Annika Selzer, Ingo J. Timm

Potenziale anonymer Datenverarbeitungen nutzen

Ein Vorschlag für Smart Cities

Durch den Einsatz von IuK-Technologien und durch das Verknüpfen von Daten kann eine Smart City in ihrer Effizienz optimiert werden. Ziel der Datenverknüpfung kann es z.B. sein, eine Stadt (und den Alltag ihrer Bürger) gesünder, sicherer und – allgemein gesprochen – lebenswerter zu machen. Der Beitrag stellt ein exemplarisches Datenverarbeitungsszenario und -system vor, mit dessen Hilfe das Potenzial anonymer Datenverarbeitungen in Smart Cities unterstützt werden kann.

1 Einleitung[1]

Seit Ende 2019 breitet sich das Coronavirus SARS-CoV-2 weltweit aus und hat zu einer Pandemie geführt, mit der die Menschen auch jetzt – fast zwei Jahre nach dem ersten Ausbruch – noch zu kämpfen haben. Um die Ausbreitung hochinfektiöser Krankheiten einzudämmen und die Zahlen von Neuinfektionen zu senken, bedarf es i.d.R. der Auswertung vieler Daten, zu denen auch personenbezogene Daten zählen können.

Durch den Einsatz von IuK-Technologien sowie durch das Verknüpfen und Auswerten von Daten kann auch eine Smart City u.a. dazu beitragen, ihre Bürger gesund zu halten oder die Ausbreitung von Krankheiten einzudämmen. Eine empirische Datenerhebung mittels 30 Interviews[2] mit Smart-City-Akteuren aus den Branchen Gesundheit, (Grund-)Versorgung sowie Forschung und Bildung, die von den Autoren dieses Beitrags durchgeführt wurde, ergab, dass bei Smart-City-Akteuren zwar ein großes Potenzial besteht, Mehrwerte für die Gesellschaft zu schaffen – z.B. um die Ausbreitung ansteckender Krankheiten einzudämmen und um „Ballungsgebiete" bestimmter Krankheiten identifizieren sowie die Ursachen bekämpfen zu können – dieses Potenzial jedoch weitestgehend unausgeschöpft bleibt.

Um die genannten Mehrwerte erreichen zu können, würde es Smart-City-Akteuren häufig ausreichen, relevante (ehemals) personenbezogene Daten – wie z.B. Daten zu Krankheitsdiagnosen – in anonymisierter Form zu verarbeiten. Umgekehrt könnte eine Re-Identifizierung jedoch für einzelne Bürger in eng begrenzten Kontexten auch von Vorteil sein, z.B. wenn auf der Grundlage der Daten eines Patienten ein Heilmittel für eine Krankheit gefunden wurde. Einer der Hauptfaktoren dafür, dass die möglichen Mehrwerte unausgeschöpft bleiben, ist der Umstand, dass die Smart-City-Akteure oft nicht beurteilen können, wann Daten aus Sicht der DSGVO anonym sind. Bedenken, die von den Interviewten in diesem Zusammenhang geäußert wurden, waren z.B., dass sie meist nicht wissen, welche Daten anonymisiert werden müssen und welche erhalten bleiben dürfen. Hemmschuhe sind auch die Umstände, dass ihre Systeme keine Anonymisierung anbieten oder sie keinen etablierten Prozess für eine Anonymisierung haben.

1 Die diesem Artikel zugrundeliegenden Forschungsarbeiten wurden vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE sowie vom BMBF im Rahmen der Förderung des Projektes AScore (FKZ 13N15663) unterstützt.

Dr. Annika Selzer

Forschungsgruppenleiterin am Fraunhofer-Institut für Sichere Informationstechnologie (SIT).

E-Mail: annika.selzer@sit.fraunhofer.de

Prof. Dr. Ingo J. Timm

Lehrstuhl für Wirtschaftsinformatik I, Universität Trier und Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) Außenstelle Universität Trier.

E-Mail: ingo.timm@dfki.de

2 Die Interviews fanden im Zeitraum vom 23.02.2021 bis 19.03.2021 auf Basis eines Interviewleitfadens statt, der zuvor von drei potenziellen Interviewpartnern validiert wurde. *Selzer/Timm*, Chances and Limitations of Personal and Anonymized Data Processing – Implementing Appropriate Technical and Organizational Measures and Creating Added Value in Smart Cities, GI Informatik 2021 (im Druck).

Basierend auf diesen Erkenntnissen möchte der vorliegende Beitrag ein exemplarisches Datenverarbeitungsszenario und -system vorschlagen, das die Anforderungen der DSGVO umsetzt sowie das Schaffen eines wie oben beschriebenen Mehrwertes im Bereich der Smart Cities ermöglicht.

2 Exemplarisches Datenverarbeitungsszenario und -system

Aus datenschutzrechtlicher Sicht scheinen sich die Anforderungen einer Verarbeitung anonymer Daten in Verbindung mit der Möglichkeit der Wiederherstellung des Personenbezugs im Einzelfall zu widersprechen, da anonyme Daten Informationen sind, die eine betroffene Person nicht oder nicht mehr identifizieren können (Erwgr. 26 DSGVO) und somit das genaue Gegenteil von personenbezogenen Daten darstellen. Die Unterscheidung dieser beiden Begriffe ist wichtig, da nur auf personenbezogene Daten die strengen Vorschriften der DSGVO anwendbar sind. Für eine rein anonyme Datenverarbeitung finden die Vorschriften hingegen keine Anwendung. Sofern ein datenschutzrechtlich Verantwortlicher personenbezogene Daten pseudonymisiert, jedoch die Zuordnungsvorschrift zwischen den Pseudonymen und den natürlichen Personen behält, findet die DSGVO auch für diese Verarbeitung vollumfänglich Anwendung. Die Formulierung, dass anonyme Daten nicht oder nicht mehr identifizierbar sein dürfen, klingt absolut. Nach herrschender Meinung hängt die Identifizierbarkeit einer Person jedoch primär vom Wissen der datenverarbeitenden Stelle bzgl. der Identität einer Person ab, so dass Informationen, für die die datenverarbeitende Stelle X einen Personenbezug herstellen kann, weil sie über das nötige Zusatzwissen verfügt, personenbezogen sind. Für die datenverarbeitende Stelle Y, die nicht über das Zusatzwissen verfügt, sind die Informationen jedoch anonym, sofern es ihr nicht möglich ist, das Zusatzwissen (z.B. durch Weisungsrechte gegenüber X) zu erlangen.[3]

Ausgehend von der herrschenden Meinung schlägt dieser Beitrag ein Datenverarbeitungsszenario vor, in dem Smart-City-Akteure ausschließlich auf (aus ihrer Perspektive) anonyme Daten zugreifen können, ohne dass für sie selbst die Möglichkeit der Re-Identifizierung der Daten besteht (Regelfall). Eine Re-Identifizierung ist nur im begründeten Einzelfall und nur für einen hierfür vorgesehenen Datentreuhänder möglich (Ausnahmefall), so dass die Smart-City-Akteure für die Nutzung der anonymen Daten im Rahmen des Regelfalls nach der hier vertretenen Meinung nicht unter die Anwendbarkeit der DSGVO fallen.

2.1 Regelfall

In dem hier betrachteten Datenverarbeitungsszenario können Smart-City-Akteure personenbezogene Daten einem Datentreuhänder überlassen[4] (Schritt 1 in der nachfolgenden Abbildung). Der Datentreuhänder bietet hierfür ein Datenverarbeitungssystem an, das sowohl Schnittstellen zu den Datenspendern als auch zu den Datennutzern bietet. Nachdem der Datenspender die personenbezogenen Daten dem Datentreuhänder überlassen hat, pseudonymisiert dieser die Daten (Schritt 2), ohne dass den zur Identifizierung der pseudonymisierten Datensätzen nötigen Zuordnungsvorschriften im Regelfall des beschriebenen Datenverarbeitungsszenarios eine weitere Funktion zukommt. Die pseudonymisierten Daten stellt er für den Zugriff durch jedermann („Datennutzer") zur Verfügung. Der Datentreuhänder schließt hierbei aus, dass die Datennutzer auf die zur De-Pseudonymisierung notwendigen zusätzlichen Informationen Zugriff erhalten können. Somit ist nur ihm selbst eine De-Pseudonymisierung möglich, so dass die Datennutzer nach der hier vertretenen Meinung im Ergebnis auf anonyme Daten[5] zugreifen (Schritt 3), auf die die Vorschriften der DSGVO keine Anwendung finden. Diese Schritte beschreiben den Regelfall des im weiteren Verlauf dieses Beitrags betrachteten Datenverarbeitungsszenarios.

Der Datentreuhänder verfügt über das nötige rechtliche und technische Wissen, um die (aus seiner Perspektive pseudonymisierten) Daten den Datennutzern so zur Verfügung zu stellen, dass sie für diese tatsächlich anonym sind.[6] Insbesondere stellt er sicher, dass die zur Verfügung gestellten Daten keine Quasi-Identifyer enthalten (so könnte z.B. die Kombination der Angaben von Geburtsdatum, Wohnort und Geschlecht einer Person – ohne weitere Angaben wie Namen, Passnummer und Postanschrift – zur Herstellung des Personenbezugs ausreichen) und jeder Datensatz, der ihm von einem Datenspender übermittelt wird, unter einem neuen Pseudonym gespeichert wird – auch wenn bspw. Datenspender A und Datenspender B personenbezogene Daten zur gleichen betroffenen Person überlassen – so dass der Datennutzer nicht erkennen kann, ob die Datensätze 1 und 2 der gleichen Person oder zwei unterschiedlichen betroffenen Personen zuzuordnen sind.

Dem Einsatz eines Datentreuhänders, so wie hier vorgeschlagen, liegt die Überlegung zugrunde, das Abrufen anonymer Daten zu ermöglichen und den Smart-City-Akteuren als Datennutzern völlige Nutzungsfreiheit zum Erreichen der eben beschriebenen Mehrwerte zu gewähren. Da der Datentreuhänder selbst die zugrundeliegenden personenbezogenen Daten verwaltet, kann er in begründeten Einzelfällen einen Personenbezug herstellen, um für die einzelne betroffene Person einen Individualmehrwert (wie z.B. die Aufnahme in eine klinische Studie) zu erzielen. Hierfür ist es wichtig, dass der Datentreuhänder die treuhänderisch verwalteten Daten ohne jegliches Eigeninteresse an der Datennutzung und -manipulation verarbeitet und in keinem Interessenskonflikt zu der Erfüllung seiner Aufgaben als Datentreuhänder oder zu sonstigen Rechten und Pflichten steht.[7]

Datentreuhänder sind insofern als „Intermediäre zwischen den Datenverarbeitern einerseits und den betroffenen Personen andererseits [zu verstehen, denen das Potenzial innewohnt,] dass die betroffenen Personen mit ihrer Hilfe ihre informationelle Selbstbestimmung [….] gegenüber den Verantwortlichen besser wahr-

3 *Karg* in *Simitis/Hornung/Spiecker*, DSGVO Kommentar, Art. 4 Nr. 1 Rdnr. 58 ff.; *Selzer* in *Jandt/Steidle*, Datenschutz im Internet, S. 127 f.; *Husemann* in *Roßnagel*, Das neue Datenschutzrecht, S. 84 f.; *Klar/Kühling* in: *Kühling/Buchner*, DSGVO BDSG, Art. 4 Nr. 1 Rn. 25 ff.; *Buchner*, DuD 2013, 804; *Kroschwald*, ZD 2014, 76; *Härting*, NJW 2013, 2066; *Kühling/Klar*, NJW 2013, 3613 f.

4 In diesem Beitrag wird der Smart-City-Akteur, der dem Datentreuhänder personenbezogene Daten überlässt, zur sprachlichen Vereinfachung als „Datenspender" bezeichnet.

5 So auch *Kühling*, ZfDR 2021, 1 (6 f.).

6 Zur vereinfachten Beschreibung des Verarbeitungsszenarios wird nachfolgend z.T. abkürzend von „anonymisierten" bzw. von „anonymen Daten" gesprochen, ohne weiter darauf einzugehen, dass die Daten pseudonymisiert wurden und den Datennutzern der Zugriff auf die personenidentifizierenden Merkmale nicht möglich ist und sein wird, so dass die Daten für sie in der Konsequenz anonym sind.

7 *Brockmeyer*, ZD 2018, 258 (258 f.); *Wieczorek*in *Specht/Mantz*, Handbuch Europäisches und deutsches Datenschutzrecht, § 7 Rdnr. 101.

Abbildung 1 | Regelfall

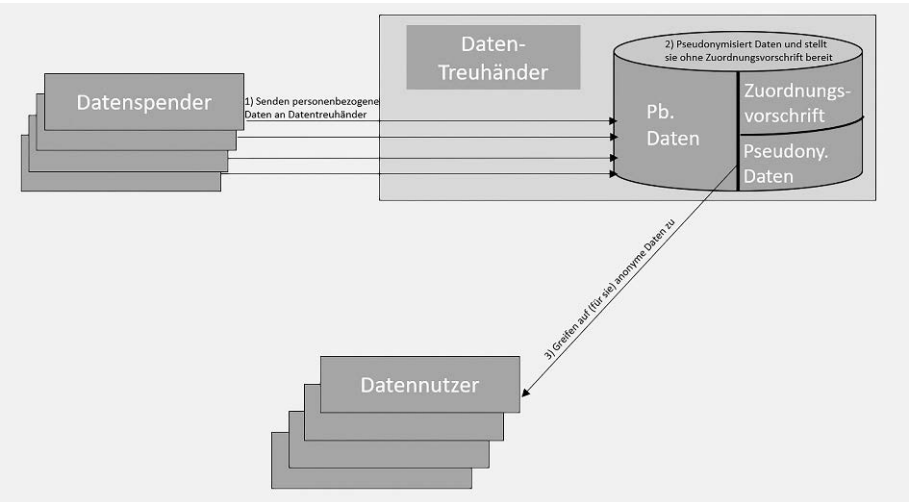
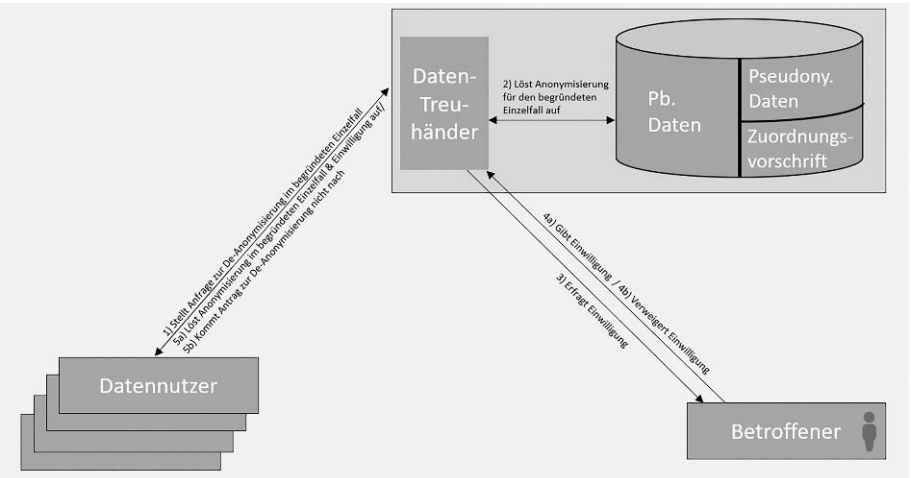


Abbildung 2 | Ausnahmefall[9]



nehmen und auf diese Weise sowohl die Datensouveränität als auch die Kommerzialisierungsfairness steigern können."[8]

2.2 Ausnahmefall

Um der Anforderung gerecht zu werden, im Einzelfall den Personenbezug wiederherstellen zu können, sieht der Ausnahmefall des hier betrachteten Datenverarbeitungsszenarios die Möglichkeit des Datennutzers vor, bei dem Datentreuhänder (per E-Mail, die aus dem Datenverarbeitungssystems des Treuhänders generiert wird) einen Antrag auf Re-Identifizierung für begründete Einzelfälle zu stellen (Schritt 1 in der nachfolgenden Abbildung). Daraufhin stellt der Datentreuhänder den Personenbezug für den einzelnen Datensatz her (Schritt 2) und erfragt bei der betroffenen Person (per E-Mail, die aus dem Datenverarbeitungssystems des Treuhänders generiert wird) die Einwilligung in die Datenweitergabe an den Datennutzer, die diese sodann erteilt oder verweigert (Schritt 3). Sofern die betroffene Person die Einwilligung in die Datenweitergabe erteilt (Schritt 4a), erhält der Datennutzer die personenidentifizierenden Merkmale und Kontaktdaten der betroffenen Person (Schritt 5a) auf dem gleichen Weg, wie er die Herstellung des Personenbezugs beantragt hat. Sofern die betroffene Person die Einwilligung verweigert (Schritt 4b), werden die personenidentifizierenden Merkmale und Kontaktdaten nicht an den Datennutzer weitergegeben (Schritt 5b).

Die Datenverarbeitung im Rahmen des beschriebenen Regel- und Ausnahmefalls führt zu einer Trennung des Datenverarbeitungssystems des Datentreuhänders: Während in Teil 1a) des Datenverarbeitungssystems personenbezogene Daten verarbeitet werden, werden in Teil 1b) des Datenverarbeitungssystems (aus Sicht des Datennutzers) ausschließlich anonyme Daten verarbeitet.

Der vorliegende Beitrag geht davon aus, dass die einzelnen Datenspender, Datennutzer sowie der Datentreuhänder jeweils eigenständige Verantwortliche sind.[10]

3 Gestaltung der Rollen im System

In dem System müssen die Rollen des Treuhänders, des Datenspenders, des Datennutzers und der betroffenen Person gestaltet werden. Die Gestaltung betrifft insbesondere die Anforderungen an sowie die Rechte der jeweiligen Rolle.

3.1 Rollen im System

Treuhänder

Wie bereits erwähnt, liegt dem Vorschlag des Einsatzes eines Datentreuhänders die Überlegung zugrunde, das Abrufen anonymer Daten zu ermöglichen[11] und den Smart-City-Akteuren als Datennutzern völlige Nutzungsfreiheit zum Erreichen der eben

8 *Kühling*, ZfDR 2021, 1; s.a. ## (in diesem Heft).

9 Quelle der Abbildung der betroffenen Person: https://freesvg.org/vector-illustration-of-simple-man-or-person-silhouette-icon.

10 Eigenständig Verantwortliche entscheiden jeweils eigenständig über die Zwecke und Mittel der Datenverarbeitung (Art. 4 Nr. 7 DSGVO). In Abgrenzung zu eigenständigen Verantwortlichen wären mehrere Organisationen gemeinsam verantwortlich, wenn sie gemeinsam über die Zwecke und Mittel der Datenverarbeitung entscheiden würden. Wiederum davon abzugrenzen wäre die Auftragsverarbeitung, bei der eine Organisation personenbezogene Daten nach Auftrag und basierend auf Weisungen für einen Verantwortlichen verarbeitet. In dem hier beschriebenen Verarbeitungsszenario entscheidet jede beteiligte Organisation eigenständig darüber, zu welchen Zwecken (z.B. „Forschung zur Verbesserung der Medikation von Patienten mit Schilddrüsenüberfunktion") und mit welchen Mitteln (z.B. Datenanalysen mittels selbstlernender künstlicher Intelligenz) sie Daten verarbeitet. Zudem verbindet keine der Organisationen die Datenverarbeitung durch andere Organisationen mit Weisungen, so dass im Ergebnis von einer jeweils eigenständigen Verantwortung auszugehen ist.

11 *Wieczorek* in *Specht/Mantz*, Handbuch Europäisches und deutsches Datenschutzrecht, § 7 Rdnr. 101.

beschriebenen Mehrwerte zu ermöglichen, da bei der Verarbeitung der durch den Datentreuhänder zur Verfügung gestellten, anonymen Daten keine datenschutzrechtlichen Vorschriften beachtet werden müssen. Gleichzeitig ermöglicht die (personenbezogene) Datenverwaltung durch den Datentreuhänder es, in begründeten Einzelfällen einen Personenbezug herzustellen, um für die einzelne, betroffene Person einen Individualmehrwert zu erzielen.

Die Rolle eines Datentreuhänders ist nicht trivial, da bei ihm eine große Anzahl personenbezogener Daten zusammengeführt wird und das Zusammenführen solch großer Mengen personenbezogener Daten, unter denen sich auch besondere Kategorien personenbezogener Daten befinden, grundsätzlich mit einem höheren Risiko für die Rechte und Freiheiten betroffener Personen verbunden ist als eine dezentrale Datenspeicherung bei den einzelnen Datenspendern. Die Gefahr einer unrechtmäßigen Nutzung der Daten durch den Datentreuhänder selbst muss daher durch von ihm zu ergreifende angemessene technische und organisatorische Schutzmaßnahmen sowie durch grundlegende, an ihn zu stellende Anforderungen verhindert werden.

Datenspender
Datenspender überlassen personenbezogene Daten ihrer Kunden und Mitarbeiter an Smart-City-Akteure, sofern durch den Datentreuhänder sichergestellt wird, dass den Smart-City-Akteuren diese Daten nur in anonymer Form vorgelegt werden und eine Re-Identifizierung nur durch den Datentreuhänder möglich ist – und diese auch nur dann erfolgt, sofern ein Smart-City-Akteur als Datennutzer für den individuellen Einzelfall die Vorteile der Aufhebung des Personenbezugs für die betroffene Person darlegen konnte und die betroffene Person mit der Herstellung des Personenbezugs einverstanden ist.

Datennutzer
Datennutzer nutzen die durch den Treuhänder in anonymer Form bereitgestellten Daten. Eine Re-Identifizierung eines Datensatzes für den Datennutzer ist nur im individuellen und begründeten Einzelfall möglich und kann nicht durch den Datennutzer selbst, sondern nur durch den Datentreuhänder herbeigeführt werden, wenn die betroffene Person mit der Herstellung des Personenbezugs einverstanden ist.

Betroffene Person
Die betroffenen Personen sind die natürlichen Personen, deren personenbezogene Daten von dem Datenspender und Treuhänder verarbeitet werden. Sofern der Datennutzer im Rahmen der anonymen Datennutzung gegenüber dem Treuhänder im Einzelfall begründen kann, warum die Re-Identifizierung eines einzelnen Datensatzes einen Mehrwert für die (hiervon) betroffene Person hat, erhält die betroffene Person die Möglichkeit, dieser Re-Identifizierung entweder zuzustimmen oder sie abzulehnen.

3.2 Anforderungen an die Rollen

Keine Weisungsbefugnisse
(Muss-Anforderung für den Treuhänder und die betroffene Person)
Ein Datentreuhänder ist für diese Rolle nur dann geeignet, wenn er über keine rechtliche oder tatsächliche Möglichkeit verfügt, die betroffenen Personen bezüglich der Erteilung einer Einwilligung in die Re-Identifizierung zu beeinflussen. Insbesondere im Angestelltenverhältnis ist es schwierig, die Freiwilligkeit der datenschutzrechtlichen Einwilligungserklärung des Arbeitnehmers – als verpflichtende Anforderung an eine datenschutzkonforme Einwilligung – zu gewährleisten.[12] Insofern ist auf eine strenge Rollentrennung zwischen dem Datentreuhänder in seiner Rolle als Treuhänder und ggf. weiteren Rollen, im Rahmen derer gegenüber betroffenen Personen Weisungsbefugnisse bestehen könnten zu achten bzw. hat der Datentreuhänder auf derartige Weisungsbefugnisse im Rahmen des hier betrachteten Systems zu verzichten.
Parallel darf eine betroffene Person nicht in rechtlicher oder tatsächlicher Weise durch den Datentreuhänder zur Erteilung der Einwilligung in die Re-Identifizierung gedrängt werden, insbesondere dürfen seitens des Datentreuhänders keine Weisungsbefugnisse zur Erteilung der Einwilligung bestehen.

Kein Eigeninteresse an der Datennutzung und -manipulation
(Muss-Anforderung für Datentreuhänder und Datenspender)
Weder der Datentreuhänder noch der Datenspender dürfen ein Eigeninteresse an der Datennutzung oder der Datenmanipulation haben.[13] So könnte z.B. ein Eigeninteresse seitens des Datentreuhänders dazu führen, dass er sich gegenüber den potenziellen Datennutzern nicht fair und diskriminierungsfrei in Bezug auf das Zur-Verfügung-Stellen der anonymen Daten verhält und ihnen gegebenenfalls anonyme Daten vorenthält.[14] Ein Eigeninteresse an der Datenmanipulation würde ggf. zur Unbrauchbarkeit der Daten seitens der potenziellen Datennutzer führen. Um Eigeninteressen an den durch den Datentreuhänder verwalteten Daten auszuschließen, wird empfohlen, den Datentreuhänder außerhalb der Branche, in deren Rahmen die Daten verwaltet werden, auszuwählen.[15] Da an der Mehrwertgenerierung im Smart-City-Kontext eine Vielzahl von Branchen beteiligt ist bzw. zumindest sein kann, sollte der Datentreuhänder keiner der beteiligten Branchen angehören.

Keine Interessenskonflikte
(Muss-Anforderung für den Datentreuhänder, den Datenspender und den Datennutzer)
Nicht weniger wichtig als ein fehlendes Eigeninteresse an der Datenverarbeitung und -manipulation ist die Anforderung, nicht in einem Interessenskonflikt zu anderen Pflichten zu stehen.[16] Dies wäre u.a. dann gegeben, wenn der Datentreuhänder ein mit einem Datenspender oder Datennutzer verbundenes Unternehmen i.S.d. §§ 15 ff. Aktiengesetz wäre, da in diesem Fall umfangreiche Weisungs- und Stimmrechte u.a. zum Erzwingen der Herausgabe personenidentifizierender Merkmale bestehen könn-

12 Vgl. *Ströbel/Wybitul* in *Specht/Mantz*, Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rdnr. 50. I.d.R. kann die Freiwilligkeit im Angestelltenverhältnis zumindest dann bejaht werden, wenn sich für den Angestellten ausschließlich Vorteile ergeben (z.B. Abschluss einer Zusatzversicherung).

13 *Brockmeyer*, ZD 2018, 258 (258 f.).

14 S. *Stender-Vorwachs/Steege* in *Oppermann/Stender-Vorwachs*, Autonomes Fahren, Rdnr. 212, die u.a. große Unternehmen wie Google sowie Versicherungsträger für ungeeignete Datentreuhänder halten. *Stender-Vorwachs/Steege* warnen auch vor den Gefahren einer Monopolbildung und werfen kartellrechtliche Fragen auf, die im Rahmen dieses Beitrags aufgrund der thematischen Ausrichtung jedoch nicht diskutiert werden.

15 *Caldarola/Schrey*, Big Data und Recht, Rdnr. 294.

16 *Brockmeyer*, ZD 2018, 258 (258 f.).

Tabelle 1 |

Rolle	Umfang der Rechte	Zeitpunkt der Rechte
Treuhänder	Personenbezogene Daten Erhebung der Daten Lesen der Daten Pseudonymisierung der Daten Speichern der Daten Anonymisierte Daten (Regelfall) Bereitstellen der Daten Lesen der Daten Speichern der Daten	Dauerhaft
	Personenbezogene Daten Ändern der Daten Löschen der Daten Anonymisierte Daten (Regelfall) Ändern der Daten Löschen der Daten De-Anonymisierte Daten (Ausnahmefall) De-Anonymisierung durchführen De-Anonymisierte Daten bereitstellen De-Anonymisierte Daten lesen De-Anonymisierte Daten speichern De-Anonymisierte Daten ändern De-Anonymisierte Daten löschen	Anlassbezogen
Datenspender	Personenbezogene Daten Weitergabe der Daten zur anony. Bereitstellung Lesen der Daten	Dauerhaft
	Personenbezogene Daten Änderungen an Daten melden	Anlassbezogen
Datennutzer	Anonymisierte Daten (Regelfall) Lesen der Daten Speichern der Daten	Dauerhaft
	De-Anonymisierte Daten (Ausnahmefall) De-Anonymisierung beantragen De-Anonymisierte Daten lesen De-Anonymisierte Daten speichern	Anlassbezogen
Betroffene Person	Personenbezogene Daten Änderungen an Daten melden	Dauerhaft
	De-Anonymisierte Daten (Ausnahmefall) De-Anonymisierung autorisieren	Anlassbezogen

ten.[17] Das Bestehen derartige Weisungs- und Stimmrechte ist – ggf. durch Verzichterklärungen – zu unterbinden.

Trennung zu anderen Beteiligten auf allen Ebenen
(Muss-Anforderung für den Datentreuhänder, den Datenspender und den Datennutzer)
Die vorhergehenden Anforderungen ergänzend müssen Datentreuhänder, Datenspender und Datennutzer nicht nur rechtlich unabhängig, sondern auch personell und räumlich voneinander getrennt sein.[18]

Vertragsschluss
(Muss-Anforderung für den Datentreuhänder, den Datenspender und den Datennutzer)
Einige der beschriebenen Anforderungen sind auf Basis eines Vertrages sicherzustellen, indem die Nutzung und der Betrieb des Datenverarbeitungssystems an einen Vertrag zwischen Datenspender und Datentreuhänder (Vertrag 1), zwischen Datennutzer und Datentreuhänder (Vertrag 2) und zwischen bestimmten betroffenen Personen und Datentreuhänder (Vertrag 3) gebunden sein muss.

3.3 Rollen-Berechtigungen

Die nachfolgende Tabelle zeigt den Umfang und den Zeitpunkt der Rechte je Rolle an. Die beschriebenen Rechte beziehen sich nur auf die im Rahmen des betrachteten Verarbeitungssystems bestehenden Rechte der einzelnen Rollen. So darf ein Datennutzer zwar die anonymen Daten, die er in seinem eigenen Datenverarbeitungssystem gespeichert hat, ändern und löschen, nicht aber in dem im Rahmen dieses Beitrags betrachteten System.

4 Weitere Anforderungen (Ausblick)

Der Beitrag stellt ein exemplarisches Datenverarbeitungsszenario und -system vor, mit dessen Hilfe anonyme Datenverarbeitungen in Smart Cities unterstützt werden können. Mithilfe dieser anonymen Datenverarbeitungen lassen sich wichtige Mehrwerte für die Gesellschaft schaffen, wie z.B. die Identifikation von „Ballungsgebieten" bestimmter Krankheiten und deren Ursachen als Ausgangspunkt zur Ableitung von Abhilfemaßnahmen gegen die krankheitsauslösenden Ursachen. Der Erfolg eines solches Systems steht und fällt jedoch mit seiner Sicherheit. Im vorgestellten Datenverarbeitungssystem bedeutet dies insbesondere, dass ein abgestuftes Schutzkonzept zur Umsetzung technischer und organisatorischer Maßnahmen vorgesehen werden muss, das berücksichtigt, an welchen Stellen im System personenbezogene, pseudonyme und anonyme Daten verarbeitet werden. Wie ein solches abgestuftes Schutzkonzept aussehen und konkret umgesetzt werden könnte, ist Gegenstand eines weiteren Beitrags in diesem Heft.[19]

17 *Caldarola/Schrey*, Big Data und Recht, Rdnr. 289.

18 Aus Platzgründen werden in diesem Beitrag nur die Muss-Anforderungen an die Rollen benannt. Als Soll-Anforderungen an den Datentreuhänder gilt es, die Rolle mit einem Notar zu besetzen, der über die notwendige Fachkunde verfügt und datenschutzrechtlich zertifiziert ist. Nicht zuletzt sollte ein zwischen dem Datentreuhänder und den einzelnen Datenspendern geschlossener Vertrag Vertragsstrafen in abschreckender Höhe vorsehen, die im Falle von Verstößen gegen die treuhänderischen Pflichten des Datentreuhänders bestehen. *Caldarola/Schrey*, Big Data und Recht, Rdnr. 293 u. 295.

19 S. dazu in der Rubrik Good Practice (in diesem Heft) „Gestaltung eines Treuhand-Systems zum anonymen Datenaustausch in einer Smart-City-Umgebung".