Alexander von Humboldt
INSTITUT FÜR INTERNET
UND GESELLSCHAFT

DATENTEILEN UNTER WAHRUNG VON GESCHÄFTSGEHEIMNISSEN

Workshop / Roundtable

Am Workshop beteiligte Unternehmen:

- Miles Mobility GmbH
- TIER Mobility SE
- Bolt Technologies OÜ
- DB InfraGO AG

Projektteam:

- Prof. Dr. Max von Grafenstein (HIIG)
- Maurice Stenzel (HIIG)
- Alexandra Auer (HIIG)
- Jochen Rabe (RSUP)
- Unterstützt durch: Sibylle Kubale (Berlin Partner für Wirtschaft und Technologie)

Datum und Ort:

- 11. Juni 2024, 09:00 - 12:00 Uhr
- Berlin Partner, Ludwig Erhard Haus, Fasanenstraße 85

Der Workshop wurde im Rahmen des Projekts "Data & Smart City Governance am Beispiel von Luftgütemanagement" durchgeführt. Das Projekt wird gefördert von dem Regierenden Bürgermeister von Berlin - Senatskanzlei - aus Mitteln des Bundesministeriums für Wohnen, Stadtentwicklung und Bauwesen sowie der Kreditanstalt für Wiederaufbau.

THEMA UND FRAGESTELLUNG

Der Workshop befasste sich mit der Frage, wie Daten unter Wahrung von Geschäftsgeheimnissen geteilt werden können. Der Schwerpunkt lag auf der gemeinsamen Nutzung von Daten im Mobilitätsökosystem, in dem Daten zwischen allen beteiligten Akteuren und in alle Richtungen ausgetauscht werden (multiperspektivischer Data Governance-Ansatz).

Themenblöcke und Key Points

Einführung:

- Vorstellung des Projekts “Data & Smart City Governance am Beispiel von Luftgütemanagement” und Verortung des Workshops in diesem Kontext
- Fokus: Teilen von Daten unter Wahrung von Geschäftsgeheimnissen
- Präsentation der Ergebnisse aus den Vorgesprächen mit den beteiligten Unternehmen sowie weiteren (beim Workshop nicht anwesend)

B2G-Szenario:

- Vorstellung des Szenarios und vertiefte Diskussion der Angreiferszenarien beim Teilen von Daten mit öffentlichen Stellen entlang exemplarischer Use Cases
- Die Bedenken der Unternehmen in diesem Szenario beziehen sich vor allem auf die Interpretation und den möglichen geschäftsschädigenden Missbrauch der Daten
- Erörterung möglicher Schutzmechanismen sowie der Auswirkungen des Data Acts (EU)
- Diskussion, inwieweit vertrauenswürdige Dritte das Gleichgewicht zwischen Risiken und Wertschöpfung beim Teilen von Daten herstellen können

B2B-Szenario:

- Vorstellung des Szenarios und vertiefte Diskussion der Angreiferszenarien beim Datenteilen zwischen Unternehmen an exemplarischen Use Cases
- Diskussion kartellrechtlicher Herausforderungen und möglicher Schutzmechanismen beim Datenteilen
- Die Unternehmen betonten die Gestaltungsspielräume beim freiwilligen Datenteilen und äußerten die Befürchtung, dass durch das geplante Mobilitätsdatengesetz und die damit verbundene Open-Data-Pflicht in den entsprechenden Data Spaces weitreichende Zugriffsrechte entstehen könnten, die den Interessen der Unternehmen zuwiderlaufen.
- Diskussion, inwieweit vertrauenswürdige Dritte das Gleichgewicht zwischen Risiken und

Wertschöpfung beim Teilen von Daten zwischen Unternehmen herstellen können

B2R/B2S-Szenario:

- Vorstellung des Szenarios und vertiefte Diskussion der Angreiferszenarien beim Datenteilen zwischen Unternehmen, Forschung/Zivilgesellschaft an exemplarischen Use Cases
- Diskussion von Standardisierungsfragen bei der Datenerhebung und Auswirkungen möglicher Interpretationen von Datenanalysen auf die Position von Unternehmen im öffentlichen Diskurs
- Diskussion, inwieweit vertrauenswürdige Dritte das Gleichgewicht zwischen Risiken und Wertschöpfung beim Teilen von Daten zwischen Unternehmen, Forschung/Zivilgesellschaft herstellen können

Anforderungen an eine Trusted Third Party (TTP):

- Konsolidierung der Anforderungen an eine vertrauenswürdige dritte Instanz
- Kernelemente: Neutralität, politische Unabhängigkeit und Gemeinnützigkeit
- Hervorgehoben wurde die Notwendigkeit einer transparenten und kooperativen Forschung, um Vertrauen aufzubauen und einen effektiven Datenaustausch zu gewährleisten

Check out:

- Aus Perspektive der Unternehmen ist Shared Data zur Wahrung von Geschäftsgeheimnissen gegenüber Open Data-Modellen vorzuziehen
- Akteursübergreifend durchgeführten Projekten wird das Potential zugeschrieben, mehr Verständnis für die individuellen Interessen aufzubauen sowie transparente Lösungswege für das Datenteilen mit Dritten zu erproben

Erkenntnisse aus dem Vorprozess

Im Vorprozess wurden Gespräche mit mehreren Vertreter*innen unterschiedlicher Mobilitätsanbieter geführt.

- Die Gesprächspartner*innen validierten, dass Daten grundsätzlich verstärkt mit Dritten (auch Wettbewerbern) zweckgebunden geteilt werden würden. Bisher sind jedoch die Risiken entweder zu hoch oder der Aufwand rechtfertigt den möglichen Mehrwert nicht.
    - Insbesondere bei der Zusammenarbeit mit öffentlichen Stellen besteht oft große Unsicherheit über den konkreten Verwendungszweck der Daten.

- Die Gesprächspartner*innen konkretisierten folgende für das Mobilitätsdaten-Ökosystem relevanten Daten
    - Streckendaten (insbesondere nicht nur Start- und Zieldaten, sondern auch

Wegedaten im engeren Sinne)
    - Kartendaten (z.B. für autonomes Fahren)
    - Nutzungsdaten von Mobilitätsobjekten (z.B. zu Nutzungsart, Auslastung, Miethöhe, Nutzererfahrungen)

- Die Gesprächspartner*innen wiesen darauf hin, dass das Interesse am Datenschutz je nach Branche und Geschäftsmodell variiert. Entscheidende Faktoren sind:
    - Rolle des Datenhalters (gewinnorientiert, privat oder öffentlich)
    - Fokus des öffentlichen / politischen Drucks (“Framing”)
    - Kosten der Dateninfrastruktur

- Die Gesprächspartner*innen bestätigten, dass die Wahrung von Geschäftsgeheimnissen und der Datenschutz in den Unternehmen ein wichtiges Thema sind. Folgende Schutzmechanismen sind dabei bisher zentral:
    - Anonymisierung der Daten (auch bei Geschäftsgeheimnissen)
    - Kontrolle des Datenzugangs und der Datennutzung
    - Kontrolle der Datenqualität (z.B. ist es insbesondere auch für Dateninhaber relevant, die Qualität ihrer Daten sicherzustellen, bevor diese z.B. in den öffentlichen Diskurs eingebracht werden)

- Die Gesprächspartner*innen bestätigten,
    - dass das Prozessmodell “Business Secret Risk Assessment” ein zielführendes Instrument zum Schutz von Geschäftsgeheimnissen beim Datenteilen darstellt. Das Modell wird in ähnlicher Form bereits in Unternehmen angewendet.
    - dass eine Trusted Third Party helfen könnte, die Risiken und Kosten beim Teilen von Daten zu reduzieren. In Bezug auf den Common European Mobility Data Space (EMDS) wurde darauf hingewiesen, dass dieser die Risiken derzeit noch nicht lösen könne. Geregelt werden darin bislang nur Fragen hinsichtlich der technischen Standardisierung. Es werden bisher nur Fragen der technischen Standardisierung geregelt. Die Umsetzung der vorgeschlagenen Standards wird jedoch noch als zu aufwendig angesehen.

1 Datenteilen zwischen Unternehmen und der öffentlichen Verwaltung (B ↔ G)

Use Cases:

Für den Datenaustausch zwischen Unternehmen und der öffentlichen Verwaltung wurden Angreiferszenarien und Mechanismen zum Schutz von Geschäftsgeheimnissen an folgendem Use Case diskutiert:

Eine Kommune knüpft die Erteilung einer Sondernutzungserlaubnis für Shared Mobility-Anbieter an das Teilen von Mobilitätsdaten.

- Die Kommune kann anhand dieser Daten die Einhaltung der in der Sondernutzungserlaubnis festgelegten Bedingungen prüfen.
- Die Kommune kann die geteilten Daten für eigene Planungen nutzen.
- Die Kommune kann mithilfe der geteilten Daten die Einsatzplanung der Ordnungsämter optimieren (nahezu in Echtzeit).
- Die Kommune wird in die Lage versetzt Mobilitätsbedürfnisse zu „managen". Dies ist eine Rolle, die einzelne Unternehmen nicht ausführen können (da sie in Konkurrenz zueinander stehen). Dies erfordert allerdings ein Umdenken in der Kommune, von der Verkehrsplanung hin zu Mobilitätsmanagement.

Angreiferszenario: "Kannibalisierung" der Anbieter durch öffentliche Stellen

- Das Teilen von Daten mit der öffentlichen Verwaltung, aus denen sich Geschäftsgeheimnisse ableiten lassen, birgt die Gefahr, dass von öffentlicher Seite konkurrierende Dienstleistungen angeboten werden. Dies wäre z.B. im Bereich der Mikromobilität der Fall, wenn frequentierte Gebiete oder lukrative Strecken der Mikromobilitätsanbieter durch zusätzlichen ÖPNV verstärkt werden oder Eigenbetriebe gegründet werden, die gezielt in Konkurrenz zu privatwirtschaftlichen Angeboten treten (Beispiel Ridesharing: Berlkönig / MuVa).
- Die Unternehmen sehen beim Teilen von Daten mit der öffentlichen Verwaltung das

Risiko einer verzerrenden Marktregulierung. Diese Gefahr konkretisiert sich zum einen, wenn bestimmten Mobilitätsformen der Zugang zum lokalen Markt gewährt, anderen aber verwehrt wird. Zum anderen könnten öffentliche Verwaltungen auf Basis der gemeinsam genutzten Daten Obergrenzen für bestimmte Fahrzeugtypen/-klassen festlegen, um eigene Mobilitätsinteressen in einer Kommune durchzusetzen. Diese Interessen sind nach Aussage der Unternehmen jedoch weniger empirisch begründet, sondern häufig eher eine "Glaubensfrage" (siehe hierzu auch das Angriffsszenario "Framing").

Angreiferszenario: Geschäftsschädigendes "Framing"

Mit öffentlichen Verwaltungen Daten zu teilen, birgt das Risiko, dass die Daten sowohl auf politischer Ebene als auch in der öffentlichen Debatte in einen Kontext gestellt werden, der sich negativ auf die Geschäftstätigkeit privatwirtschaftlicher Akteure auswirkt:

- Bezogen auf die politische Ebene: Der entscheidende Risikofaktor für ein negatives Framing von Daten ist vor allem das politische Interesse einer Kommune.
- Bezogen auf die öffentliche Debatte: Es besteht die Gefahr, dass Daten in (vermeintliche) Zusammenhänge gestellt werden, um bereits bestehende Vorurteile zu bestätigen. Dabei bezieht sich die Interpretation oft weniger direkt auf die geteilten Daten (die andere Schlussfolgerungen nahe legen können), sondern vielmehr auf vorgelagerte Interessen und politische Agenden.

Konsolidierung der Schutzmechanismen:

Die beteiligten Unternehmen bestätigen die aus dem Vorprozess abgeleiteten Schutzmechanismen:

- Mit der öffentlichen Verwaltung werden derzeit von einigen Unternehmen nur Daten über die stehenden Shared Mobility-Fahrzeuge geteilt. Durch die Reduktion auf einen Start- und einen Zielpunkt wird verhindert, dass exakte Rückschlüsse auf die gefahrene Strecke (und damit auf die Wirtschaftlichkeit des Unternehmens) gezogen werden können.
- Einige Unternehmen teilen Daten mit öffentlichen Verwaltungen auf der Grundlage von Datenüberlassungserklärungen. Darin wird festgelegt, wer die Daten zu welchem Zweck verarbeiten darf und welche Schutzmaßnahmen getroffen werden, um die Daten vor dem Zugriff Dritter zu schützen.

Schutzmechanismus zur Wahrung der Verhältnismäßigkeit:

- Die derzeit geplante Verpflichtung von Unternehmen, Verkehrsdaten unentgeltlich zur Verfügung zu stellen (Mobilitätsdatengesetz), wird von den Unternehmen kritisch

gesehen. Das Teilen von Daten als Open Data ist zum einen mit Aufwand für die bereitstellenden Unternehmen verbunden und birgt zum anderen die Gefahr, dass Geschäftsgeheimnisse unentgeltlich mit unbekannten Dritten geteilt werden müssen. Konkrete Anwendungsfälle sind derzeit noch weitgehend unklar. Sofern konkrete Use Cases nachgewiesen würden, könnten der erforderliche Aufwand und die Risiken in Relation zum konkreten Nutzen gesetzt werden. Werden die Daten jedoch nicht nachgefragt, übersteigen Aufwand und Risiken den möglichen Mehrwert.

- Die Unternehmen sprechen sich dafür aus, Daten über ein Data Sharing-Modell und nicht als Open Data (und damit bedingungslos) zu teilen. Auf diese Weise können wesentliche Kontrollmechanismnen beim Datenteilen gewährleistet werden und der Zugriff von öffentlichen Verwaltungen und Dritten geregelt werden.

Schutzmechanismus zur Wahrung der Fairness:

- Die Unternehmen sehen ein asymmetrisches Machtverhältnis beim Teilen von Daten zwischen Unternehmen und öffentlichen Verwaltungen.
- Das “Quid pro quo”-Prinzip sollte zur Regel werden, wenn Daten mit öffentlichen Stellen geteilt werden. Dies bedeutet:
    - Die Unternehmen sprechen sich dafür aus, dass alle Daten zwischen den Akteuren geteilt werden, die für die Erbringung eines Dienstes erforderlich sind (im Mobilitätsbereich insbesondere kommunale Infrastrukturdaten). Dies könnte z.B. durch ein Informationszugangsgesetz (oder andernfalls ein spezifisches Zugriffsgesetz) geregelt werden.
    - Wenn die für die Erbringung eines Dienstes idealen Daten in einer Kommune nicht vorhanden sind, sollte geprüft werden, welche Daten stattdessen geteilt werden könnten.
    - Daraus resultiert auch: Die Unternehmen könnten ableiten, wenn die Stadt (basierend auf ihren Daten) Verkehrsmaßnahmen plant.

2 Datenteilen zwischen Unternehmen (B ↔ B)

Use Cases:

Für den Datenaustausch zwischen Unternehmen wurden Angreiferszenarien und Mechanismen zum Schutz von Geschäftsgeheimnissen an folgenden Use Cases diskutiert:

- Unternehmen teilen Daten organisiert über Verband mit anderen Unternehmen, um die eigene Marktposition zu evaluieren.
- Unternehmen teilen Daten untereinander, um die gegenüber dem eigenen Unternehmen ausgestellten Bußgelder (pro Fahrzeugkategorie) mit dem Wettbewerb zu vergleichen. Hintergrund ist die hohe Erfolgsquote bei Widersprüchen gegen unrechtmäßig ausgestellte Bußgeldbescheide (bis zu 50%).
- Unternehmen teilen Daten für die Dienstebereitstellung auf externen Plattformen.

Angreiferszenario: Ableitung von Informationen über die wirtschaftliche Leistungsfähigkeit

- Beim Teilen von Daten mit anderen Unternehmen besteht die Gefahr, dass Informationen über die eigene wirtschaftliche Leistungsfähigkeit an Dritte weitergegeben oder daraus abgeleitet werden können. Alle Daten, bei denen diese Möglichkeit grundsätzlich besteht, werden von den Unternehmen als Geschäftsgeheimnisse eingestuft. Solche Daten werden daher in der Regel nicht direkt an andere Unternehmen weitergegeben.
- Beispiel: Im Bereich der Shared Mobility kann z.B. von den Standzeiten eines Fahrzeugs auf den damit erzielten Umsatz geschlossen werden, da z.B. die Minutenpreise für die Nutzung eines Fahrzeugs öffentlich bekannt sind.

Angreiferszenario: Offenlegung von Wettbewerbsvorteilen

- Beim Teilen von Daten mit anderen Unternehmen besteht das Risiko, dass Wettbewerbsvorteile eines Unternehmens gegenüber Konkurrenten offengelegt oder abgeleitet werden können.
- Beispiel: Im Bereich Shared Mobility kann z.B. aus den Startpunkten der Fahrzeuge die Gebietsabdeckung eines Unternehmens ermittelt werden. Auf dieser Basis könnten Dritte z.B. bisher unbekannte “Hotspots” identifizieren und in diesen Gebieten gezielt in den Wettbewerb eintreten.

Angreiferszenario: Kartellrechtliche Risiken

- Beim Teilen von Daten mit anderen Unternehmen, z.B. zur Erstellung von Branchenberichten, Marktübersichten oder für die Öffentlichkeitsarbeit, besteht die Gefahr von Kartellrechtsverstößen. Konkret geht es um das Risiko einer Bildung von Oligopolen oder den möglichen Vorwurf eines abgestimmten Marktverhaltens.

Konsolidierung der Schutzmechanismen:

Bestätigung der Schutzmechanismen auf der Folie.

Gestaltungsspielraum im freien Wettbewerb:

- Bei der Ausgestaltung der Bedingungen für die Datenweitergabe in den Datenüberlassungsverträgen besteht nach Ansicht der Unternehmen ausreichend Spielraum, um die Risiken zu minimieren. So können die zu teilenden Daten, die Zwecke ihrer Verarbeitung sowie ggf. Regelungen für den Fall von Verstößen klar geregelt werden.

Präzisierung für das Datenteilen in (Mobility) Data Spaces:

- Die Unternehmen äußerten die Sorge, dass im Mobilitätsdatengesetz der freie Zugang zu Mobilitätsdaten festgelegt wird. Dies hätte zur Folge, dass Geschäftsgeheimnis relevante Daten zu Open Data (und damit frei zugänglich) werden und etwas reguliert werden würde, was in der Praxis bereits besser geregelt wird. In gleicher Weise sehen die Unternehmen Risiken mit Blick auf das Datenteilen in den Common European Data Spaces (CEDS) und sprechen sich daher für Data Sharing Agreements zwischen den teilenden Akteuren und gegen eine gesetzlich verordnete freie Zugänglichkeit (Open Data) aus.

Präzisierung der Aggregation zur kartellrechtlichen Konformität:

- Zum Zweck der Brancheninformation: Aufgrund kartellrechtlicher Bestimmungen dürfen Daten, die als Geschäftsgeheimnis einzustufen sind, nicht direkt zwischen Unternehmen geteilt werden. Die Aggregation der Daten durch einen Intermediär kann dieses Problem jedoch lösen. Ein solcher Mittler kann sicherstellen, dass geteilte Daten ausschließlich aggregiert an die Unternehmen zurückgespielt werden. Es müssen Daten von mindestens drei Unternehmen aggregiert werden, sodass keine Rückschlüsse auf einzelne Unternehmen gezogen werden können (etwa indem die eigenen Daten aus der Aggregation herausgerechnet werden).
- Mechanismus beim Datenteilen in Interessenverbänden: Wenn Daten innerhalb von Interessenverbänden (z.B. Bundesverbänden der Industrie) geteilt werden sollen, müssen alle betroffenen Akteure (bspw. alle relevanten Anbieter in einem

Marktsegment) angefragt werden. Um kartellrechtskonform zu agieren, erhalten alle relevanten Unternehmen im Interessenverband die aggregierten Daten bzw. die abgeleiteten Informationen unabhängig davon, ob sie selbst Daten geliefert haben.

Prototyping bei vernetzten Lösungen:

- Die Unternehmen stehen im freien Wettbewerb und stellen dennoch bilateral Daten zur Verfügung, um vernetzte, tiefenintegrierte Lösungen zu schaffen. Bei der Entwicklung vernetzter Systeme hat sich nach Aussage der Unternehmen das Prototyping als hilfreich erwiesen. Ein klar abgegrenztes Testfeld für prototypische Lösungen im Vorfeld eines möglichen Rollouts stellt einen geeigneten Schutzmechanismus dar, um die Interessen aller an einem System beteiligten Akteure auszuloten, Interessenkonflikte zu lösen und Geschäftsgeheimnisse zu schützen.

3 Datenteilen zwischen Unternehmen und Forschungsstellen (B ↔ R)

bzw. zwischen Unternehmen und der Zivilgesellschaft (B ↔ S)

Use Case:

Für den Datenaustausch zwischen Unternehmen und Forschungsstellen wurden Angreiferszenarien und Mechanismen zum Schutz von Geschäftsgeheimnissen an folgendem (bislang fiktiven) Use Case diskutiert:

- Unternehmen teilen Daten über (Beinahe-)Unfälle mit Forschungseinrichtungen oder der Öffentlichkeit. Solche Daten könnten dazu beitragen, dem Gemeinwohl zu dienen und die Auseinandersetzung mit dem gesellschaftlichen Interesse zu unterstützen. Auf Basis solcher Daten könnten beispielsweise lokale Unfallschwerpunkte identifiziert werden, die durch Stadtplanung gezielt entschärft werden könnten. Dadurch würde gesellschaftlicher Mehrwert entstehen.

Angreiferszenario Stellung in der Öffentlichkeit:

- Den Unternehmen zufolge spielen Unfallzahlen von Mobilitätsanbietern im öffentlichen Raum eine große Rolle. Dabei sehen sich die Unternehmen jedoch häufig mit Schlagzeilen konfrontiert, in denen die Daten nach Ansicht der Unternehmen verkürzt, polarisiert oder sogar gänzlich fehlleitend dargestellt werden. Dies sei zum Beispiel dann der Fall, wenn die für die Interpretation der Information entscheidenden Daten nicht ausreichend in Zusammenhang gesetzt werden (beispielsweise wenn gestiegene Unfallzahlen nicht ins Verhältnis zu einer gestiegenen Nutzung oder ins Verhältnis zu den allgemeinen Unfallzahlen gesetzt werden). Solchen Angriffen könnten Unternehmen begründet entgegentreten, indem Unfalldaten anbieterübergreifend verarbeitet werden, um auf diese Weise die Sicherheit solcher Mobilitätsformen zu kommunizieren.
- Unternehmen stehen in diesem Szenario vor der Herausforderung, dass es keine standardisierten technischen und begrifflichen Definitionen für spezifisches Verhalten (bspw. für gefährliches Fahrverhalten oder Unfälle) gibt.
    - Beispiel: Nicht alle Mieter*innen eines Fahrzeugs melden jeden Sturz mit

leichten Blessuren (z.B. Schürfwunden) in gleicher Weise als Unfall an die Anbieter. Vordergründig ist aus diesem Grund die Frage der Datenlage. Eine mögliche niederschwellige Definition eines Unfalls im Sinne eines Versicherungsfalls würde der Breite möglicher Szenarien mit einem potentiellen gesellschaftlichen Mehrwert nicht gerecht werden.

- Die Interpretation der Daten wäre daher sehr uneinheitlich. Dies wäre für die Unternehmen vor allem dann problematisch, wenn sich aufgrund unterschiedlicher Unfalldefinitionen deutliche Unterschiede in den Unfallzahlen ergeben. Dies birgt für die Unternehmen das Risiko, dass sich der Fokus der öffentlichen Interpretation vom eigentlichen Zweck des Datenteilens (Identifikation von Unfallschwerpunkten) hin zu einem Anbieter verschiebt, der im Vergleich zu seinen Wettbewerbern unfallträchtig erscheint. Die Unternehmen würden Unfalldaten daher nicht teilen, da sich eine solche Interpretation negativ auf den Geschäftsbetrieb eines Unternehmens auswirken kann.

Angreiferszenario "Blackbox Forschung":

Der Hintergrund des Szenarios ist die Überlegung, dass Daten mit verschiedenen Akteuren je nach Verwendungskontext unter bestimmten Bedingungen geteilt werden könnten. So könnte hinsichtlich einer kommerziellen Nutzung und einer Verarbeitung für Forschungszwecke dahingehend unterschieden werden, dass Forschungseinrichtungen Daten kostenlos zur Verfügung gestellt werden, um über die Beantwortung der Forschungsfragen einen gesellschaftlichen Mehrwert zu schaffen.

- Die Unternehmen stehen einer freien Bereitstellung von Daten für Forschungszwecke kritisch gegenüber. Der Grund dafür ist, dass die möglichen Use Cases in der Forschung so vielfältig sein können, dass die Risiken aufgrund der Breite möglicher Verarbeitungsszenarien nicht kalkulierbar sind.
- Demgegenüber wurde von Seiten der Unternehmen geäußert, dass der konkrete Nutzen häufig fehle. Ein konkreter Nutzen könnte den Risiken beispielsweise dann gegenübergestellt werden, wenn aus Forschungsergebnissen auch konkrete Folgen abgeleitet werden. Dies könnte im Mobilitätskontext z.B. dadurch erreicht werden, dass Ergebnisse an Kommunen weitergegeben werden, die daraufhin infrastrukturelle Anpassungen planen und umsetzen.
- Grundsätzlich bestehen jedoch seitens der Wirtschaft Vorbehalte gegenüber der Abgrenzung der Kategorie "Forschung" zu anderen Akteursgruppen mit ihren jeweiligen Interessen. Um diese Vorbehalte auszuräumen, müsste klar definiert werden, welche Institutionen unter welchen Bedingungen unter diese Kategorie fallen und entsprechend Daten verarbeiten dürfen. Dies erscheint vor dem Hintergrund der Vielzahl forschender Einrichtungen und ihrer unterschiedlichen Träger- und Finanzierungsmodelle (insbesondere Universitäten, Hochschulen und Institute in staatlicher, privater oder stiftungsrechtlicher Trägerschaft) und der daraus resultierenden Nähe zu ggf. konkurrierenden Interessengruppen durchaus risikobehaftet.

Konsolidierung der Schutzmechanismen:

Einheitlichkeit bei der Interpretation der Daten:

- Die Unternehmen haben deutlich gemacht, dass Risiken bei der Interpretation von (Unfall-)Daten nicht dadurch reduziert werden können, dass relevante Informationen aus den Daten entfernt werden. Entscheidend ist hierbei vielmehr eine einheitliche technische und begriffliche Definition eines bestimmten Verhaltens oder Ereignisses. Dies ist weniger eine Frage der Anonymisierung als vielmehr eine Frage der Datenqualität. Die notwendige Einheitlichkeit bei der Interpretation der Daten könnte durch ein gemeinsames Methodenset verbessert werden.
- Die Problematik des negativen Framings in der Öffentlichkeit lässt sich aus Sicht der Unternehmen damit jedoch nicht vollständig lösen. Daten können hier entweder nur gegen bestimmte Aussagen wirken oder diese zusätzlich untermauern. Framing im öffentlichen Diskurs findet aber auch unabhängig davon statt, ob und in welcher Qualität Daten zu einem Phänomen / zu einer bestimmten Fragestellung vorliegen.

4 Anforderungen an eine Trusted Third Party (TTP)

In Bezug auf die Datenteilungsszenarien zwischen den verschiedenen Akteuren (B ↔ G, B ↔ B, B ↔ R / S) sowie die dabei diskutierten Angreiferszenarien wurde mit den Unternehmen die Einbindung einer vertrauenswürdigen dritten Instanz (sog. Trusted Third Party / TTP) zum Schutz von Geschäftsgeheimnissen beim Teilen von Daten erörtert. Konkret wurde zusammengetragen, welche Anforderungen ein solcher Intermediär erfüllen müsste, damit Unternehmen ihre Daten trotz enthaltener Geschäftsgeheimnisse teilen würden.

Den Unternehmen zufolge müsste zuvorderst die Unabhängigkeit einer solchen Trusted Third Party dauerhaft sichergestellt sein. Dazu zählt insbesondere:

- Um Eigeninteressen (vgl. hierzu insbesondere die o.g. Angreiferszenarien) zweifelsfrei ausschließen zu können, muss die institutionelle Verankerung einer solchen Instanz transparent sein. Konkret bedeutet dies, dass sie weder politisch angebunden sein noch eigens zu diesem Zweck aus einer Branche heraus gegründet werden dürfen.
- Eine solche Instanz sollte nach neutralen Grundsätzen und transparenten Bestimmungen agieren. Sie darf nicht im Auftrag der verschiedenen Interessengruppen handeln, sondern müsste (etwa analog zur Justiz) ein unabhängiges Organ sein.
- Die Finanzierung eines solchen Intermediärs sollte zu gleichen Teilen von den Akteursgruppen selbst getragen werden. Dahinter steht die Überlegung, dass Unabhängigkeit und Neutralität nicht mehr gewährleistet werden können, sobald ein Akteur mehr oder weniger als andere an der Finanzierung beteiligt ist.
- Eine Gewinnerzielungsabsicht sollte nach Ansicht der Unternehmen für eine solche Instanz ausgeschlossen sein. Die Rechtsform einer gGmbH wird hierfür als geeignet angesehen.
- Die Unternehmen betonen, dass die grundsätzliche Anschlussfähigkeit an alle Akteure (Kommunen, Unternehmen, Wissenschaft und Zivilgesellschaft) von einer solchen Instanz gewährleistet werden muss. Eine Insellösung für bestimmte Akteure wird als nicht zielführend erachtet.

CHECK OUT

- Die Unternehmen betonten, dass es keine kategorische Abwehrhaltung gegenüber der Datenweitergabe an Dritte (insbesondere öffentliche Stellen) gebe, sondern dass es um unternehmerische Schutzinteressen gehe. Daran anschließend äußerten sie die Hoffnung, dass ein besseres Wissen über die Zusammenhänge in Datenökonomie zu einem gesteigerten Verständnis wirtschaftlicher Interessen führen würde.
- Der Forschung wird dabei eine Schlüsselrolle zugeschrieben. Gemeinsame Projekte verschiedener Akteure können nach Ansicht der Unternehmen dazu beitragen, Vertrauen zu schaffen und gemeinsam Lösungen für die zukünftig zunehmende Relevanz datenbasierter Entscheidungen zu entwickeln.