschlossen, die vorliegende Stellungnahme vorzulegen, um dazu beizutragen, dass die durch diese Tätigkeiten verursachten Risiken für die Grundrechte von EU-Bürgern ermittelt und überwacht werden können.

1. Umfang der Stellungnahme: Schwerpunktlegung auf drei bestimmte Entwicklungen des Internet der Dinge

Bisher lässt sich nicht mit Gewissheit vorhersagen, in welchem Umfang sich das Internet der Dinge weiterentwickeln wird. Dies liegt teilweise daran, dass die Frage, wie die im IoT erhebbaren Daten in etwas Nützliches und somit kommerziell Rentables umgewandelt werden können, weitgehend offen bleibt. Ebenso ungeklärt ist die Frage der möglichen Konvergenz und etwaiger Synergien des IoT mit anderen technischen Entwicklungen wie dem Cloud-Computing und „Predictive Analytics“, die bisher nur Entwicklungen auf Schwellenmärkten betreffen.

Die Artikel-29-Arbeitsgruppe hat daher beschlossen, sich in dieser Stellungnahme auf drei bestimmte Entwicklungen des Internet der Dinge („Wearable Computing“, „Quantified Self“ und Domotik) zu konzentrieren, die (1) direkt mit dem Nutzer verknüpft sind und (2) Geräte und Dienste betreffen, die tatsächlich verwendet werden und sich daher für eine Analyse nach Maßgabe der Datenschutzbestimmungen eignen. Auf B2B-Anwendungen und globalere Fragen wie die Entwicklung „intelligenter Städte“ oder „intelligenter Verkehrssysteme“ sowie Maschine-zu-Maschine-Entwicklungen wird in dieser Stellungnahme nicht näher eingegangen. Nichtsdestotrotz können die Grundsätze und Empfehlungen dieser Stellungnahme auch außerhalb ihres engen Rahmens Gültigkeit besitzen und auch auf diese anderen Entwicklungen zutreffen.

1.1 **Wearable Computing**

Der Begriff „Wearable Computing“ bezieht sich auf Kleidungsstücke und Alltagsgegenstände wie Armbanduhren und Brillen, in die Sensoren integriert werden, um deren Funktionen zu erweitern. Bei tragbaren Dingen, besteht die Wahrscheinlichkeit, dass diese schnell angenommen werden, weil sie den Nutzen vertrauter Alltagsgegenstände erweitern und kaum von nicht vernetzten Geräten zu unterscheiden sind. In sie können Kameras, Mikrofone und Sensoren integriert sein, die Daten erfassen und an den Gerätehersteller übertragen können. Zudem wird durch die Verfügbarkeit von Programmierschnittstellen (API) (z. B. „Android Wear“[3]) auch die Entwicklung von Anwendungen durch Drittanbietern gefördert, die auf diese Weise Zugang zu den von diesen Objekten gesammelten Daten erhalten.

[2] Diese Stellungnahme sollte auch in Verbindung mit den im Jahr 2014 von der Arbeitsgruppe angenommenen Stellungnahmen zur Anwendung der Begriffe der Notwendigkeit und der Verhältnismäßigkeit sowie des Datenschutzes im Bereich der Strafverfolgung (WP 211) bzw. zur Überwachung (WP 215) gelesen werden.

[3] http://developer.android.com/wear/index.html

1.2 **Quantified Self**

„Quantified-Self"-Dinge werden dafür konzipiert, regelmäßig von Personen getragen zu werden, die Informationen über ihre Gewohnheiten und Lebensweisen erfassen möchten. Beispielsweise kann eine Person jede Nacht einen „Sleep Tracker" tragen, um einen umfassenden Überblick über ihre Schlafphasen zu erhalten. Bei anderen Geräten hingegen liegt der Schwerpunkt auf der Bewegungsverfolgung: Leistungszähler beispielsweise messen quantitative Indikatoren für physische Aktivitäten von Personen (z.B. verbrannte Kalorien oder gelaufenen Entfernungen) und zeigen diese an.

Andere Objekte messen das Gewicht, den Puls oder andere Gesundheitsindikatoren. Durch die Überwachung von Verhaltenstendenzen und -änderungen über einen gewissen Zeitraum können die erhobenen Daten analysiert und - beispielsweise mittels Bewertung der Qualität und der Auswirkungen der körperlichen Betätigung anhand vorab eingestellter Grenzwerte - qualitative gesundheitsbezogene Informationen gewonnen sowie innerhalb bestimmter Grenzen sogar Aussagen über das Vorliegen etwaiger Krankheitssymptome getroffen werden.

„Quantified-Self"-Sensoren müssen häufig unter bestimmten Bedingungen getragen werden, um die betreffenden Informationen zu gewinnen. So kann beispielsweise ein am Gürtel der betroffenen Person angebrachter Beschleunigungsmesser mit Hilfe geeigneter Algorithmen Bauchbewegungen messen *(Rohdaten)*, Informationen über den Atemrhythmus *(aggregierte Daten und extrahierte Informationen)* sammeln und die Belastungswerte der betroffenen Person *(Anzeigedaten)* anzeigen Auf einigen Geräten werden dem Nutzer nur die letztgenannten Informationen angezeigt, doch möglicherweise kann der Gerätehersteller oder der Dienstanbieter auch auf weitere Daten zugreifen, die zu einem späteren Zeitpunkt ausgewertet werden können.

Im Bereich „Quantified Self" stellen sich verschiedene Herausforderungen aufgrund der Art der erhobenen, möglicherweise vertraulichen gesundheitsbezogenen Daten sowie des Umfangs der Datenerhebung. Insofern als hierbei die Nutzer motiviert werden sollen, gesund zu bleiben, bestehen viele Verbindungen zum Ökosystem der elektronischen Gesundheitsdienste. Gleichwohl haben aktuelle Untersuchungen Zweifel an der Genauigkeit der Messungen und den daraus gezogenen Schlussfolgerungen aufkommen lassen.[4]

1.3 **Domotik**

Heute kann man auch in Büros oder Wohnungen IoT-Geräte wie „vernetzte" Glühbirnen, Thermostate, Rauchmelder, Wetterstationen, Waschmaschinen oder Backöfen finden, die über das Internet ferngesteuert werden können. So können Objekte mit Bewegungssensoren feststellen und aufzeichnen, wann ein Nutzer zu Hause ist und welches seine Bewegungsmuster sind und womöglich bestimmte vorab eingestellte Funktionen auslösen (z. B. eine Lampe einschalten oder die Raumtemperatur verändern). Die meisten Domotik-Geräte sind konstant vernetzt und können Daten an den Hersteller übermitteln.

Es ist offensichtlich, dass die Domotik spezielle Herausforderungen in Bezug auf den Datenschutz und den Schutz der Privatsphäre mit sich bringt, da die Auswertung des Nutzungsverhaltens in diesem Zusammenhang Details über die Lebensweise, Gewohnheiten oder Entscheidungen der Bewohner oder einfach nur über ihre Anwesenheit zu Hause offenlegen kann.

[4] http://bits.blogs.nytimes.com/2014/04/27/for-fitness-bands-slick-marketing-but-suspect-results

Die drei oben genannten Gerätekategorien stehen exemplarisch für die meisten Fragen zum Datenschutz im aktuellen Internet der Dinge. Gleichwohl können sich diese Kategorien auch überlappen: Ein „tragbares“ Gerät wie eine „intelligente“ Uhr beispielsweise kann auch dazu verwendet werden, die Herzfrequenz zu messen (z. B. für eine „Quantified Self“-Bewertung).

2. Mit dem Internet der Dinge verbundene Herausforderungen für den Datenschutz und den Schutz der Privatsphäre

Die Artikel 29-Arbeitsgruppe hat diese Stellungnahme erstellt, weil das Internet der Dinge ihrer Meinung nach eine ganze Reihe von Herausforderungen bezüglich des Datenschutzes und des Schutzes der Privatsphäre mit sich bringt, von denen einige neu und andere altbekannt sind, aber durch die mit der Weiterentwicklung des IoT verbundene exponentielle Zunahme der Datenverarbeitung, verstärkt werden. Die Wichtigkeit der Anwendung des Rechtsrahmens der EU für den Datenschutz und der diesbezüglichen, nachfolgend genannten praktischen Empfehlungen ist im Lichte dieser Herausforderungen zu sehen.

2.1 **Mangelnde Kontrolle und Informationsasymmetrie**

Aufgrund der Notwendigkeit, Dienstleistungen ständig und unauffällig zu erbringen, können Nutzer in der Praxis durch Dritte überwacht werden. Je nachdem, ob die Erhebung und Verarbeitung dieser Daten transparent ist oder nicht, kann dies dazu führen, dass Nutzer die Kontrolle über die Weitergabe ihrer Daten verlieren.

Generell führt die Interaktion zwischen Objekten, zwischen Objekten und den Geräten von Personen, zwischen Personen und anderen Objekten und zwischen Objekten und Back-End-Systemen zur Erzeugung von Datenflüssen, die kaum mit den klassischen zur Gewährleistung eines geeigneten Schutzes der Interessen und Rechte der betroffenen Personen verwendeten Werkzeugen gehandhabt werden können. Im Gegensatz zu anderen Inhalten können im Internet der Dinge übertragene Daten beispielsweise vor ihrer Veröffentlichung möglicherweise nicht ausreichend von der betroffenen Person überprüft werden und dadurch für den Nutzer unbestreitbar das Risiko eines Kontrollverlusts und einer übermäßigen Selbstentblößung entstehen. Auch kann die Kommunikation zwischen Objekten automatisch und standardmäßig ausgelöst werden, ohne dass die Person sich dessen bewusst ist. Ohne die Möglichkeit, wirksam zu kontrollieren, wie die Objekte interagieren, oder durch die Festlegung aktiver oder nicht aktiver Zonen für bestimmte Dinge virtuelle Grenzen zu setzen, wird es außergewöhnlich schwierig, den erzeugten Datenfluss zu kontrollieren. Die anschließende Datenverwendung zu kontrollieren und somit eine mögliche schleichende Ausweitung der Zweckbestimmung zu verhindern, wird noch schwieriger. Dieses Problem der mangelnden Kontrolle, das sich auch bei anderen technischen Entwicklungen wie dem Cloud-Computing oder bei großen Datenmengen stellt, wird sogar zu einer noch größeren Herausforderung, wenn man sich bewusst macht, dass diese unterschiedlichen neu entstehenden Technologien auch in Kombination miteinander verwendet werden können.

2.2 **Qualität der Einwilligung des Nutzers**

In vielen Fällen ist sich der Nutzer der von bestimmten Objekten ausgeführten Datenverarbeitung möglicherweise nicht bewusst. Dieser Mangel an Information stellt ein großes Hindernis für den Nachweis der Einwilligung nach dem EU-Recht dar, wonach die betroffene Person in Kenntnis der Sachlage sein muss. Unter diesen Umständen kann sich nicht auf die Einwilligung als rechtliche Grundlage für die entsprechende Datenverarbeitung gemäß dem EU-Recht berufen werden.

Tragbare Geräte wie „intelligente“ Uhren sind darüber hinaus nicht erkennbar[5]: Die meisten Menschen können vermutlich eine normale Uhr nicht von einer vernetzten Uhr unterscheiden, wobei letztere Kameras, Mikrofone und Bewegungssensoren enthalten kann, die Daten erfassen und übertragen können, ohne dass die betreffende Person sich dessen bewusst ist oder gar dieser Datenverarbeitung zustimmt. Dies wirft das Problem der Erkennbarkeit der Datenverarbeitung beim „Wearable Computing“ auf, das vielleicht durch die Einführung einer geeigneten Kennzeichnung gelöst werden könnte, die für die betroffene Person sichtbar wäre.

Darüber hinaus ist - zumindest in einigen Fällen - die Möglichkeit auf bestimmte Dienste oder Funktionen eines IoT-Gerätes zu verzichten eher ein theoretisches Konzept als eine echte Alternative. Solche Situationen führen zu der Frage, ob die Einwilligung des Nutzers zu der zugrunde liegenden Datenverarbeitung dann als ohne Zwang erteilt erachtet werden kann und somit nach EU-Recht gültig ist.

Darüber hinaus sind klassische Mechanismen zum Einholen der Einwilligung einer Person im Internet der Dinge möglicherweise schwierig anzuwenden, was zu einer „geringwertigen“ Einwilligung führt, die auf einem Mangel an Informationen beruht oder auf die tatsächliche Unmöglichkeit zurückzuführen ist, eine genau abgestimmte Einwilligung im Einklang mit den vom Nutzer zum Ausdruck gebrachten Vorlieben zu geben. In der Praxis scheinen die mit Sensoren ausgestatteten Endgeräte heute üblicherweise so entwickelt zu werden, dass sie weder selbstständig Informationen noch einen gültigen Mechanismus zur Einholung der Einwilligung der betreffenden natürlichen Person bieten. Jedoch sollten von den Akteuren im Internet der Dinge neue Wege in Betracht gezogen werden, um die Einwilligung des Nutzers einzuholen, beispielsweise indem Einwilligungsmechanismen durch die Geräte selbst eingeführt werden. Konkrete Beispiele wie „Privacy Proxies“ und „Sticky Policies“ werden weiter unten in diesem Dokument behandelt.

2.3 **Rückschlüsse aus den Daten und Wiederverwendung der ursprünglichen Verarbeitung**

Infolge des Wachstums der vom Internet der Dinge erzeugten Datenmengen in Kombination mit den modernen Technologien für Datenanalysen und -abgleiche können diese Daten für sekundäre Zwecke genutzt werden – und zwar unabhängig davon, ob diese Zwecke mit der Zweckbestimmung der ursprünglichen Datenverarbeitung zusammenhängen oder nicht. Dritte, die um Zugang zu den erfassten Daten ersuchen, wollen diese Daten möglicherweise für vollkommen andere Zwecke verwenden.

Scheinbar unbedeutende Daten, die ursprünglich von einem Gerät (wie dem Beschleunigungsmesser und dem Gyroskop eines Smartphones) erhoben wurden, können dann verwendet werden, um auf andere Informationen mit einer vollkommen anderen Bedeutung (wie den Fahrgewohnheiten der betreffenden Person) zu schließen. Diese Möglichkeit, Rückschlüsse aus derartigen „Rohinformationen“ zu ziehen, gilt es bei der Analyse der klassischen Risiken des aus der Informatik bekannten Phänomens der Informationsfusion[6] mit zu berücksichtigen.

[5] Wie in Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten erläutert, stellen sich beim Wearable Computing auch besondere Herausforderungen durch die fortlaufende, über einen längeren Zeitraum erfolgende Erhebung der Daten von sich in der Nähe befindenden Dritten.

[6] Die Informationsfusion umfasst Methoden zur Verknüpfung von aus unterschiedlichen Sensoren oder Informationsquellen stammenden Daten zwecks Gewinnung von neuem, präziserem Wissen über Messwerte und Ereignisse.

Durch „Quantified Self“ wird auch aufgezeigt, wie viele Informationen durch Aggregation und erweiterte Analyse aus Bewegungssensoren erschlossen werden können. Diese Geräte verwenden häufig einfache Sensoren, um Rohdaten (z. B. die Bewegungen der betroffenen Person) zu erfassen und verwenden komplexe Algorithmen für die Gewinnung von diesbezüglichen Informationen (z. B. die Zahl der Schritte) und leiten aus diesen wiederum potenziell sensible Informationen (z.B. über den Gesundheitszustand des Endnutzers) ab, die diesem angezeigt werden.

Solch eine Entwicklung birgt bestimmte Herausforderungen. Tatsächlich war der Nutzer im vorliegenden Fall zwar damit einverstanden, dass die ursprünglichen Informationen für einen bestimmten Zweck veröffentlicht wurden, doch möglicherweise wollte er diese sekundären Informationen, die ja zu vollkommen anderen Zwecken genutzt werden könnten, nicht offenlegen. Daher ist es von großer Bedeutung, dass die Akteure im Internet der Dinge dafür Sorge tragen, dass die Daten auf jeder Ebene (ob roh, extrahiert oder angezeigt) ausschließlich für Zwecke genutzt werden, die mit dem ursprünglichen Zweck der Verarbeitung übereinstimmen, und dem Nutzer sämtliche dieser Zwecke bekannt sind.

2.4 **In die Privatsphäre eingreifende Erstellung von Verhaltensmustern und Profilen**

Obwohl verschiedene Objekte einzelne Informationen getrennt erfassen, können ausreichende Datenmengen, die erhoben und ausgewertet wurden, bestimmte Aspekte von Gewohnheiten, Verhaltensmustern und Vorlieben einer Person offenbaren. Wie oben angeführt, wird die Gewinnung von Erkenntnissen aus unbedeutenden oder gar anonymen Daten durch die zunehmende Verbreitung von Sensoren erleichtert und so umfassende Möglichkeiten für die Profilerstellung schaffen

Darüber hinaus können Analysen von Informationen aus dem Internet der Dinge die Erfassung des genauen und vollständigen Lebens einer Person und ihrer Verhaltensmuster ermöglichen.

In dem gleichen Maße, wie die verstärkte Videoüberwachung das Verhalten der Bürger im öffentlichen Raum beeinflusst hat, dürfte sich dieser Trend auf das Verhalten des Einzelnen auswirken. Über das Internet der Dinge kann diese Form der Überwachung nun selbst die intimste Privatsphäre des Menschen einschließlich seines Zuhauses reichen. Dadurch entsteht ein gewisser Druck, ungewöhnliche Verhaltensweisen zu vermeiden, um zu verhindern, dass Dinge, die als abnorm aufgefasst werden können, entdeckt werden. Eine solche Entwicklung würde stark in das Privat- und Intimleben der Menschen eingreifen und sollte daher genau kontrolliert werden.

2.5 **Eingeschränkte Möglichkeit, bei der Nutzung von Dienstleistungen anonym zu bleiben**

Durch die vollständige Entwicklung der Funktionen des Internet der Dinge könnten die derzeitigen Möglichkeiten für eine anonyme Nutzung dieser Dienstleistungen beschnitten und generell der Möglichkeit, unentdeckt zu bleiben, Grenzen gesetzt werden.

Beispielsweise werden durch tragbare Objekte, die sich nah an der betroffenen Person befinden, weitere Kennungen wie die MAC-Adressen anderer Geräte verfügbar, wodurch ein die Standort-Überwachung der betroffenen Person ermöglichender Fingerabdruck erstellt werden kann. Mit Hilfe mehrerer erfasster MAC-Adressen von mit Sensoren ausgestatteten Geräten lassen sich eindeutige, Fingerabdrücke und stabilere Kennungen erstellen, die die Akteure im Internet der Dinge sodann bestimmten Personen zuordnen können. Diese Fingerabdrücke und Kennungen könnten für eine

Vielzahl von Zwecken verwendet werden, so unter anderem zur Standortanalyse[7] oder zur Analyse der Bewegungsmuster von Menschenmengen oder einzelnen Personen.

Diese Entwicklung sollte zusammen mit der Tatsache betrachtet werden, dass derartige Daten später mit weiteren Daten aus anderen Systemen (z.B. Videoüberwachung oder Internetprotokolle) kombiniert werden können.

Unter diesen Umständen sind einige der Sensordaten besonders anfällig für Angriffe mit dem Ziel unbefugter Rückschlüsse auf die Identität.

Dies zeigt deutlich, dass es immer schwieriger werden wird, im Internet der Dinge anonym zu bleiben und seine Privatsphäre zu schützen. In dieser Beziehung gibt das IoT Anlass zu erheblichen Bedenken in Bezug auf den Datenschutz und den Schutz der Privatsphäre.

2.6 **Sicherheitsrisiken: Sicherheit oder Leistungsfähigkeit**

Das Internet der Dinge birgt im Bereich der Sicherheit viele Herausforderungen: Die Gerätehersteller müssen aufgrund der sicherheits- und ressourcenbezogenen Anforderungen einen ausgewogenen Kompromiss zwischen der erforderlichen Leistungsfähigkeit der Batterien einerseits und der gebotenen technischen Sicherheit der Geräte andererseits finden. Unklar ist bisher insbesondere, wie die Gerätehersteller die Umsetzung der Vertraulichkeits-, Vollständigkeits-, und Verfügbarkeitsmaßnahmen auf allen Ebenen der Datenverarbeitung mit der Notwendigkeit einer optimalen Nutzung von Rechenkapazitäten und Energie durch die Objekte und Sensoren vereinbaren können.

Daher besteht das Risiko, dass Alltagsgegenstände durch das Internet der Dinge zu möglichen Zielen für Angriffe auf die Privatsphäre und die Informationssicherheit werden und dass diese Ziele gleichzeitig weiter verbreitet werden als das Internet in seiner aktuellen Form. Weniger sichere vernetzte Geräte eröffnen wirkungsvolle Angriffsmöglichkeiten (beispielsweise für eine einfach gemachte Überwachung oder für Datenschutzverletzungen), die dazu führen können, dass persönliche Daten gestohlen oder kompromittiert werden, was weitreichende Auswirkungen auf die Verbraucherrechte und auf die Wahrnehmung der Sicherheit im Internet der Dinge durch die betroffenen Personen haben kann.

IoT-Geräte sollen außerdem Daten austauschen und in den Infrastrukturen der Dienstleister speichern. Daher muss bei der Sicherheit des Internet der Dinge nicht nur die Sicherheit der Endgeräte, sondern auch die der Kommunikationsverbindungen, der Speicherinfrastrukturen und sonstiger Eingänge dieses Ökosystems berücksichtigt werden.

Ebenso gewährleistet das Vorhandensein verschiedener Verarbeitungsebenen, die von unterschiedlichen Akteuren entwickelt und umgesetzt werden, keine angemessene Koordinierung zwischen diesen Ebenen und kann somit zu Schwachstellen führen, die ausgenutzt werden können.

Beispielsweise sind die meisten derzeit auf dem Markt erhältlichen Sensoren nicht in der Lage, eine verschlüsselte Kommunikationsverbindung aufzubauen, da die dafür erforderlichen Rechenkapazitäten ihre leistungsschwachen Batterien überfordern würden. Was eine durchgehende Sicherheit anbelangt,

[7] Analyse der Anzahl der sich zu einer bestimmten Zeit an einem bestimmten Standort aufhaltenden Personen und ihrer dortigen Verweildauer.

so kann bei einer Integration von unterschiedlichen Akteuren stammender physischer und logischer Komponenten nur das Sicherheitsniveau der schwächsten Komponente gewährleistet werden.

3. Anwendbarkeit des EU-Rechts auf die Verarbeitung personenbezogener Daten im Internet der Dinge

3.1 Anwendbares Recht

Der geltende Rechtsrahmen für die Beurteilung der vom Internet der Dinge aufgeworfenen Fragen zum Datenschutz und Schutz der Privatsphäre besteht aus der Richtlinie 95/46/EG sowie den einschlägigen Bestimmungen der Richtlinie 2002/58/EG, geändert durch Richtlinie 2009/136/EG.

Dieser Rahmen findet Anwendung, wenn die Bedingungen für die Anwendbarkeit gemäß Artikel 4 der Richtlinie 95/46/EG erfüllt sind. Die Arbeitsgruppe hat in ihrer Stellungnahme 8/2010[8] zum anwendbaren Recht ausführliche Leitlinien zur Auslegung der Bestimmungen von Artikel 4 vorgegeben.

Insbesondere ist gemäß Artikel 4 Absatz 1 Buchstabe a der Richtlinie das einzelstaatliche Recht des Mitgliedstaats auf alle Verarbeitungen personenbezogener Daten anwendbar, „die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden“, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt. Der Begriff „Niederlassung“ im Kontext des internetgestützten Wirtschaftssystems wurde kürzlich ausführlich vom Europäischen Gerichtshof ausgelegt.[9]

Das einzelstaatliche Recht eines Mitgliedstaats ist auch anwendbar, wenn der für die Verarbeitung Verantwortliche nicht im Gebiet der Gemeinschaft niedergelassen ist, aber auf „Mittel“ zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind (Artikel 4 Absatz 1 Buchstabe c). Daher unterliegt ein (an der Entwicklung, dem Vertrieb oder dem Betrieb von IoT-Endgeräten beteiligter) Akteur im Internet der Dinge, der als für die Verarbeitung Verantwortlicher gilt und im Sinne von Artikel 4 Absatz 1 Buchstabe a der Richtlinie 95/46/EG nicht im Gebiet der Gemeinschaft niedergelassen ist, vermutlich dem EU-Recht, wenn er Daten verarbeitet, die durch „Mittel“ von sich in der EU befindenden Nutzern erhoben werden.

Sämtliche Objekte, die zur Erhebung und Weiterverarbeitung der Daten von Personen im Zusammenhang mit der Erbringung von Dienstleistungen im Internet der Dinge verwendet werden, gelten als Mittel im Sinne der Richtlinie. Hierunter fallen selbstverständlich die Geräte selbst (Schrittzähler, „Sleep Tracker“, „vernetzte“ Haushaltsgeräte wie Thermostate, Rauchmelder, vernetzte Brillen oder Uhren usw.), aber auch die Endgeräte der Nutzer (Smartphones oder Tablets), auf denen Software oder Apps installiert wurden, um die Umgebung durch eingebettete Sensoren oder Netzwerkschnittstellen zu überwachen und die von den Geräten erfassten Daten dann an die beteiligten für die Verarbeitung Verantwortlichen zu übermitteln.

Für die Klärung des rechtlichen Status der verschiedenen am Internet der Dinge beteiligten Akteure - und somit auch für die Ermittlung der geltenden Rechtsvorschriften für die von diesen vorgenommene Datenverarbeitung und ihrer Pflichten – ist es von wesentlicher Bedeutung, dass zunächst geklärt wird,

[8] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_de.pdf

[9] Urteil des Gerichtshofes (Große Kammer) vom 13. Mai 2014, Rechtssache C-131/12, Google Spain, ECLI:EU:C:2014:317 (Randnummern 45 bis 60).

welche Rollen diese Akteure innehaben. Wie sich diese Rollen ermitteln lassen, wird im nachfolgenden Abschnitt 3.3 analysiert.

3.2 **Der Begriff „personenbezogene Daten“**

Die Verarbeitung personenbezogener Daten im Sinne von Artikel 2 der Richtlinie 95/46/EG unterliegt dem EU-Recht. Die Arbeitsgruppe hat in ihrer Stellungnahme 4/2007[10] zu dem Begriff „personenbezogene Daten“ ausführliche Leitlinien zu dessen Auslegung vorgegeben.

Im Kontext des Internet der Dinge kann eine Person häufig anhand der von den „Dingen“ erzeugten Daten identifiziert werden. Derartige (beispielsweise durch die zentrale Steuerung von Beleuchtung, Heizung, Lüftung und Klimaanlage erzeugte) Daten können die Erkennung der Lebensmuster einer bestimmten Person oder einer Familie ermöglichen.

Darüber hinaus sind möglicherweise auch personenbezogene Daten, die erst nach Anwendung von Pseudonymisierungs- oder gar Anonymisierungstechniken verarbeitet werden sollen, als personenbezogene Daten zu betrachten. Die große, im Kontext des Internet der Dinge automatisch verarbeitete Datenmenge birgt nämlich das Risiko eines Rückschlusses auf die Identität. An dieser Stelle verweist die Arbeitsgruppe auf die einschlägigen Entwicklungen, die sie in ihrer unlängst veröffentlichten Stellungnahme zu Anonymisierungstechniken[11] beschrieben hat, die die Ermittlung dieser Risiken erleichtern soll und Empfehlungen zur Umsetzung der genannten Techniken enthält.

3.3 **Akteure im Internet der Dinge als für die Verarbeitung Verantwortliche mit Sitz in der EU**

Der Begriff „für die Verarbeitung Verantwortlicher“ und seine Wechselbeziehung mit dem Begriff „Auftragsverarbeiter“ spielen eine wichtige Rolle bei der Anwendung der Richtlinie 95/46/EG, da sie die jeweiligen Pflichten der verschiedenen an der Durchführung der Datenverarbeitung beteiligten Organisationen in Bezug auf die Datenschutzbestimmungen der EU bedingen. Die Akteure können diesbezüglich auf die Stellungnahme 1/2010 der Artikel-29-Arbeitsgruppe zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ [12] zurückgreifen, die Leitlinien für die Anwendung der Begriffe auf komplexe Systeme mit mehreren Akteuren sowie viele Szenarien mit für die Verarbeitung Verantwortlichen und Auftragsverarbeitern enthalten, die allein oder gemeinsam mit anderen handeln und mit einem unterschiedlichen Grad an Autonomie und Verantwortung ausgestattet sind.

Die Verwirklichung des Internet der Dinge impliziert mitunter ein Zusammenwirken mehrerer Komponenten bzw. Akteure wie Gerätehersteller, soziale Plattformen, Anwendungen von Drittanbietern, Geräteverleiher oder -vermieter, Datenvermittler[13] oder Datenplattformen.

---

[10] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf

[11] Stellungnahme 5/2014 zu Anonymisierungstechniken, angenommen am 10. April 2014 (WP 216), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf

[12] Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, angenommen am 16. Februar 2010 (WP 169), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf

[13] Datenvermittler kaufen Daten von Unternehmen, um eine Liste von Personen zu erstellen, die zur gleichen Kategorie oder Gruppe gehören. Diese Kategorien oder Gruppen werden von den Datenvermittlern bestimmt,

Wegen der Komplexität des Netzes der beteiligten Akteure ist es (zwingend) erforderlich, die gesetzlichen Pflichten, denen diese Akteure bezüglich der Verarbeitung personenbezogener Daten unterliegen, entsprechend den Besonderheiten ihrer jeweiligen Eingriffe genau unter ihnen aufzuteilen.

3.3.1 Hersteller von Endgeräten

Hersteller von Endgeräten im Bereich des Internet der Dinge verkaufen nicht ausschließlich physische Objekte an ihre Kunden oder White-Label-Produkte an andere Organisationen. Sie können auch die Betriebssysteme der „Dinge" entwickelt oder modifiziert haben oder Software installiert haben, die deren Gesamtfunktion steuert und unter anderem bestimmt, welche Daten wie oft erhoben und wann und an wen Daten zu welchem Zweck übermittelt werden (z. B. könnten Unternehmen die Kosten für die Versicherung ihrer Mitarbeiter durch die Daten der Tracking-Geräte, die sie diese tragen lassen, beeinflussen[14]). Die meisten Gerätehersteller erheben und verarbeiten die von den Geräten erfassten Daten zu Zwecken, die sie vollständig festgelegt haben, und gelten somit als für die Verarbeitung Verantwortliche im Sinne des EU-Rechts.

3.3.2 Soziale Plattformen

Von der Datenverarbeitung betroffene Personen nutzen vernetzte Objekte eher, wenn sie die Daten öffentlich mit anderen Nutzern teilen können. Insbesondere die Nutzer von „Quantified-Self"-Geräten neigen dazu, Daten in sozialen Netzwerken mit anderen zu teilen, um eine Art positiven Wettbewerb in der Gruppe zu fördern.

Dieses Teilen der durch „Dinge" gesammelten und aggregierten Daten in sozialen Netzwerken erfolgt häufig automatisch, sobald der Nutzer die Anwendung entsprechend eingestellt hat. Häufig ist diese Veröffentlichungsfunktion Teil der vom Hersteller angebotenen Standardeinstellungen der Anwendungen.

Die Zusammenführung dieser Daten auf sozialen Plattformen impliziert, dass für diese nun bestimmte Zuständigkeiten bezüglich des Datenschutzes gelten. Da diese Daten von den Nutzern zu den sozialen Plattformen hochgeladen wurden, gelten letztere, wenn die Daten von ihnen für bestimmte, von ihnen selbst festgelegte Zwecke verarbeitet werden, nach dem EU-Recht als für die Verarbeitung Verantwortliche. So verwendet beispielsweise ein soziales Netzwerk die von einem Schrittzähler gesammelten Informationen, um darauf zu schließen, dass die Nutzerin regelmäßig läuft und zeigt ihr Werbung für Laufschuhe. Die Folgen dieser Einstufung wurden in der Stellungnahme zur Nutzung sozialer Netzwerke der Artikel-29-Datenschutzgruppe[15] aufgezeigt.

3.3.3 Drittanbieter von Anwendungs- und Softwaredienstleistungen

Viele Sensoren verfügen über Programmierschnittstellen (API), um die Entwicklung von Anwendungen zu erleichtern. Um derartige Anwendungen zu nutzen, muss die betroffene Person Anwendungen von Drittanbietern installieren, die diesen den Zugriff auf die vom Gerätehersteller gespeicherten Daten ermöglichen. Bei der Installation dieser Anwendungen muss dem App-Entwickler meist der Zugang zu den Daten über die API gewährt werden.

---

können aber demographische Merkmale, Einkünfte oder das für ein bestimmtes Thema oder Produkt bekundete Interesse widerspiegeln.

[14] Mit derartigen Tracking-Geräten können Arbeitgeber die Gesundheit ihrer Mitarbeiter überwachen, http://www.advisory.com/Daily-Briefing/2013/01/04/With-tracking-devices-employers-may-track-workers-health

[15] Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke (WP 163), angenommen am 12. Juni 2009, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_de.pdf

Einige Anwendungen „belohnen“ die Nutzer bestimmter Objekte: Beispielsweise könnte eine von einer Krankenversicherung entwickelte Anwendung die Nutzer von „Quantified-Self-Objekten“ belohnen oder ein Wohnungsversicherungsunternehmen könnte eine bestimmte Anwendung entwickeln, die gewährleistet, dass die vernetzten Feuermelder der Klienten richtig eingestellt sind. Falls derartige Daten nicht richtig anonymisiert werden, begründet ein solcher Datenzugriff eine Verarbeitung gemäß Artikel 2 der Richtlinie 95/46/EG, so dass der App-Entwickler, der diesen Zugriff auf die Daten eingerichtet hat, als für die Verarbeitung Verantwortlicher im Sinne des EU-Rechts zu betrachten ist.

Derartige Apps werden üblicherweise auf „Opt-In“-Basis installiert. Da der Datenzugriff einer vorherigen Einwilligung unterliegt, muss letztere eindeutig, für den konkreten Fall und in Kenntnis der Sachlage erteilt werden. Die Praxis zeigt jedoch, dass die Genehmigungsanfragen von Drittanbietern von Anwendungen häufig nicht genug Informationen anzeigen, um die Einwilligung des Nutzers tatsächlich als für den konkreten Fall und in Kenntnis der Sachlage und somit als nach EU-Recht wirksam (siehe unten) erscheinen zu lassen..

3.3.4 Sonstige Dritte

Auch andere Dritte als Gerätehersteller und Drittanbieter von Anwendungs- und Softwaredienstleistungen können die Endgeräte des Internet der Dinge nutzen, um Informationen über Personen zu erheben und zu verarbeiten. So möchten vielleicht Krankenversicherungen an ihre Kunden Schrittzähler ausgeben, um zu kontrollieren, wie häufig diese Sport treiben,[16] und die Versicherungsprämien dementsprechend anzupassen.

Im Gegensatz zu den Geräteherstellern haben diese Dritten keine Kontrolle über die vom Objekt gesammelten Daten. Dennoch gelten sie als für deren Verarbeitung Verantwortliche, da sie die von den Geräten erfassten Daten zu bestimmten, von ihnen selbst festgelegten Zwecken erheben und speichern.

Beispiel: Eine Versicherungsgesellschaft startet einen Wettbewerb und bietet Teilnehmern, die niedrigere Prämien zahlen wollen, einen Schrittzähler an. Teilnehmer, die das Angebot annehmen, erhalten einen von der Gesellschaft konfigurierten und registrierten Schrittzähler. Die Teilnehmer haben Zugriff auf die vom Schrittzähler erfassten Daten, aber die Geräte selbst gehören dem Unternehmen „FeelGood“, das ebenfalls Zugang zu den Daten der Teilnehmer hat. In diesem Zusammenhang sind die Teilnehmer als betroffene Personen zu betrachten, und ihnen muss der Zugang zu ihrem Konto für die Schrittzähleranwendung gewährt werden, wohingegen die Versicherungsgesellschaft als für die Verarbeitung Verantwortlicher gilt.

[16] Mit den Tracking-Geräten können Arbeitgeber die Gesundheit ihrer Mitarbeiter überwachen, http://www.advisory.com/Daily-Briefing/2013/01/04/With-tracking-devices-employers-may-track-workers-health

3.3.5 Datenplattformen des Internet der Dinge

Aufgrund mangelnder Standardisierung und Kompatibilität wird das Internet der Dinge auch als „Intranet der Dinge“ betrachtet, in dem jeder Hersteller seine eigenen Schnittstellen und Datenformate festlegt. Die Daten werden dann in geschlossenen Umgebungen gespeichert, die es Nutzern unmöglich machen, ihre Daten von einem Gerät auf ein anderes zu übertragen (oder diese auch nur zusammenzuführen).

Dennoch sind Smartphones und Tablets zur natürlichen Schnittstelle zum Internet für die von zahlreichen Geräten des Internet der Dinge erfassten Daten geworden. Infolgedessen haben Hersteller zunehmend Plattformen entwickelt, die die von unterschiedlichen Geräten gesammelten Daten beherbergen sollen, damit sie zentral und einfacher verwaltet werden können.

Solche Plattformen können auch als für die Verarbeitung Verantwortliche im Sinne des EU-Datenschutzrechts gelten, wenn die Entwicklung solcher Dienste tatsächlich beinhaltet, dass die personenbezogenen Daten der Nutzer für deren eigene Zwecke verwendet werden sollen.

3.4 **Natürliche Personen als betroffene Personen: Teilnehmer, Nutzer, Nicht-Nutzer**

Teilnehmer und generell sämtliche Nutzer des Internet der Dinge gelten als betroffene Personen im Sinne des EU-Rechts. Werden die von ihnen erhobenen und gespeicherten Daten ausschließlich für persönliche oder häusliche Zwecke genutzt, fallen sie unter die „Ausnahmeklausel für Privathaushalte“ der Richtlinie 95/46/EG[17]. Das Geschäftsmodell des Internet der Dinge bedeutet jedoch in der Praxis, dass die Daten der Nutzer systematisch an Gerätehersteller, Anwendungsdienstleister und andere Drittanbieter übermittelt werden, die als für die Verarbeitung Verantwortliche gelten. „Die Ausnahmeklausel für Privathaushalte“ findet daher im Zusammenhang mit dem Internet der Dinge nur begrenzte Anwendung.

Von der Verarbeitung von Daten im IoT können auch Personen betroffen sein, die weder Teilnehmer noch Nutzer des Internet der Dinge sind. So erfassen beispielsweise tragbare Geräte wie „intelligente“ Brillen auch Daten über andere betroffene Personen als den Träger des Geräts. Es ist hervorzuheben, dass dieser Faktor jedoch nicht die Anwendbarkeit des EU-Rechts auf diese Situationen ausschließt. Die Anwendung der Datenschutzbestimmungen der EU wird nicht durch das Eigentum an einem Gerät oder einem Endgerät bedingt, sondern durch die Verarbeitung personenbezogener Daten selbst, und unabhängig davon, wer die von den Daten betroffene Person ist.

4. Pflichten der IoT-Akteure

Akteure des Internet der Dinge, die (allein oder gemeinsam mit anderen) nach dem Unionsrecht als für die Verarbeitung Verantwortliche gelten, müssen die verschiedenen, ihnen in Anwendung der Richtlinie 95/46/EG obliegenden Pflichten und gegebenenfalls die einschlägigen Bestimmungen der Richtlinie 2002/58/EG einhalten. In der vorliegenden Stellungnahme wird ausschließlich auf die Anwendung jener Bestimmungen eingegangen, die in diesem Zusammenhang besonderer Aufmerksamkeit bedürfen, doch dies bedeutet keineswegs, dass die übrigen Bestimmungen nicht zur Anwendung gebracht werden müssen.

[17] Siehe Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, angenommen am 12. Juni 2009 (WP 163).

4.1 Anwendung von Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation

Artikel 5 Absatz 3 der Richtlinie 2002/58/EG ist auf Situationen anwendbar, in denen ein Akteur des Internet der Dinge Informationen speichert oder Zugang zu bereits auf IoT-Geräten gespeicherten Informationen erhält, insofern das Gerät als „Endgerät" im Sinne dieser Bestimmung gilt.[18] Diese Bestimmung schreibt vor, dass der betroffene Teilnehmer oder Nutzer in die Speicherung oder den Zugang einwilligen muss, damit sie als rechtmäßig betrachtet werden kann, sofern sie nicht „unbedingt erforderlich ist, um einen vom Teilnehmer oder Nutzer ausdrücklich gewünschten Dienst der Informationsgesellschaft zur Verfügung zu stellen."[19] Dies ist besonders wichtig, da auch andere Akteure, die weder Nutzer noch Teilnehmer sind, Zugang zu dem betreffenden Endgerät - und damit auch zu darauf gespeicherten Daten, die sensible Informationen privater Natur enthalten – haben können.[20]

Die Einwilligungsanforderung von Artikel 5 Absatz 3 betrifft in erster Linie die Gerätehersteller, aber auch alle Akteure, die auf die in dieser Infrastruktur gespeicherten Rohdaten zugreifen möchten. Sie gilt auch für jeden für die Verarbeitung Verantwortlichen, der weitere Daten auf dem Gerät eines Nutzers speichern möchte.

Unter diesen Umständen müssen die Akteure im Internet der Dinge sicherstellen, dass die betroffene Person nachdem sie von dem für die Verarbeitung Verantwortlichen klare und umfassende Informationen (unter anderem über die Zwecke der Verarbeitung) erhalten hat, ihre Einwilligung zu dieser Speicherung und/oder diesem Zugang erteilt hat.

Daher muss, bevor auf Informationen zugegriffen werden kann, welche verwendet werden können, um den Fingerabdruck eines Gerätes (einschließlich tragbarer Geräte) zu erzeugen, die Einwilligung des Nutzers eingeholt werden, Die Arbeitsgruppe hat bereits in ihrer Arbeitsunterlage 02/2013 (WP 208) Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies oder ähnlicher Tracking-Technologien vorgegeben und wird weitere Leitlinien zu diesem Thema in ihrer kommenden Stellungnahme zum Thema „Device Fingerprinting" (Erfassung des Geräte-Fingerabdrucks) vorstellen.

Beispiel: Ein Schrittzähler erfasst die Zahl der vom Nutzer gemachten Schritte und speichert diese Informationen in seinem internen Speicher. Der Nutzer hat eine Anwendung auf seinem Computer installiert, die die Zahl der Schritte direkt vom Gerät herunterlädt. Will der Gerätehersteller die Daten des Schrittzählers auf seine Server hochladen, muss er die Einwilligung des Nutzers gemäß Artikel 5 Absatz 3 der Richtlinie 2002/58/EG einholen.

Sobald der Hersteller die Daten auf seine Server hochgeladen hat, werden nur die aggregierten Daten über die Zahl der Schritte pro Minute aufbewahrt. Eine Anwendung, die Zugang zu diesen auf den Servern des Geräteherstellers gespeicherten Daten fordert, unterliegt in diesem Fall zwar nicht Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation, aber den Bestimmungen der Richtlinie 95/46/EG zur Rechtmäßigkeit dieser Weiterverarbeitung.

[18] Der Begriff „Endgerät" in Artikel 5 Absatz 3 ist so zu verstehen wie der Begriff „Mittel" in Artikel 4 Absatz 1 Buchstabe c.

[19] Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten (WP 202), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_de.pdf

[20] Vgl. Erwägungsgrund 25 der Richtlinie 2002/58/EG.

Darüber hinaus können der Eigentümer des IoT-Gerätes und die Person, deren Daten überwacht werden (die betroffene Person), verschiedene Personen sein. Dies kann zu einer aufgeteilten Anwendung von Artikel 5 Absatz 3 der Richtlinie 2002/58/EG und der Richtlinie 95/46/EG führen.

Beispiel: Eine Autovermietung installiert in ihren Leihwagen intelligente Fahrzeugortungsgeräte. Während die Autovermietung als Eigentümer des Geräts bzw. als Teilnehmer des Ortungsdienstes betrachtet wird, gilt die das Fahrzeug mietende Person als der Nutzer des Geräts. Artikel 5 Absatz 3 schreibt vor, dass der Gerätehersteller (mindestens) die Einwilligung des Nutzers (d.h. in diesem Fall der das Fahrzeug mietenden Person) einholt. Darüber hinaus unterliegt die Rechtmäßigkeit der Verarbeitung personenbezogener Daten der das Fahrzeug mietenden Person den besonderen Anforderungen von Artikel 7 der Richtlinie 95/46/EG.

4.2 Rechtsgrundlage für die Verarbeitung (Artikel 7 der Richtlinie 95/46/EG)

Akteure im Internet der Dinge, die als für die Verarbeitung Verantwortliche gelten (siehe Abschnitt 4.3), müssen eine der in Artikel 7 der Richtlinie aufgeführten Anforderungen erfüllen, damit die Verarbeitung personenbezogener Daten rechtmäßig ist. Diese Anforderungen gelten für einige Akteure zusätzlich zur Anwendung von Artikel 5 Absatz 3, wenn die Verarbeitung über die Speicherung der oder den Zugang zu den im Endgerät des Nutzers bzw. Teilnehmers gespeicherten Informationen hinausgeht.[21]

Für das Vorgehen in der Praxis sind in diesem Zusammenhang drei Rechtsgrundlagen maßgeblich:

Die Einwilligung (Artikel 7 Buchstabe a) ist die erste Rechtsgrundlage, auf die im Zusammenhang mit dem Internet der Dinge grundsätzlich sowohl durch die Gerätehersteller als auch durch soziale Plattformen oder Datenplattformen, Geräteverleiher oder Drittanbieter von Anwendungs- und Softwaredienstleistungen zurückgegriffen werden sollte. Die Arbeitsgruppe hat ferner Leitlinien zur gleichzeitigen Anwendung der Anforderungen von Artikel 7 Buchstabe a und Artikel 5 Absatz 3 der Richtlinie 2002/58/EG[22] vorgegeben. Die Bedingungen für die Gültigkeit einer derartigen Einwilligung nach dem Unionsrecht waren zudem Gegenstand einer früheren Stellungnahme[23] der Arbeitsgruppe.

Gemäß Artikel 7 Buchstabe b ist die Verarbeitung auch dann zulässig, wenn sie für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich ist. Der Geltungsbereich dieser Rechtsgrundlage ist durch das Kriterium der „Erforderlichkeit“ eingeschränkt, das eine unmittelbare und objektive Verbindung zwischen der Verarbeitung und dem von der betroffenen Person erwarteten Zweck der Vertragserfüllung erfordert.

Drittens lässt Artikel 7 Buchstabe f die Verarbeitung von Daten zu, wenn sie zur Verwirklichung des berechtigten Interesses erforderlich ist, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, dem bzw. denen die Daten übermittelt werden, sofern

[21] Zur Formulierung von Artikel 5 Absatz 3 und Artikel 7 Buchstabe a siehe insbesondere die Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten, angenommen am 27. Februar 2013 (WP 202), (S. 14 ff.) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_de.pdf und Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/E (WP 217) – (S. 26, 32, 46).

[22] Stellungnahme WP 202, S. 14 ff.

[23] Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011 (WP187), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf

nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, insbesondere der Schutz der Privatsphäre, bei der Verarbeitung personenbezogener Daten, die gemäß Artikel 1 Absatz 1 geschützt sind, überwiegen.

In seinem Urteil in der Rechtssache *Google Spain*[24] hat der Europäische Gerichtshof grundlegende Leitlinien für die Auslegung dieser Bestimmung vorgegeben, die die von ihm bereits in den verbundenen Rechtssachen ASNEF und FECEMD (C-468/10 und C-469/10) vorgegebenen Leitlinien ergänzen. Im Zusammenhang mit dem Internet der Dinge berührt die Verarbeitung der personenbezogenen Daten einer natürlichen Person in Situationen, in denen Daten ohne IoT-Geräte nicht oder nur sehr schwer miteinander hätten verknüpft werden können, sehr wahrscheinlich deren Grundrechte auf Privatsphäre und auf den Schutz personenbezogener Daten. Diese Situationen können auftreten, wenn die erhobenen Daten die Gesundheit, die Wohnung oder die Intimsphäre, den Standort sowie viele weitere Aspekte des Privatlebens einer Person betreffen. Wegen seiner potenziellen Schwere kann ein solcher Eingriff nicht allein mit dem wirtschaftlichen Interesse eines Akteurs im IoT an der Verarbeitung der Daten gerechtfertigt werden. Weitere Interessen, die von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen werden, müssen zum Tragen kommen.[25]

Beispiel: Im Rahmen eines Plans zur Förderung öffentlicher Verkehrsmittel und zur Verringerung der Umweltverschmutzung will der Stadtrat das Parken im Stadtzentrum durch Zugangsbeschränkungen und Parkgebühren regulieren. Die Höhe der Gebühr wird dabei von mehreren Parametern wie Motortyp (Diesel, Benzin, Elektro) und Alter des Fahrzeugs abhängig gemacht. Sobald ein Fahrzeug sich einem freien Parkplatz nähert, kann ein Sensor das Nummernschild erfassen und, nach Abgleich mit der Datenbank, den gemäß den vorher festgelegten Kriterien automatisch anzusetzenden Aufpreis oder Nachlass errechnen. In diesem Fall kann die Verarbeitung der Informationen des Nummernschildes zur Bestimmung der Gebühr das berechtigte Interesse des für die Verarbeitung Verantwortlichen erfüllen. Die Weiterverarbeitung (beispielsweise in Form der Erfassung) - nicht-anonymisierter - Informationen über Fahrzeugbewegungen durch das der Beschränkung unterliegende Gebiet, hingegen würde die Anwendung anderer Rechtsgrundlagen erfordern.

4.3 **Grundsätze der Datenqualität**

Gemeinsam stellen die in Artikel 6 der Richtlinie 95/46/EG verankerten Grundsätze einen Eckstein des Datenschutzrechts der EU dar.

Personenbezogene Daten sollten nach Treu und Glauben und auf rechtmäßige Weise erhoben und verarbeitet werden. Das Prinzip von Treu und Glauben erfordert insbesondere, dass personenbezogene Daten niemals erhoben und verarbeitet werden, ohne dass die betroffene Person Kenntnis davon hat. Diese Bestimmung ist in Bezug auf das Internet der Dinge umso bedeutsamer, als die Sensoren so entwickelt wurden, dass sie unauffällig (d.h. so unsichtbar wie möglich) sind. Dennoch müssen für die Verarbeitung Verantwortliche im IoT (also in erster Linie die Gerätehersteller) alle Personen in der geografischen oder digitalen Nähe vernetzter Geräte informieren, wenn Daten über sie oder ihr Umfeld erfasst werden. Die Einhaltung dieser Bestimmung geht über eine strenge rechtliche Anforderung hinaus: Eine Erhebung nach Treu und Glauben ist eine der wichtigsten Erwartungen der Nutzer an das IoT und insbesondere an das „Wearable Computing“.

[24] Urteil des Gerichtshofes (Große Kammer) vom 13. Mai 2014, Google Spain, Rechtssache C-131/12, ECLI:EU:C:2014:317 (Randnummer 74 ff.).
[25] Stellungnahme WP 217.

Beispiel: Ein Gesundheitsgerät nutzt eine kleine Leuchte, um zu kontrollieren, wie das Blut in den Venen fließt und daraus Informationen zum Herzschlag abzuleiten. Das Gerät enthält einen weiteren Sensor, der den Sauerstoffgehalt im Blut misst, jedoch werden die diesbezüglichen Daten weder auf dem Gerät selbst noch auf der Anwenderschnittstelle angezeigt. Selbst wenn der Sauerstoffsensor voll funktionsfähig ist, sollte er ohne vorherige Inkenntnissetzung des Nutzers nicht aktiviert werden. Zur Aktivierung dieses Sensors ist die ausdrückliche Einwilligung des Nutzers erforderlich.

Der Grundsatz der Zweckbindung bedeutet, dass Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden dürfen. Eine Weiterverarbeitung, die nicht in einer mit diesen ursprünglichen Zweckbestimmungen zu vereinbarenden Weise erfolgt, wäre nach EU-Recht rechtswidrig. Dieser Grundsatz soll es den Nutzern ermöglichen, zu wissen, wie und für welche Zwecke ihre Daten genutzt werden, und zu entscheiden, ob sie einem für die Verarbeitung Verantwortlichen ihre Daten anvertrauen. Diese Zwecke müssen *vor* der Verarbeitung der Daten bestimmt werden, wodurch plötzliche Änderungen in den wichtigen Bedingungen der Verarbeitung ausgeschlossen werden. Dies bedeutet, dass IoT-Akteure einen guten Überblick über ihr Geschäftsmodell haben sollten, bevor sie beginnen, personenbezogene Daten zu erheben.

Darüber hinaus sollten die über die betroffene Person erhobenen Daten unbedingt für den im Vorfeld von dem für die Verarbeitung Verantwortlichen festgelegten spezifischen Zweck erforderlich sein („Grundsatz der Datenminimierung"). Für diesen Zweck nicht notwendige Daten sollten nicht „für alle Fälle" oder weil „sie später nützlich sein könnten" erfasst und gespeichert werden. Einige Akteure sind der Auffassung, dass der Grundsatz der Datenminimierung die Möglichkeiten des Internet der Dinge einschränken und somit ein Hindernis für Innovationen darstellen könnte, da die Datenverarbeitung in Form einer explorativen Analyse zur Erkennung nicht-offensichtlicher Zusammenhänge und Entwicklungen potenzielle Vorteile berge. Die Arbeitsgruppe kann diesen Standpunkt nicht nachvollziehen und unterstreicht erneut, dass der Grundsatz der Datenminimierung eine wesentliche Rolle beim Schutz der Datenschutzrechte, die dem Einzelnen durch das EU-Recht gewährt werden, spielt und als solcher gewahrt werden sollte.[26] Dieser Grundsatz bedeutet insbesondere, dass wenn personenbezogene Daten nicht für die Erbringung einer bestimmten Dienstleistung im Internet der Dinge erforderlich sind, der betroffenen Person zumindest die Möglichkeit geboten werden sollte, diese Dienstleitung anonym zu nutzen.

Artikel 6 besagt weiterhin, dass im Zusammenhang mit dem Internet der Dinge erfasste und verarbeitete personenbezogene Daten nicht länger aufbewahrt werden dürfen, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist. Die Prüfung der Erforderlichkeit muss durch jeden der Akteure bei der Erbringung einer spezifischen Dienstleistung im IoT ausgeführt werden, da die Zwecke ihrer jeweiligen Verarbeitung tatsächlich unterschiedlich sein können. So sollten beispielsweise personenbezogene Daten, die von einem Nutzer übermittelt werden, wenn er an einem bestimmten Dienst im Internet der Dinge teilnimmt, sofort gelöscht werden, wenn dieser die Teilnahme beendet. Gleichermaßen sollten Informationen, die der Nutzer in seinem Konto löscht, nicht gespeichert bleiben. Nutzt der Nutzer den Dienst oder die

[26] In der Praxis erfolgt die Sondierungsforschung jedoch niemals völlig zufällig: Der allgemeine Zweck jeder Forschung ist, zumindest teilweise, traditionell vorgegeben, wenn auch nur aus organisatorischen und finanziellen Gründen. Es ist schwer vorstellbar, dass die Datenverarbeitung für bestimmte Forschungen mit dem ursprünglichen Zweck der Datenerhebung vereinbar ist und somit gegen EU-Recht verstößt.

Anwendung über eine bestimmte Zeit nicht, sollte sein Profil in einen inaktiven Zustand versetzt werden. Nach einer weiteren Zeitspanne sollten die Daten gelöscht werden. Bevor diese Maßnahmen ergriffen werden, sollte der Nutzer mit allen dem entsprechenden Akteur zur Verfügung stehenden Mitteln darüber informiert werden.

4.4 **Verarbeitung sensibler Daten (Artikel 8)**

Anwendungen im Internet der Dinge können personenbezogene Daten verarbeiten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über die Gesundheit oder das Sexualleben, die als „sensible Daten" gelten und gemäß Artikel 8 der Richtlinie 95/46/EG besonders geschützt werden müssen. In der Praxis erfordert die Anwendung von Artikel 8 auf sensible Daten im Internet der Dinge, dass für die Verarbeitung Verantwortliche die ausdrückliche Einwilligung des Nutzers einholen, sofern dieser die Daten nicht selbst veröffentlicht hat.

Eine solche Situation tritt wahrscheinlich in spezifischen Kontexten wie den „Quantified-Self"-Geräten auf. Dabei erfassen die Geräte zumeist Daten über das Wohlbefinden der betroffenen Person. Diese Daten stellen nicht notwendigerweise gesundheitsbezogene Daten als solche dar, können aber schnell Informationen zur Gesundheit der betroffenen Person liefern, da sie regelmäßig aufgezeichnet werden und somit Schlussfolgerungen aus den innerhalb eines bestimmten Zeitraums aufgetretenen Schwankungen ermöglichen. Für die Verarbeitung Verantwortliche sollte eine solche potenzielle Änderung der Datenkategorie vorhersehen und entsprechende Maßnahmen ergreifen.

Beispiel: Das Unternehmen X hat eine Anwendung entwickelt, die durch die Analyse der Rohdaten von Elektrokardiogramm-Signalen, die von handelsüblichen, für den Verbraucher allgemein erhältlichen Sensoren erzeugt werden, Muster für eine vorliegende Drogensucht erkennen kann. Die Anwendungsplattform kann bestimmte Merkmale aus den EKG-Rohdaten extrahieren, die laut den Ergebnisse früherer Untersuchungen mit dem Konsum von Drogen verbunden sind. Das Produkt, das mit den meisten auf dem Markt erhältlichen Sensoren kompatibel ist, könnte als eigenständige Anwendung oder auch über eine Internetschnittstelle, die das Hochladen der Daten erfordert, genutzt werden. Für die Verarbeitung der Daten zu diesem Zweck sollte die ausdrückliche Einwilligung des Nutzers eingeholt werden. Die Erfüllung dieser Pflicht zur Einholung einer Einwilligung kann unter den gleichen Bedingungen und gleichzeitig mit der Einholung der Einwilligung der betroffenen Person gemäß Artikel 7 Buchstabe a erfolgen.

4.5 **Transparenzanforderungen (Artikel 10 und 11)**

Über die Anforderungen von Artikel 6 Buchstabe a zur Erhebung der Daten nach Treu und Glauben hinaus müssen für die Verarbeitung Verantwortliche in Anwendung von Artikel 10 und 11 den betroffenen Personen spezifische Informationen mitteilen: die Identität des für die Verarbeitung Verantwortlichen, die Zweckbestimmungen der Verarbeitung, die Empfänger der Daten und das Bestehen von Auskunfts- und Berichtigungsrechten (einschließlich Informationen darüber, wie die Verbindung des Objekts getrennt werden kann, um die Offenlegung weiterer Daten zu verhindern).

Abhängig von den Anwendungen können diese Informationen beispielsweise unter Verwendung der drahtlosen Verbindung auf das Objekt selbst übertragen werden, oder indem sich in der Nähe von Sensoren befindende Nutzer durch Näherungstests, die von einem zentralen Server ausgeführt werden und die Privatsphäre wahren sollen, darüber informiert werden.

Diese Informationen müssen darüber hinaus in Übereinstimmung mit dem Grundsatz der Verarbeitung nach Treu und Glauben deutlich und verständlich sein. Beispielsweise könnte der Gerätehersteller auf mit Sensoren ausgestattete Objekte einen QR-Code oder Flashcode aufdrucken, der Aufschluss über den Typ des Sensors und die von ihm erfassten Informationen sowie über die Zweckbestimmung der Datenerhebung gibt.

4.6 **Sicherheit (Artikel 17)**

Artikel 17 der Datenschutzrichtlinie sieht vor, dass der für die Verarbeitung Verantwortliche „*die geeigneten technischen und organisatorischen Maßnahmen durchführen muss, die für den Schutz [...] personenbezogener Daten erforderlich sind*", und dass „*der für die Verarbeitung Verantwortliche im Fall einer Verarbeitung in seinem Auftrag einen Auftragsverarbeiter auszuwählen hat, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bietet.*"

Demnach bleibt jeder als für die Verarbeitung Verantwortlicher geltende Akteur vollständig für die Sicherheit der Datenverarbeitung verantwortlich. Wenn durch ungeeignete Konstruktion oder Wartung der verwendeten Geräte verursachte Sicherheitsmängel zum Verstoß gegen den Grundsatz der Sicherheit führen, ist der für die Verarbeitung Verantwortliche haftbar. In diesem Sinne ist es erforderlich, dass die für die Verarbeitung Verantwortlichen Sicherheitsbewertungen der Systeme als Einheit - auch auf Ebene der Komponenten - unter Anwendung der Grundsätze der „komponierbaren Sicherheit" ausführen. Gleichermaßen müssen für die betreffenden Geräte Zertifizierungen angewendet und Anpassungen an international anerkannte Sicherheitsstandards vorgenommen werden, um die Gesamtsicherheit des IoT-Ökosystems zu verbessern.

Unterauftragnehmer, die Hardwarekomponenten im Auftrag anderer Akteure entwickeln und herstellen, ohne dabei personenbezogene Daten zu verarbeiten, können, streng genommen, nicht gemäß Artikel 17 der Richtlinie 95/46/EG für etwaige durch Sicherheitsmängel dieser Geräte auftretende Verstöße gegen den Datenschutz zur Verantwortung gezogen werden. Dennoch spielen sie eine wichtige Rolle bei der Aufrechterhaltung der Sicherheit des IoT-Ökosystems. Akteure, die gegenüber betroffenen Personen unmittelbar für den Datenschutz verantwortlich sind, sollten sicherstellen, dass diese Unterauftragnehmer bei der Entwicklung und Herstellung ihrer Produkte in Bezug auf den Schutz der Privatsphäre an hohe Sicherheitsstandards gebunden sind.

Wie bereits erwähnt, müssen die Sicherheitsmaßnahmen unter Berücksichtigung der spezifischen operativen Einschränkungen der IoT-Geräte umgesetzt werden. So können die meisten Sensoren bisher keine verschlüsselte Verbindung aufbauen, da der physischen Autonomie des Gerätes oder der Kostenkontrolle Vorrang eingeräumt wird.

Darüber hinaus können Geräte, die im Internet der Dinge betrieben werden, sowohl aus technischen als auch aus wirtschaftlichen Gründen nur schwer gesichert werden. Da ihre Komponenten drahtlose Kommunikationsinfrastrukturen nutzen und durch eingeschränkte Ressourcen in Bezug auf Energie und Rechenleistung gekennzeichnet sind, sind die Geräte anfällig für physische Angriffe, Lauschangriffe oder Angriffe auf Proxy-Server. Die derzeit am häufigsten genutzten Technologien (z. B. PKI-Infrastrukturen), können nicht ohne Weiteres auf IoT-Geräte übertragen werden, da die meisten Geräte nicht die für die Verarbeitungsaufgaben erforderliche Rechenleistung besitzen. Das IoT umfasst eine komplexe Lieferkette mit mehreren Akteuren, die unterschiedliche Grade von Verantwortung tragen. Ein etwaiger Sicherheitsverstoß kann seinen Ursprung bei jedem von ihnen haben, insbesondere wenn man die Maschine-zu-Maschine-Umgebungen berücksichtigt, die auf dem

Austausch von Daten zwischen Geräten basieren. Daher sollte der Notwendigkeit Rechnung getragen werden, sichere und „schlanke“ Protokolle zu verwenden, die sich für Umgebungen mit geringen Ressourcen eignen.

In einem solchen Kontext, in dem geringe Rechenkapazitäten eine sichere und effiziente Kommunikation in Frage stellen können, ist es nach Auffassung der Artikel-29-Arbeitsgruppe umso wichtiger, den Grundsatz der Datenminimierung einzuhalten und die Verarbeitung personenbezogener Daten (und insbesondere deren Speicherung auf dem betreffenden Gerät) auf das erforderliche Minimum zu reduzieren.

Des Weiteren werden Geräte, die so konzipiert sind, dass sie direkt über das Internet zugänglich sind, nicht immer vom Nutzer selbst konfiguriert. Wenn Geräte dieser Art mit den Standardeinstellungen betrieben werden, können Eindringlinge problemlos Zugang zu ihnen erlangen. Sicherheitspraktiken, die auf Netzwerkeinschränkungen, der standardmäßigen Deaktivierung unwichtiger Funktionen und der Verhinderung von aus nicht vertrauenswürdigen Quellen stammenden Software-Updates (und somit der Eingrenzung der Gefahr potenzieller Schadsoftware-Angriffe durch Quellcodeveränderungen) beruhen, können dazu beitragen, die Auswirkungen und den Umfang möglicher Datenschutzverletzungen einzugrenzen. Solche Sicherheitsmaßnahmen zum Schutz der Privatsphäre sollten daher in Anwendung des Grundsatzes eines „eingebauten Datenschutzes“ von Beginn an vorgesehen werden.

Darüber hinaus führt das Fehlen automatischer Aktualisierungen zu häufig nicht gepatchten Sicherheitslücken, die durch spezielle Suchmaschinen leicht entdeckt werden können. Selbst in den Fällen, in denen sich die Nutzer der sich auf ihre eigenen Geräte auswirkenden Sicherheitslücken bewusst sind, kann es sein, dass sie keinen Zugang zu den Aktualisierungen des Anbieters haben, sei es aufgrund von Hardware-Einschränkungen oder aber aufgrund veralteter Technologie, die verhindert, dass das betreffende Gerät Software-Aktualisierungen unterstützt. Wenn ein Hersteller den Support für ein Gerät einstellt, sollten alternative Supportlösungen angeboten werden (z. B. die Öffnung der Software für die Open-Source-Gemeinschaft). Die Nutzer müssen darüber informiert werden, dass ihre Geräte wahrscheinlich anfällig für nicht beseitigte Sicherheitslücken sind.

Einige auf dem Markt erhältliche „Self-Tracker“-Systeme (Schrittzähler, „Sleep-Tracker“) haben zudem Sicherheitslücken, die es Angreifern ermöglichen, an die Anwendungen und Gerätehersteller übermittelte Beobachtungswerte zu manipulieren. Es ist unerlässlich, dass diese Geräte einen geeigneten Schutz gegen Datenmanipulationen bieten, insbesondere wenn die von diesen Sensoren übermittelten Werte indirekt die gesundheitsbezogenen Entscheidungen der Nutzer beeinflussen.

Nicht zuletzt sei darauf hingewiesen, dass auch eine geeignete Informationspolitik in Bezug auf Datenschutzverletzungen durch die Verbreitung von Fachwissen und Leitlinien dabei helfen kann, die negativen Auswirkungen etwaiger Software- und Konzeptionsschwachstellen einzugrenzen.

5. Rechte der betroffenen Person

Akteure des Internet der Dinge müssen die Rechte der betroffenen Personen im Einklang mit den Bestimmungen der Artikel 12 und 14 der Richtlinie 95/46/EG beachten und entsprechende organisatorische Maßnahmen ergreifen. Diese Rechte sind nicht auf Teilnehmer von IoT-Diensten oder Gerätebesitzer beschränkt und betreffen alle Personen, deren personenbezogenen Daten verarbeitet werden.

5.1 **Auskunftsrecht**

Artikel 12 Buchstabe a besagt, dass betroffene Personen berechtigt sind, von dem für die Verarbeitung Verantwortlichen eine Mitteilung in verständlicher Form über die Daten, die Gegenstand der Verarbeitung sind, sowie die verfügbaren Informationen über die Herkunft der Daten zu erhalten.

In der Praxis sind die Nutzer des IoT meist an spezifische Systeme gebunden. Die Geräte senden die Daten zunächst an den Gerätehersteller, der diese dann dem Nutzer über ein Internetportal oder eine App zugänglich macht. Dies ermöglicht den Herstellern, Online-Dienste bereitzustellen, die die Leistungsfähigkeit der Geräte unterstützen, aber es kann auch verhindern, dass die Nutzer den mit ihrem Gerät interagierenden Dienst frei wählen können.

Darüber hinaus haben Endnutzer selten Zugang zu den von den IoT-Geräten gesammelten Rohdaten. Sie haben eindeutig ein größeres Interesse an den ausgewerteten Daten als an den Rohdaten, die für Sie eventuell keinen Sinn ergeben. Dennoch können solche Daten für den Endnutzer nützlich sein, wenn es darum geht, zu verstehen, was der Gerätehersteller aus diesen Daten über ihn ableiten kann. Außerdem kann der Endnutzer, wenn er Zugriff auf diese Rohdaten hat, die Daten an einen anderen für die Verarbeitung Verantwortlichen übermitteln und den Dienstanbieter wechseln (beispielsweise wenn der ursprüngliche Verantwortliche seine Datenschutzbestimmungen so ändert, dass der Endnutzer darüber unzufrieden ist). Bisher haben die Menschen in derartigen Fällen praktisch keine andere Möglichkeit, als die Nutzung der Geräte zu beenden, da die meisten Hersteller keine solche Funktion anbieten und lediglich Zugang zu eingeschränkten Darstellungen der gespeicherten Rohdaten bieten.

Die Artikel-29-Arbeitsgruppe ist der Auffassung, dass eine solche Haltung die wirksame Ausübung des den betroffenen Personen durch Artikel 12 Buchstabe a der Richtlinie 95/46/EG zugesicherten Auskunftsrechts verhindert. Sie ist zudem der Ansicht, dass die Akteure des Internet der Dinge vielmehr Maßnahmen ergreifen sollten, die es den Nutzern ermöglichen, dieses Recht wirksam durchzusetzen und einen anderen, möglicherweise nicht vom selben Gerätehersteller angebotenen Dienst zu wählen. Es wäre sinnvoll, die bestehenden Standards für den Datenaustausch in diese Richtung weiterzuentwickeln.

Diese Maßnahmen wären umso wichtiger, als das „Recht auf Datenübertragbarkeit“, das durch den Vorschlag für eine Datenschutz-Grundverordnung als eine Abwandlung des Auskunftsrechts eingeführt werden dürfte, darauf abzielt, jedwede „Bindung“ der Nutzer eindeutig zu beenden.[27] Ziel des EU-Gesetzgebers ist es, Wettbewerbshindernisse abzubauen und neue Akteure dabei zu unterstützen, auf diesem Markt Neuerungen einzuführen.

5.2 **Möglichkeit zur Widerrufung der Einwilligung und zum Widerspruch gegen die Datenverarbeitung**

Betroffene Personen müssen die Möglichkeit haben, ihre für eine spezifische Verarbeitung erteilte Einwilligung zu widerrufen und gegen die Verarbeitung der sie betreffenden Daten Widerspruch einzulegen. Die Ausübung dieser Rechte muss ohne technische oder organisatorische Einschränkungen oder Behinderungen möglich sein, und die zur Erfassung des Widerrufs bereitgestellten Werkzeuge müssen zugänglich, sichtbar und effizient sein.

Die Widerrufsverfahren sollten feingliedrig sein und folgendes abdecken: (1) alle von einem bestimmen Objekt erhobenen Daten (Beispiel: die Forderung, dass eine gegebene Wetterstation keine

[27] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf

Daten mehr über Luftfeuchtigkeit, Temperatur und Geräusche erhebt), (2) einen spezifischen Datentyp, der von einem beliebigen Objekt gesammelt wird (ein Nutzer sollte beispielsweise die Erhebung von Daten durch ein Geräusche erfassendes Gerät – sei es ein „Sleep-Tracker“ oder eine Wetterstation – jederzeit beenden können) und, (3) eine bestimmte Datenverarbeitung (der Nutzer soll beispielsweise verlangen können, dass sowohl sein Schrittzähler als auch seine Uhr seine Schritte nicht weiter zählen).

Da es wahrscheinlich ist, dass tragbare „vernetzte Dinge“ vorhandene Objekte mit üblichen Funktionen ersetzen werden, sollten für die Verarbeitung Verantwortliche die Möglichkeit anbieten, die „Vernetzt“-Funktion solcher Objekte (wie „intelligente“ Uhren oder Brillen) abzuschalten, damit diese wie das ursprüngliche, unvernetzte Gerät funktionieren. Die Arbeitsgruppe hat sich bereits dafür ausgesprochen, dass betroffene Personen ihre „Einwilligung jederzeit zurückziehen können“ sollten, ohne hierfür den Dienst „verlassen zu müssen.“[28]

Beispiel: Ein Nutzer installiert in seiner Wohnung einen vernetzten Brandmelder. Dieser enthält einen Anwesenheitssensor, einen Hitzesensor, einen Ultraschallsensor und einen Lichtsensor. Einige der Sensoren sind zum Erkennen eines Brandes notwendig, während andere nur zusätzliche Funktionen bieten, über die er im Voraus informiert wurde. Der Nutzer sollte die Möglichkeit haben, diese zusätzlichen Funktionen (d.h. die betreffenden Sensoren) abzuschalten und nur den Brandmelder zu nutzen.

Interessanterweise stellen einige aktuelle Entwicklungen in diesem Bereich darauf ab, betroffenen Personen - beispielsweise im Rahmen von „Sticky Policies“[29] oder „Privacy Proxies“[30] - größere Kontrolle über die Funktionen des Einwilligungsmanagement zu geben.

6. Schlussfolgerungen und Empfehlungen

Nachfolgend sind einige Empfehlungen aufgeführt, die nach Auffassung der Artikel-29-Datenschutzgruppe die Anwendung der genannten gesetzlichen Anforderungen der EU auf das Internet der Dinge erleichtern können.

Die nachfolgenden Empfehlungen stellen lediglich Leitlinien dar, die die bisher von der Artikel-29-Datenschutzgruppe angenommenen Dokumente ergänzen sollen.

[28] Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten, angenommen am 16. Mai 2011 (WP 185), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_de.pdf

[29] In dieser Hinsicht kann das Konzept der sogenannten Sticky Policies die Einhaltung des Datenschutzrahmens unterstützen, indem Informationen zu Bedingungen und Beschränkungen der Datennutzung in die Daten selbst eingebunden werden. Mittels Sticky Policies könnten folglich der Kontext der Datennutzung, ihr Zweck, die Regeln für den Zugang Dritter und eine Liste vertrauensvoller Nutzer festgelegt werden.

[30] Der Rückgriff auf Privacy Proxies wäre eine Möglichkeit, den betroffenen Personen echte Kontrolle darüber zu verschaffen, wie die Daten beim Austausch mit den Sensoren verarbeitet werden müssen, indem diesen Personen ermöglicht wird, Präferenzen zu äußern (auch in Bezug auf den Erhalt und den Widerruf von Einwilligungen sowie auf Wahlmöglichkeiten bezüglich der Zweckbindung). Von einem Gerät ausgehende Datenanfragen müssten so nach Maßgabe vorab festgelegter Richtlinien bearbeitet werden, die den Zugang zu den Daten unter der Kontrolle des Nutzers regeln. Durch eine solche Kopplung von Sensoren und Richtlinien könnten Anträge Dritter auf Erhebung von, Sensordaten oder auf Zugang zu diesen entweder genehmigt, eingeschränkt oder ohne Weiteres abgelehnt werden.

Diesbezüglich möchte die Arbeitsgruppe besonders auf ihre früheren Empfehlungen zu Apps auf intelligenten Endgeräten[31] hinweisen. Da Smartphones Bestandteil des Umfelds des Internet der Dinge sind und an beiden Ökosystemen eine vergleichbare Gruppe von Akteuren beteiligt ist, betreffen diese Empfehlungen direkt das IoT. Insbesondere sollten App-Entwickler und Gerätehersteller den Endnutzern ein angemessenes Informationsniveau, einfache „Opt-Out"-Möglichkeiten und/oder gegebenenfalls die Möglichkeit einer differenzierten Einwilligung bieten. Darüber hinaus sollte der für die Verarbeitung Verantwortliche, sofern keine Einwilligung eingeholt wurde, die Daten vor der Wiederverwendung oder der Weitergabe an Dritte anonymisieren.

6.1 **Empfehlungen für alle Akteure**

- Vor der Einführung etwaiger neuer Anwendungen im Internet der Dinge sollten Datenschutzfolgenabschätzungen durchgeführt werden. Die dabei zu befolgende Methodik kann auf dem Rahmen für Datenschutzfolgenabschätzungen aufbauen, den die Artikel-29-Datenschutzgruppe am 12. Januar 2011 für RFID-gestützte Anwendungen angenommen hat.[32] Sofern angemessen bzw. durchführbar, sollten die Akteure in Betracht ziehen, die einschlägigen Datenschutzfolgenabschätzungen der breiten Öffentlichkeit zugänglich zu machen. Für bestimmte IoT-Ökosysteme (z. B. „intelligente" Städte) könnten spezielle Rahmen für die Datenschutzfolgenabschätzungen ausgearbeitet werden.

- Viele IoT-Akteure benötigen lediglich aggregierte Daten und haben keinen Bedarf für die von IoT-Geräten gesammelten Rohdaten. Sie müssen die Rohdaten direkt nach der Extraktion der für ihre Datenverarbeitung erforderlichen Daten löschen. Grundsätzlich sollte die Löschung zum nächstmöglichen Zeitpunkt nach der Erhebung der Rohdaten (z. B. auf dem Gerät nach der Verarbeitung) erfolgen.

- Jeder IoT-Akteur sollte die Grundsätze des eingebauten Datenschutzes und der datenschutzfreundlichen Grundeinstellung anwenden.

- Im Kontext des Internet der Dinge ist die Befähigung der Nutzer von grundlegender Bedeutung. Betroffene Personen und Nutzer müssen in der Lage sein, ihre Rechte auszuüben und somit gemäß dem Grundsatz der Selbstbestimmung über Daten jederzeit die „Kontrolle" über ihre Daten haben.

- Die Methoden für die Auskunftserteilung, für die Belehrung über das Recht auf Widerspruch gegen die Datenverarbeitung und für die Einholung der Einwilligung sollten so nutzerfreundlich wie möglich gestaltet werden. Insbesondere die Verfahren für die Auskunftserteilung und die Einholung der Einwilligung müssen auf Informationen ausgerichtet werden, die für den Nutzer verständlich sind und nicht auf allgemeine Datenschutzbestimmungen auf der Webseite des für die Verarbeitung Verantwortlichen beschränkt sein sollten.

- Endgeräte und Anwendungen sollten so konzipiert werden, dass sie den Nutzern und betroffenen Personen, die keine Nutzer sind, beispielsweise über die physische Schnittstelle des Gerätes oder per Signalübertragung auf einem Funkkanal Informationen geben.

---

[31] Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten (WP 202), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_de.pdf

[32] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf

6.2 **Hersteller von Betriebssystemen und Endgeräten**

- Hersteller von Endgeräten müssen die Nutzer über die Art der von den Sensoren erhobenen und weiterverarbeiteten Daten, über die Art der an sie übermittelten Daten und über deren Verarbeitung und Zusammenführung informieren.

- Die Gerätehersteller sollten in der Lage sein, alle anderen beteiligten Akteure zu informieren, sobald eine betroffene Person ihre Einwilligung widerruft oder der Datenverarbeitung widerspricht.

- Die Gerätehersteller müssen bei der Gewährung des Zugangs zu Anwendungen differenzierte Wahlmöglichkeiten bieten. Diese Differenziertheit sollte nicht nur in Bezug auf die Kategorie der erhobenen Daten bestehen, sondern auch in Bezug auf den Zeitpunkt und die Häufigkeit der Datenerhebung. Ähnlich der „Bitte nicht stören"-Funktion von Smartphones sollten IoT-Geräte über eine „Bitte nicht erheben"-Funktion verfügen, mit der die Tätigkeit der Sensoren zeitlich programmiert oder letztere schnell deaktiviert werden können.

- Um die Standortbestimmung zu verhindern, sollten die Gerätehersteller die Erfassung des Geräte-Fingerabdrucks einschränken, indem sie vorsehen, dass drahtlose Schnittstellen abgeschaltet werden, sobald sie nicht verwendet werden, oder dass zufällige Identifikatoren (wie zufällige MAC-Adressen bei der Suche nach Wi-Fi-Netzen) verwendet werden und somit keine ständige Kennung für eine Standortbestimmung genutzt werden kann.

- Um die Transparenz und die von den Nutzern ausgeübte Kontrolle zu erhöhen, sollten die Hersteller Werkzeuge bereitstellen, mit denen die Daten lokal gelesen, bearbeitet und geändert werden können, bevor sie an einen für die Verarbeitung Verantwortlichen übermittelt werden. Darüber hinaus sollten die von einem Endgerät verarbeiteten personenbezogenen Daten in einem Format gespeichert werden, das die Übermittlung der Daten ermöglicht.

- Für die Nutzer besteht ein Auskunftsrecht in Bezug auf ihre Daten. Ihnen sollten Werkzeuge zur Verfügung gestellt werden, mit denen der Export ihrer Daten in einem strukturierten und gängigen Format möglich ist. Daher sollten die Gerätehersteller für Nutzer, die die gespeicherten aggregierten Daten und/oder die Rohdaten erhalten wollen, eine anwenderfreundliche Benutzeroberfläche bereitstellen.

- Die Hersteller der Endgeräte sollten einfache Werkzeuge bereitstellen, mit denen die Nutzer über aufgedeckte Sicherheitslücken benachrichtigt und die Geräte entsprechend aktualisiert werden. Ist ein Gerät veraltet und wird es nicht mehr aktualisiert, sollte der Hersteller den Nutzer darüber informieren und sicherstellen, dass dieser sich dessen bewusst ist. Zudem sollten alle Akteure informiert werden, die von der Sicherheitslücke betroffen sein könnten.

- Die Hersteller sollten ein Verfahren der eingebauten Sicherheit anwenden und einige Komponenten den wichtigsten kryptographischen Primitiven widmen.

- Sie sollten die Datenmenge, die die Geräte verlässt, so weit wie möglich begrenzen und zu diesem Zweck sicherstellen, dass die Rohdaten direkt auf dem Gerät in aggregierte Daten umgewandelt werden. Die aggregierten Daten sollten ein Standardformat besitzen.

- Im Gegensatz zu Smartphones können IoT-Geräte von mehreren Personen genutzt oder gar gemietet werden (z. B. „intelligente Häuser"). Daher sollte eine geeignete Einstellungsmöglichkeit

bestehen, durch die sichergestellt wird, dass zwischen verschiedenen Personen, die das gleiche Gerät nutzen, unterschieden werden kann und diese nichts über die Aktivitäten des anderen erfahren können.

- Die Gerätehersteller sollten mit Normungsgremien und Datenplattformen zusammenarbeiten und auf ein gemeinsames Protokoll hinwirken, in dem Präferenzen in Bezug auf die Datenerhebung und -verarbeitung durch die für die Verarbeitung Verantwortlichen - insbesondere mit Blick auf Fälle, in denen diese Daten durch unauffällige Geräte erhoben werden – formuliert werden.

- Die Hersteller sollten lokale Kontroll- und Verarbeitungsstellen („personal privacy proxies“) einsetzen, die den Nutzern ermöglichen, sich ein klares Bild von den durch ihre Geräte erhobenen Daten zu machen und die lokale Speicherung und Verarbeitung ohne Datenübermittlung an den Hersteller erleichtern.

6.3 **Anwendungsentwickler**

- Es sollten Hinweise oder Warnungen entwickelt werden, die die Nutzer regelmäßig auf die über Sensoren erfolgende Datenerhebung aufmerksam machen. Wenn der Anwendungsentwickler keinen direkten Zugang zum Endgerät hat, sollte die App den Nutzer regelmäßig mit Hilfe einer Mitteilung darüber informieren, dass sie weiterhin Daten erhebt.

- Anwendungen sollten den Nutzer dabei unterstützen, sein Recht auf Auskunft, Änderung und Löschung der von den IoT-Geräten erhobenen personenbezogenen Daten auszuüben.

- Anwendungsentwickler sollten Werkzeuge bereitstellen, mit denen die betroffenen Personen die Rohdaten und/oder die aggregierten Daten in einem einheitlichen und nutzbaren Format exportieren können.

- Anwendungsentwickler sollten insbesondere der Art der verarbeiteten Daten und der Möglichkeit, aus ihnen sensible personenbezogene Daten zu erschließen, Rechnung tragen.

- Anwendungsentwickler sollten nach dem Grundsatz der Datenminimierung verfahren: Falls sich der angestrebte Zweck mit aggregierten Daten erreichen lässt, sollten sie nicht auf die betreffenden Rohdaten zugreifen. Auch sollten die Anwendungsentwickler generell nach dem Grundsatz des „eingebauten Datenschutzes“ vorgehen und die Menge der erhobenen Daten auf die für die Erbringung der Dienstleistung erforderlichen Daten beschränken.

6.4 **Soziale Plattformen**

- Schon im Rahmen der Standardeinstellungen von sozialen Anwendungen auf IoT-Geräten sollten die Nutzer aufgefordert werden, die von ihren Geräten erzeugten Daten vor der Veröffentlichung auf sozialen Plattformen zu überprüfen, zu bearbeiten und auszuwählen.

- Die von IoT-Geräten an soziale Plattformen übermittelten Informationen sollten standardmäßig nicht öffentlich sein und nicht von Suchmaschinen indexiert werden.

6.5 **Eigentümer von IoT-Geräten und weitere Empfänger**

- Die Einwilligung zur Nutzung eines vernetzten Gerätes und der daraus resultierenden Datenverarbeitung muss in Kenntnis der Sachlage und ohne Zwang erfolgen. Nutzer sollten nicht wirtschaftlich bestraft werden oder schlechteren Zugang zu den Funktionen ihrer Geräte haben, wenn sie sich entscheiden, das Gerät oder einen bestimmten Dienst nicht zu nutzen.

- Die betroffene Person, deren Daten im Rahmen einer Vertragsbeziehung mit dem Nutzer eines vernetzten Gerätes (z. B. ein Hotel, einer Krankenversicherung oder einer Autovermietung) verarbeitet werden, sollte in der Lage sein, das Gerät zu verwalten. Unabhängig vom etwaigen Bestehen einer Vertragsbeziehung muss jede betroffene Person, die kein Nutzer ist, ihre Rechte auf Auskunft und auf Widerspruch gegen die Datenverarbeitung ausüben können.

- Nutzer von IoT-Geräten sollten betroffene Personen, die keine Nutzer sind und deren Daten erfasst werden, über das Vorhandensein der IoT-Geräte und die Art der erhobenen Daten informieren. Darüber hinaus sollten sie respektieren, wenn die betroffene Person es vorzieht, dass ihre Daten nicht durch das Gerät erhoben werden.

6.6 **Normungsgremien und Datenplattformen**

- Normungsgremien und Datenplattformen sollten mobile und kompatible sowie eindeutige und selbsterklärende Datenformate fördern, die die Übertragung von Daten zwischen verschiedenen Parteien ermöglichen und den betroffenen Personen verstehen helfen, welche Daten konkret von den IoT-Geräten über sie erhoben werden.

- Normungsgremien und Datenplattformen sollten sich nicht nur auf das Format der Rohdaten konzentrieren, sondern auch auf neue Formate für aggregierte Daten.

- Normungsgremien und Datenplattformen sollten Datenformate unterstützen, die so wenig starke Identifikatoren wie möglich enthalten, um die korrekte Anonymisierung der IoT-Daten zu erleichtern.

- Normungsgremien sollten zertifizierte Standards ausarbeiten, die als Grundlage für Garantien für die Sicherheit und den Schutz der personenbezogenen Daten der betroffenen Personen dienen können.

- Normungsgremien sollten verschlankte Verschlüsselungs- und Kommunikationsprotokolle entwickeln, die auf die Besonderheiten des Internet der Dinge zugeschnitten sind und Vertraulichkeit, Unversehrtheit, Authentifizierung und Zugangskontrolle gewährleisten.