

Brüssel, den 25.4.2018  
SWD(2018) 125 final

**ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN**

**Leitfaden für die gemeinsame Nutzung von Daten des Privatsektors in der europäischen  
Datenwirtschaft**

*Begleitunterlage zur*

**Mitteilung der Europäischen Kommission an das Europäische Parlament, den Rat, den  
Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen**

**„Aufbau eines gemeinsamen europäischen Datenraums“**

{COM(2018) 232 final}

## 1. Einleitung

Die datengesteuerte Innovation trägt in Europa wesentlich zu Wachstum und Beschäftigung bei. Die Bedeutung der Online-Datenerhebung, die wachsende Verbreitung von Daten, die von mit dem Internet der Dinge (IoT) verbundenen Objekten generiert werden, die zunehmende Verfügbarkeit von Instrumenten für die Auswertung riesiger Datenmengen (*Big Data Analytics*) und die aufkommende breite Verfügbarkeit bestimmter Anwendungen der künstlichen Intelligenz sind wesentliche technische Triebkräfte. Da Daten keine Konkurrenzprodukte sind und identische Daten folglich für eine ganze Palette neuer Produkte oder Dienstleistungen oder neuer Produktionsverfahren verwendet werden können, liegt es nahe, dass es für Unternehmen effizient sein kann, mehr Daten, die sie zusammen mit anderen Unternehmen besitzen, auch gemeinsam zu nutzen, sodass der mit den Daten verbundene Wert maximal ausgeschöpft werden kann.

Neue datengesteuerte Geschäftsmodelle, die sich auf diese technischen Triebkräfte stützen, stellen nicht nur für große Unternehmen, sondern auch für KMU und Start-ups in Europa eine Chance dar. Ebenso beginnt auch der öffentliche Sektor, die Chancen der datengesteuerten Innovation zu ergreifen. Schon jetzt profitieren Unternehmen vom Zugang zu Informationen des öffentlichen Sektors, die als offene Daten<sup>1</sup> verfügbar sind, sowie vom gegenseitigen Datenaustausch. Gleichwohl sehen sich KMU und Start-ups noch immer Hindernissen gegenüber, wenn sie selbst ihre Daten bereitstellen oder Daten von anderen Unternehmen weiterverwenden. Dies ist insbesondere dann der Fall, wenn es sich um maschinengenerierte, nicht personenbezogene Daten handelt. Analog dazu müssen öffentliche Stellen ihre Abläufe modernisieren und das Potenzial neuer Datenquellen ausschöpfen, um stärker datengesteuert und kosteneffizienter zu werden. Dies dürfte den Bürgern und Unternehmen, darunter insbesondere den KMU, zugutekommen. Während in bestimmten Fällen relevante datengestützte Dienstleistungen auf dem Markt verfügbar sind, kann es für den öffentlichen Sektor bisweilen erforderlich sein, Daten von einem Privatunternehmen direkt zu analysieren oder einen geregelten Datenerwerb einzurichten, z. B. zur Erstellung amtlicher Statistiken. Aufgrund von Bedenken hinsichtlich der Vertraulichkeit von Daten oder wahrgenommenen Risiken für die Geschäftsinteressen von Unternehmen werden solche Daten mitunter für den öffentlichen Sektor nicht zugänglich gemacht. Damit sind Fragen der Bereitstellung und der (Weiter-)Verwendung von Daten („gemeinsame Datennutzung“) im Rahmen zweier Konstellationen zu betrachten, d. h. in Geschäftsbeziehungen zwischen Unternehmen („B2B“) sowie in Beziehungen zwischen Unternehmen und Behörden/öffentlichem Sektor („B2G“).

Die Kommission hat bereits Maßnahmen vorgeschlagen, um die Verfügbarkeit von Daten für Unternehmen zu verbessern. Mit der Datenschutz-Grundverordnung (DSGVO) und der e-Datenschutz-Richtlinie<sup>2</sup> hat die EU einen robusten Rahmen für die Verarbeitung personenbezogener Daten und elektronischer Kommunikationsdaten eingerichtet, der Vertrauen im digitalen Umfeld schaffen und damit eine Grundvoraussetzung für die gemeinsame Datennutzung erfüllen soll. Durch den Rahmen entsteht die Basis für einen

---

<sup>1</sup> Auch über das Europäische Datenportal: <https://www.europeandataportal.eu/de/homepage>.

<sup>2</sup> Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37). Siehe auch: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), COM(2017) 10 final vom 10. Januar 2017.

künftigen Wettbewerbsvorteil europäischer Wirtschaftsakteure, wenn es darum geht, Datentechnologien optimal zu nutzen. Darüber hinaus wird es durch den Vorschlag für eine Verordnung über den freien Verkehr nicht personenbezogener Daten<sup>3</sup> einfacher werden, solche Daten innerhalb der EU zu übertragen.

In ihrer Mitteilung „Aufbau einer europäischen Datenwirtschaft“ vom 10. Januar 2017<sup>4</sup> hat die Kommission erstmals auf mögliche Probleme beim Datenzugang hingewiesen, die insbesondere von Maschinen generierte Daten und die Beziehungen zwischen Plattformen und Unternehmen betreffen. Ebenso wurde die Bedeutung des Zugangs zu Daten des Privatsektors für im öffentlichen Interesse liegende Zwecke aufgegriffen.

Auf der Grundlage dieser Mitteilung wurde ein breiter Dialog mit den Interessenträgern geführt. Dabei wurde festgestellt, dass der zentrale Sachverhalt gegenwärtig keine horizontalen legislativen Maßnahmen rechtfertigt und ein Leitfaden angemessener wäre.<sup>5</sup>

In der Mitteilung, die durch die vorliegende Arbeitsunterlage der Kommissionsdienststellen ergänzt wird<sup>6</sup>, legt die Kommission eine Reihe von Grundsätzen fest, die zu beachten sind, damit Dateninteraktionen zwischen Unternehmen sowie zwischen Unternehmen und Behörden für alle Beteiligten erfolgreich verlaufen.

Darüber hinaus soll diese Arbeitsunterlage der Kommissionsdienststellen einen „Werkzeugkasten“ für jene Unternehmen darstellen, die gleichzeitig Dateninhaber und Datennutzer sind. Daher umfasst sie einen Leitfaden zu rechtlichen, geschäftlichen und technischen Aspekten der gemeinsamen Datennutzung, der sich in der Praxis anwenden lässt, wenn Datenübertragungen zwischen Unternehmen desselben Sektors oder verschiedener Sektoren erwogen und vorbereitet werden.

Die Leitlinien in diesem Dokument richten sich an alle Sektoren der Wirtschaft. Infolge der unterschiedlichen Struktur der einzelnen Märkte müssten diese möglicherweise durch sektorspezifische Maßnahmen ergänzt werden.

Das Dokument stellt jedoch keine Aussage über die Rechtslage dar und greift auch nicht die Auslegung des EU-Rechts durch den Gerichtshof der Europäischen Union (EuGH) vor. Für die Kommission schafft das Dokument keinerlei Verpflichtung in Bezug auf die Anwendung des EU-Rechts, insbesondere nicht im Hinblick auf die Wettbewerbsvorschriften nach Artikel 101 und 102 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV).

## **2. Grundsätze für die gemeinsame Datennutzung zwischen Unternehmen („B2B“) und Unternehmen und Behörden („B2G“)**

**Um faire Märkte für IoT-Objekte sowie für Produkte und Dienstleistungen, die auf von solchen Objekten erzeugten Daten beruhen, zu gewährleisten,** sind in der Mitteilung, die durch diese Arbeitsunterlage der Kommissionsdienststellen ergänzt wird<sup>7</sup>, die folgenden Grundsätze festgelegt worden:

---

<sup>3</sup> COM(2017) 495 final.

<sup>4</sup> COM(2017) 9 final.

<sup>5</sup> <https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-building-european-data-economy>

<sup>6</sup> COM(2018) 232.

<sup>7</sup> COM(2018) 232.

a) **Transparenz:** Aus den einschlägigen Verträgen sollte auf transparente und verständliche Art und Weise ersichtlich sein, i) welche Personen oder Einrichtungen Zugang zu den durch das Produkt oder die Dienstleistung erzeugten Daten haben, sowie die Art und Detailliertheit dieser Daten und ii) zu welchem Zweck diese Daten verwendet werden.

b) **Gemeinsame Wertschöpfung:** In den einschlägigen Verträgen sollte anerkannt werden, dass mehrere Beteiligte zur Erzeugung der Daten beigetragen haben, wenn Daten als Nebenprodukt der Verwendung eines Produkts oder einer Dienstleistung anfallen.

c) **Gegenseitige Achtung der Geschäftsinteressen aller Beteiligten:** Die einschlägigen Verträge sollten der Notwendigkeit Rechnung tragen, dass geschäftliche Interessen und Geheimnisse sowohl der Dateninhaber als auch der Datennutzer zu schützen sind.

d) **Gewährleistung eines unverfälschten Wettbewerbs:** Die einschlägigen Verträge sollten der Notwendigkeit Rechnung tragen, beim Austausch sensibler Geschäftsinformationen einen unverfälschten Wettbewerb zu wahren.

e) **Minimierung der Datenabhängigkeit von einem Anbieter:** Unternehmen, die Produkte oder Dienstleistungen anbieten, die Daten als Nebenprodukt generieren, sollten so weit wie möglich die Datenübertragbarkeit erlauben und ermöglichen.<sup>8</sup> Zudem sollten sie, soweit möglich und entsprechend den Merkmalen des Marktes, auf dem sie tätig sind, in Betracht ziehen, dasselbe Produkt oder dieselbe Dienstleistung jeweils sowohl mit Datentransfer als auch ohne oder mit nur begrenztem Datentransfer anzubieten.

Zudem heißt es in der Mitteilung, dass **Daten des Privatsektors öffentlichen Stellen** für eine Weiterverwendung zu Vorzugsbedingungen leichter bereitgestellt werden könnten, wenn die folgenden Grundsätze eingehalten werden:

a) **Verhältnismäßigkeit bei der Verwendung von Daten des Privatsektors:** Anträge auf Bereitstellung von Daten des Privatsektors für die Weiterverwendung zu Vorzugsbedingungen sollten durch ein klares und nachweisbares öffentliches Interesse gerechtfertigt sein. Der Antrag sollte angemessen, für das öffentliche Interesse zweckdienlich und im Hinblick auf Detailliertheit, Relevanz und Datenschutz verhältnismäßig sein. Kosten und Aufwand der Bereitstellung und Weiterverwendung von Daten des Privatsektors sollten in einem angemessenen Verhältnis zum erwarteten Nutzen für die Öffentlichkeit stehen.

b) **Zweckbindung:** Die Verwendung von Daten des Privatsektors sollte eindeutig auf einen oder mehrere Zwecke beschränkt sein, die in den vertraglichen Bestimmungen über die Zusammenarbeit zwischen Unternehmen und Behörden möglichst eindeutig festzulegen sind. Dies kann auch eine befristete Datennutzungsdauer einschließen. Dem Unternehmen des Privatsektors sollte gesondert zugesichert werden, dass die erlangten Daten nicht in anderen Verwaltungs- oder Gerichtsverfahren verwendet werden; die strengen rechtlichen und ethischen Bestimmungen für die statistische Geheimhaltung im Europäischen Statistischen System könnten in dieser Hinsicht als Muster dienen.

c) **Schadensvermeidung:** Bei der Datenzusammenarbeit zwischen Unternehmen und Behörden muss gewährleistet sein, dass berechnete Interessen, insbesondere der Schutz von Geschäftsgeheimnissen und anderen vertraulichen Geschäftsinformationen, gewahrt werden.

---

<sup>8</sup> Beispielsweise Daten, die von Robotern im Zusammenhang mit industriellen Prozessen erzeugt werden und für den Kundendienst (Reparatur und Wartung) von Bedeutung sind, oder Daten über die Bewertung von Dienstleistern.

Die Datenzusammenarbeit von Unternehmen und Behörden sollte es den Unternehmen weiterhin ermöglichen, die aus den fraglichen Daten abgeleiteten Erkenntnisse bei anderen Interessenten gewinnbringend zu verwerten.

**d) Bedingungen für die Weiterverwendung:** Vereinbarungen über die Datenzusammenarbeit zwischen Unternehmen und Behörden sollten für beide Seiten von Vorteil sein und gleichzeitig dem öffentlichen Interesse dienen, indem sie den öffentlichen Stellen Vorzugsbedingungen gegenüber anderen Kunden sichern.

Dies sollte sich insbesondere in der Höhe der vereinbarten Entschädigung niederschlagen, die mit dem verfolgten öffentlichen Interesse verknüpft werden könnte.

Vereinbarungen über die Datenzusammenarbeit zwischen Unternehmen und Behörden, an denen dieselben Behörden beteiligt sind, die dieselben Aufgaben wahrnehmen, sollten diskriminierungsfrei behandelt werden.

Vereinbarungen über die Datenzusammenarbeit zwischen Unternehmen und Behörden sollten den Bedarf an anderen Arten der Datenerhebung wie Umfragen verringern. Dadurch sollte die Gesamtbelastung für Bürger und Unternehmen abnehmen.

**e) Umgang mit Beschränkungen in Daten des Privatsektors:** Um mögliche qualitative Beschränkungen in Daten des Privatsektors, einschließlich möglicher Verzerrungen, zu verringern, sollten Unternehmen, die Daten liefern, auch eine zumutbare und verhältnismäßige Unterstützung anbieten, um die Bewertung der Qualität der Daten für die angegebenen Zwecke zu erleichtern. Dazu gehört auch die Möglichkeit, die Daten gegebenenfalls zu kontrollieren oder anderweitig nachzuprüfen. Unternehmen sollten nicht verpflichtet sein, die Qualität der betreffenden Daten zu verbessern. Öffentliche Stellen sollten ihrerseits sicherstellen, dass Daten aus verschiedenen Quellen so verarbeitet werden, dass eine mögliche auswahlbedingte Verzerrung vermieden wird.

**f) Transparenz und Einbeziehung der Gesellschaft:** Die Zusammenarbeit zwischen Unternehmen und Behörden sollte hinsichtlich der Vertragsparteien und ihrer Ziele transparent sein. Von öffentlichen Stellen erlangte Erkenntnisse und bewährte Verfahren für die Zusammenarbeit zwischen Unternehmen und Behörden sollten öffentlich bekannt gemacht werden, sofern die Vertraulichkeit der Daten dadurch nicht gefährdet wird.

### **3. Gemeinsame Datennutzung zwischen Unternehmen (B2B) – ein Leitfadens**

Die Bereitstellung und Weiterverwendung von Daten zwischen Unternehmen kann in zahlreichen Formen erfolgen, was technische Verfahren, zugrunde liegende Geschäftsmodelle und das Rechtsinstrument, auf dem die Regelungen für die gemeinsame Datennutzung basieren, angeht. In diesem Abschnitt werden einige Formen ausführlicher beschrieben.

#### **3.1 Modelle für die gemeinsame Datennutzung zwischen Unternehmen**

Die zugrunde liegenden Geschäftsmodelle für die gemeinsame Datennutzung können sich recht stark unterscheiden und richten sich in hohem Maße nach den jeweiligen Datenarten und dem strategischen Geschäftsinteresse. Sie können von einem Open-Data-Ansatz bis hin zu exklusiven Datenpartnerschaften mit nur einer Partei reichen:

- a) **Open-Data-Ansatz:** Ein solches Konzept der offenen Daten, in dessen Rahmen die jeweiligen Daten vom Datenlieferanten einem prinzipiell offenen Kreis von (Weiter-

)Verwendern mit möglichst wenig Einschränkungen und entweder ohne oder gegen äußerst geringes Entgelt bereitgestellt werden, ist möglich, wenn der Datenlieferant ein großes Interesse an der Weiterverwendung der Daten hat. Dies gilt beispielsweise für Dienstleister, die das Ökosystem eines dritten Anwendungsentwicklers nutzen wollen, um ihre Endkunden zu erreichen.

- b) **Gewinnbringende Verwertung der Daten auf einem Datenmarktplatz:** Die gewinnbringende Verwertung von Daten bzw. der Datenhandel kann über einen Datenmarktplatz aufgrund bilateraler Verträge gegen Entgelt erfolgen. Dies kann sich für Unternehmen lohnen, die keine potenziellen Weiterverwender ihrer Daten kennen und auf eine einmalige gewinnbringende Verwertung ihrer Daten abzielen. Eine solche Verfahrensweise erscheint möglich, sofern 1) die Risiken einer unrechtmäßigen Verwendung der jeweiligen Daten begrenzt sind, 2) der Datenlieferant dem (Weiter-)Verwender vertrauen kann, oder 3) der Datenlieferant über technische Verfahren verfügt, um eine unrechtmäßige Verwendung zu verhindern oder zu erkennen. Durch Mustervertragsbedingungen lassen sich die Kosten senken, die mit der Ausarbeitung von Datennutzungsvereinbarungen verbunden sind.
- c) **Datenaustausch über eine geschlossene Plattform:** Der Datenaustausch kann über eine geschlossene Plattform erfolgen, die entweder von einem Hauptakteur in einer Umgebung für die gemeinsame Datennutzung oder einem unabhängigen Vermittler eingerichtet wird. Die Daten können dabei gegen Entgelt oder beispielsweise gegen innerhalb der Plattform erbrachte Mehrwertdienste bereitgestellt werden. Diese Lösung ermöglicht es, Mehrwertdienste anzubieten, und bietet damit eine komplexere Lösung für stabilere Datenpartnerschaften. Außerdem sind so mehr Mechanismen für die Kontrolle der Datenverwendung möglich, während Mustervertragsbedingungen die Kosten senken können, die mit der Ausarbeitung von Datennutzungsvereinbarungen verbunden sind. Ist die gemeinsame Datennutzung exklusiv, sind dabei die Wettbewerbsvorschriften einzuhalten.<sup>9</sup>

Ebenso sind Variationen und Kombinationen dieser Modelle möglich, die an den jeweiligen kommerziellen Bedarf anzupassen sind. Der Begriff „gemeinsame Datennutzung“ wird verwendet, um alle potenziellen Formen und Modelle zu beschreiben, nach denen der Datenzugang bzw. die Datenübertragung zwischen Unternehmen erfolgt.

### **3.2 Rechtliche Aspekte der gemeinsamen Datennutzung: Vereinbarungen über die Datennutzung oder -lizenzierung**

Die gemeinsame Datennutzung zwischen Unternehmen erfolgt in der Regel auf einer vertraglichen Grundlage. In Vereinbarungen über die Nutzung bzw. Lizenzierung von Daten vereinbaren die Parteien den Gegenstand und Wert des Vertrags sowie alle anderen Modalitäten, die in die Vertragsbedingungen einfließen. Vereinbarungen über die gewinnbringende Verwertung von Daten können nicht nur bilateral sein, sondern auch zwischen mehreren Parteien geschlossen werden.

---

<sup>9</sup> Siehe hierzu die Leitlinien der Kommission für vertikale Beschränkungen (ABl. C 130 vom 19.5.2010, S. 1) sowie die Erläuterungen zu den Prioritäten der Kommission bei der Anwendung von Artikel 82 des EG-Vertrags [nunmehr Artikel 102 AEUV] auf Fälle von Behinderungsmissbrauch durch marktbeherrschende Unternehmen (ABl. C 45 vom 24.2.2009, S. 7).

Die einschlägigen Bedingungen in Vereinbarungen über die Datennutzung bzw. -lizenzierung sind besonders sorgfältig festzulegen, damit bestehende und insbesondere solche Rechtsvorschriften eingehalten werden, die dem Datenaustausch entgegenstehen oder ihn besonderen Auflagen unterwerfen, und sichergestellt ist, dass die strategischen Interessen aller Parteien und der Wettbewerb gewahrt bleiben.

Derzeit werden bereits Mustervertragsbedingungen für verschiedene Vereinbarungen über eine gemeinsame Datennutzung sowie für bestimmte Sektoren bzw. Formen der gemeinsamen Datennutzung ausgearbeitet. Über ein Unterstützungszentrum für die gemeinsame Datennutzung, das Anfang 2019 die Arbeit aufnehmen soll, plant die Kommission derzeit, bewährte Verfahren, bestehende Mustervertragsbedingungen und Checklisten zusammenzutragen.<sup>10</sup>

Die folgenden Überlegungen können Unternehmen bei der Vorbereitung und/oder Aushandlung von Datennutzungsvereinbarungen helfen:

a) Welche Daten sollen bereitgestellt werden?

- Beschreiben Sie die Daten, die Sie teilen möchten, so konkret und präzise wie möglich (z. B. FuE-Daten, Kundendaten, Diagnosedaten), darunter auch das Ausmaß der künftig zu erwartenden Aktualisierungen. Sofern Auslegungsressourcen, die eine Analyse ermöglichen (wie Verfahren und Modelle), zusammen mit Datensätzen genutzt werden, sind diese zu beschreiben.
- Welche Qualitätsstufe kann für die Daten – auch im Laufe der Zeit – gewährleistet werden? Gemeinsam genutzte Daten müssen von guter Qualität, d. h. akkurat, zuverlässig und gegebenenfalls aktuell, sein. Stellen Sie sicher, dass keine Daten fehlen, doppelt vorhanden oder unstrukturiert sind. Geben Sie die Quelle/Herkunft der Daten sowie die Art ihrer Erfassung bzw. Zusammenstellung an. Gegebenenfalls kann ein Verfahren für die Meldung von Fehlern in den Daten eingerichtet werden.
- Geht es bei der gemeinsamen Datennutzung um einen Datensatz oder einen Datenstrom?
- Stellen Sie sicher, dass alle rechtlichen Verpflichtungen eingehalten werden, die dem Zugang zu den Daten bzw. der Übertragung der Daten an Dritte entgegenstehen können. Beachten Sie potenzielle Rechte, die Dritte an den Daten haben könnten. Überprüfen Sie die Rechte an den von den Daten verkörperten Inhalten (Rechte des geistigen und gewerblichen Eigentums).
- Stellen Sie die Einhaltung der Datenschutzvorschriften sicher. Überprüfen Sie unter anderem, ob eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten vorhanden ist, die mit der Datenschutz-Grundverordnung vereinbar ist.

b) Wer kann auf die Daten zugreifen und diese (weiter-)verwenden?

- Stellen Sie sicher, dass im Vertrag auf transparente, klare und verständliche Weise festgelegt ist, wer das Recht hat, auf die Daten zuzugreifen, die Daten (weiter) zu verwenden und die Daten zu verbreiten und unter welchen Auflagen. Geben Sie an, ob und wie Daten für die Weiterverwendung lizenziert werden können. Erläutern Sie

---

<sup>10</sup> Siehe hierzu den Anhang des Durchführungsbeschlusses der Kommission über die Annahme des Arbeitsprogramms für 2018 und über die Finanzierung des Bereichs Telekommunikation der Fazilität „Connecting Europe“ (CEF), S. 42.

die Bedingungen von Lizenzen für die Weiterverwendung und Verbreitung von Daten auf verständliche Weise. Ebenso ist der Bedarf an Unterlizenzierungen zu klären: Solche sind entweder ausdrücklich auszuschließen, oder es sind die Bedingungen, unter denen sie zulässig sind, sowie die hierfür infrage kommenden Datenarten anzugeben.

- Das Recht auf Zugang zu und (Weiter-)Verwendung von Daten muss nicht unbeschränkt sein. In der Vereinbarung kann beispielsweise das Zugangsrecht eingeschränkt und bestimmten Berufsgruppen wie Landwirten vorbehalten werden. Ebenso können bestimmte Verwendungszwecke für die Daten festgelegt werden, wie die begrenzte gewerbliche Nutzung.
- c) Was darf der (Weiter-)Verwender mit den Daten machen?
- Der (Weiter-)Verwender sollte bei den Vertragsverhandlungen so offen und verständlich wie möglich darlegen, wie die Daten verwendet werden, darunter auch die Verwendung durch nachgelagerte Parteien. Dies stellt Transparenz sicher und erhöht das Vertrauen des Datenlieferanten.
  - Geben Sie genau an, wozu die Daten verwendet werden können, darunter auch Rechte an Derivaten der Daten (Analytik).
  - Legen Sie Regeln zur Nichtoffenlegung in Bezug auf nachgelagerte Parteien fest.
- d) Legen Sie die technischen Mittel für den Datenzugang und/oder -austausch fest, darunter auch die
- Häufigkeit des Datenzugangs und maximale Datenmengen;
  - die IT-Sicherheitsanforderungen;
  - den Leistungsumfang für Unterstützung.
- e) Welche Daten muss ich schützen und wie?
- Stellen Sie sicher, dass angemessene Schutzmaßnahmen für Ihre Daten bestehen. Diese Maßnahmen sollten auf die Vorgänge der gemeinsamen Datennutzung und auf die Datenspeicherung angewendet werden, da Daten von organisierten kriminellen Vereinigungen und einzelnen Hacker gestohlen oder missbraucht werden können. Daten können auch versehentlich offengelegt werden, etwa durch menschliches Versagen oder technische Probleme. Ebenso können Daten einem unbefugten Zugang oder einer unbefugten Offenlegung unterliegen oder verloren gehen.
  - Stellen Sie sicher, dass Geschäftsgeheimnisse, sensible gewerbliche Informationen, Lizenzen, Patente und Rechte des geistigen Eigentums geschützt werden. Keine Partei darf einen Datenaustausch ausnutzen, um von der anderen Partei sensible Informationen zu erhalten.
- f) Legen Sie Haftungsregelungen fest, sofern fehlerhafte Daten bereitgestellt werden, die Datenübertragung unterbrochen wird, die Auswertung von geringer Qualität ist, falls diese Auswertung zusammen mit den Datensätzen weitergegeben wird, oder es zu Zerstörung/Verlust oder Veränderungen der Daten (sofern unrechtmäßig oder zufällig) kommt, die Schäden verursachen können.
- g) Legen Sie die Rechte beider Parteien in Bezug auf die Durchführung von Prüfungen der Einhaltung gegenseitiger Verpflichtungen fest.

- h) Welche Laufzeit soll der Vertrag haben? Wie sieht es mit den Rechten für die Kündigung des Vertrags aus? Welche Kündigungsfrist sollten gegenüber Ihren Partnern gelten?
- i) Vereinbaren Sie das geltende Recht und Verfahren für die Streitbeilegung.

### 3.3 Die technischen Aspekte der gemeinsamen Datennutzung

Es gibt eine Reihe technischer Verfahren für die gemeinsame Datennutzung zwischen Unternehmen. Einige dieser Verfahren können Regeln für die Datennutzung umfassen und gleichzeitig eine vertrauenswürdige und sichere Umgebung für den Austausch von Datensätzen bieten.<sup>11</sup>

Dabei ist zwischen drei Verfahren zu unterscheiden: a) der Dateninhaber macht bestimmte Daten direkt einer größeren Zahl von Weiterverwendern zugänglich, beispielsweise über eine Anwendungsprogrammierschnittstelle (API); b) der Dateninhaber macht bestimmte Daten über einen Vermittler (einen Datenmarktplatz) einem oder mehreren Weiterverwendern zugänglich, bei eingeschränkter Kontrolle über die anschließende Verwendung; c) der Dateninhaber macht bestimmte Daten in einer Umgebung, die eine stärkere Kontrolle und Rückverfolgbarkeit der anschließenden Verwendung ermöglicht, über einen Vermittler (Datenraum oder -plattform) einem oder mehreren Weiterverwendern zugänglich.

- a) **Gemeinsame Datennutzung mit einem Anbieter und vielen Nutzern über eine Anwendungsprogrammierschnittstelle (API) oder eine industrielle Datenplattform:** Bestimmte Unternehmen, die mit anderen Unternehmen Dateninteraktionen betreiben, nutzen unilaterale Verfahren, um technisch einen Datenzugang zu ermöglichen. Beispiele sind APIs oder besondere Plattformen, die für Speicherung, Verarbeitung und Austausch von Daten eingerichtet werden.

Die Schaffung eines Datenzugangs für Dritte über öffentliche APIs – d. h. APIs, die einer breiteren Öffentlichkeit und nicht nur Beteiligten innerhalb derselben Organisation offenstehen – ist immer häufiger zu beobachten. Die Zahl der APIs ist seit 2010 stark angestiegen, und dieser Trend setzt sich fort.<sup>12</sup>

APIs können insbesondere kleineren Unternehmen ermöglichen, Geschäftsdaten problemlos zu verwenden bzw. weiterzuverwenden. Benutzerfreundliche und wohl durchdachte APIs tragen dazu bei, Ökosysteme zu schaffen und auf neue und innovative Produkte auszudehnen, die auf bereits vorhandene Datenbestände zurückgreifen.

APIs können die Interoperabilität erleichtern und es beispielsweise Softwareanwendungen ermöglichen, Datensätze und Datenströme untereinander auszutauschen.<sup>13</sup> Überdies können APIs selbst Spezifizierungen der Datensätze enthalten und auf technischer Ebene die Verwaltung von Zugangsrechten übernehmen.

---

<sup>11</sup> Die beschriebenen Verfahren und Beispiele wurden einer Studie zur gemeinsamen Datennutzung zwischen Unternehmen in Europa entnommen, die von Everis im Auftrag der Kommission durchgeführt wurde (Bericht steht noch aus).

<sup>12</sup> <http://www.programmableweb.com/api-research>

<sup>13</sup> Weiterführende Informationen enthält der vom Share PSI-Netzwerk, das von der Europäischen Kommission unter dem Rahmenprogramm für Wettbewerbsfähigkeit und Innovation kofinanziert wird, entwickelte Leitfaden zu APIs. <http://www.w3.org/TR/dwbp/#useanAPI>.

Auf dieser Grundlage ermutigt die Kommission<sup>14</sup> Unternehmen in ganz Europa, die breitere Nutzung offener, standardisierter und gut dokumentierter APIs zu erwägen. Dies könnte auch die Bereitstellung von Daten in maschinenlesbaren Formaten mit den zugehörigen Metadaten beinhalten.

**TomTom** ist ein niederländischer Anbieter von Verkehrs- und Navigationssystemen und Kartenprodukten. Laut einer von der Kommission finanzierten Studie<sup>15</sup> erzielt das Unternehmen seine Einnahmen zu einem Großteil mit Daten (Karten und Online-Dienste), die es an andere Unternehmen lizenziert.

TomTom bietet Anwendungsprogrammierschnittstellen<sup>16</sup> für Entwickler, um einen Datenzugang zu ermöglichen.

Laut TomTom hat dies gegenüber anderen technischen Mitteln für die gemeinsame Datennutzung folgende Vorteile:

- einfacher und schneller Datenzugang,
- Überwachung der Datenverwendung,
- Überprüfung von Vertragsverletzungen,
- schnelle Reaktionsmöglichkeit bei Datenmissbrauch (d. h. Kündigung oder Aussetzung des Datenzugangs).

Ebenso entwickeln insbesondere größere Unternehmen **gesonderte Datenplattformen**, um regelmäßige Dateninteraktionen mit Dritten zu steuern. Diese bieten zusätzliche Funktionen für den Datenaustausch (insbesondere in zwei Richtungen), die Speicherung innerhalb der Plattform und für zusätzliche, neben den Daten erbrachten Leistungen (anhand von Datenanalytik).

**Airbus** ist ein multinationales europäisches Unternehmen, das zivile und militärische luftfahrttechnische Erzeugnisse konstruiert, herstellt und verkauft.

Nachdem Airbus Behörden und Geschäftspartnern bereits über verschiedene Verfahren Daten zur Verfügung gestellt hat, startete das Unternehmen im Juni 2017 Skywise<sup>17</sup> – eine „offene digitale Datenplattform für die Luftfahrt“.

Kundenunternehmen stellen Daten als Gegenleistung für auf Datenanalytik basierende Dienstleistungen zur Verfügung.

Hauptvorteil dieses auf Hadoop-Software basierenden technischen Ansatzes ist die nahtlose Integration in die bestehenden IT-Infrastrukturen der Fluggesellschaften. Dies erleichtert es den Teilnehmern, ihre Daten auf der Plattform zur Verfügung zu stellen. Airbus indes kann auf Basis des ursprünglichen Dateiformats arbeiten und mithilfe gängiger Tabellen- und Visualisierungswerkzeuge über die Plattform Erkenntnisse bereitstellen.

**b) Gewinnbringende Verwertung der Daten über einen Datenmarktplatz mit vielen Anbietern und vielen Nutzern:** Der Begriff „Datenmarktplatz“ wird hier verwendet, um

<sup>14</sup> COM(2017) 9 final.

<sup>15</sup> Everis, Studie zur gemeinsamen Datennutzung zwischen Unternehmen in Europa (Veröffentlichung in Kürze)

<sup>16</sup> <https://developer.tomtom.com/tomtom-maps-apis-developers>

<sup>17</sup> <https://services.airbus.com/maintenance/expertise-and-other-services/skywise/skywise>

einen bestimmten Vermittler zu bezeichnen, der drei wesentliche Funktionen haben kann: 1) Zusammenführung des potenziellen Datenlieferanten und des Datenkäufers; dies kann spezifische Konstellationen umfassen, in deren Rahmen der potenzielle Lieferant und der potenzielle Käufer in der ersten Phase zur Vorbereitung der Datenübertragung anonym bleiben können, zumal durch die Bereitstellungs- bzw. Kaufabsicht bereits Geschäftsgeheimnisse offengelegt werden können (künftige Geschäftsstrategien); 2) die eigentliche Übertragung der Daten (und der vereinbarten Vergütung), darunter insbesondere die Zusicherung, dass der Verhandlungsgegenstand im Laufe der Verhandlungen nicht verändert wird; 3) Zertifizierungsfunktion, wonach die Transaktion tatsächlich erfolgt ist und gegebenenfalls in die Unternehmensbilanz einfließen kann. Zudem können solche Vermittler weitere Dienstleistungen erbringen, wie Mustervertragsklauseln oder Anonymisierungsdienste (sofern personenbezogene oder vertrauliche Daten ausgetauscht werden). Die Aufgabe solcher Vermittler endet, nachdem die Daten übertragen wurden.

**DAWEX**<sup>18</sup> ist ein französisches Unternehmen, das sich selbst als einen 2015 gegründeten „globalen Datenmarktplatz“ bezeichnet.

Dawex kauft bzw. verkauft keine Daten. Stattdessen bringt Dawex Unternehmen zusammen, die an der gewinnbringenden Verwertung und Weiterverwendung von Daten interessiert sind, und fördert die Transparenz zwischen Datenlieferanten und -nutzern, indem sichergestellt wird, dass diese kommunizieren und die Transaktion direkt über die Plattform ausführen.

Dawex hat eine Reihe von Werkzeugen entwickelt, um Datenlieferanten und -nutzern zu helfen, die Daten zu verstehen, zu bewerten und sich hierüber auszutauschen. Visualisierungswerkzeuge (z. B. Heatmaps und Kacheldiagramme) verschaffen Datennutzern verschiedene Informationen über einen vollständigen Datensatz, der sich vor Abschluss einer Transaktion sicher gemeinsam nutzen lässt. Stichprobeninstrumente generieren automatisch auf Algorithmen basierende repräsentative Datenstichproben, um störende Rückschlüsse zu vermeiden. Datennutzer und -lieferanten kommunizieren mithilfe einer in die Plattform eingebetteten Nachrichtenübermittlungsfunktion. Darüber hinaus unterstützt DAWEX die Aushandlung der Verträge gemäß Musterbedingungen, die automatisch generiert werden können.

- c) **Gemeinsame Datennutzung über einen technischen Dienstleister:** Anders als die vorgenannten Vermittler konzentrieren sich solche technischen Dienstleister im Wesentlichen darauf, neben dem Datenaustausch weitere Dienstleistungen zu erbringen, darunter die Verarbeitung der relevanten Daten zur Erfüllung bestimmter geschäftlicher Bedürfnisse oder Anliegen. Vor allem aber würde ein solcher Vermittler weitere Funktionen bieten, mit denen der Datenlieferant die Verwendung der Daten kontrollieren könnte, darunter insbesondere die Einhaltung der Bestimmungen der Vereinbarung über die Datenübertragung. Dies kann Formen einer Rückverfolgung der erfolgten Datennutzung beinhalten, wie der Protokollierung sämtlicher Datenzugriffe und Verarbeitungsvorgänge. Dabei könnten die Distributed-Ledger-Technologie (*Blockchain*) angewendet oder Formen des digitalen Wasserzeichens (*Digital Watermarking*) entwickelt werden. Schließlich könnte der Vermittler innerhalb der Gemeinschaft der Datenraum- bzw. Plattformnutzer ebenfalls Instanzen der Selbstregulierung aufbauen und

<sup>18</sup> <https://www.dawex.com/de/>

dabei eine Reihe von Sanktionen für Datennutzer, die gegen einzelne Datenübertragungsvereinbarungen verstoßen, vorsehen.

**Nallian**<sup>19</sup> hat eine cloudgestützte Plattform geschaffen, die eine gemeinsame Datennutzung in Echtzeit ermöglicht und die Prozesssynchronisierung unterstützt. Das Unternehmen setzt eine grundlegende technologische Ebene für die gemeinsame Datennutzung ein, die sich anpassen lässt, um die Bedürfnisse von Datennutzern in bestimmten Gemeinschaften oder Bereichen zu erfüllen. Die Plattform basiert auf Cloud-Technik in Kombination mit einem Werkzeug für die Verwaltung von Gemeinschaften.

Die gegenwärtigen Nutzer der technischen Lösung von Nallian sind Unternehmen, die im Logistikbereich, in vertikalen Lieferketten sowie in multimodalen Verkehrsnetzen operieren. Für diese Unternehmen ist offenbar die Fähigkeit entscheidend, Fragmentierungsprobleme zu lösen und Daten nahtlos gemeinsam nutzen zu können.

Die Plattform akzeptiert eine Vielfalt an Möglichkeiten, um Daten in die Cloud einzupflegen, darunter der bloße Datei-Upload sowie API-gestützte Integrationen. Die Plattform ist mit wertschöpfenden APIs und Apps bestückt, die ein gemeinsames Datenmodell nutzen, um alle auf der Plattform gespeicherten Daten zu verwerten und Nutzern wertvolle Erkenntnisse zu bieten. Ebenso nimmt die Plattform Daten entgegen, die über vernetzte Geräte oder über elektronischen Datenaustausch (EDI) gesendete B2B-Nachrichten übermittelt werden.

Ferner können Lieferanten mit der Plattform präzise überwachen, wer auf welche Daten zu welchen Zwecken Zugriff hat. Diese Überwachung wird durch eine in die Plattform eingebettete Rechtegewährungsfunktion gewährleistet, die Datenlieferanten die Möglichkeit bietet, für die verschiedenen Mitglieder der Nutzergemeinschaft bis zur Feldebene, darunter auch App-Anbieter, Rollen und Teilungsregeln festzulegen. Überdies ermöglicht die Plattform die Anonymisierung und Aggregation von Daten, um die erforderlichen Datenschutzbestimmungen einzuhalten.

#### **4. Eine erfolgreiche B2G-Zusammenarbeit im Datenbereich – Checkliste zur Vorgehensweise**

Die Bereitstellung und Weiterverwendung von Daten zwischen Unternehmen und Behörden (B2G) kann im Hinblick auf die zugrunde liegenden Verfahren und das Rechtsinstrument, auf dem beide basieren, in zahlreichen Formen erfolgen. In diesem Abschnitt werden einige Formen ausführlicher beschrieben.

##### **4.1 Modelle für die gemeinsame Datennutzung zwischen Unternehmen und Behörden**

- a) **Datenspenden:** Die Bereitstellung von Daten zwischen Unternehmen und Behörden könnte über Datenspenden erfolgen. Dies kann als eine Form der sozialen Verantwortung der Unternehmen betrachtet werden. Eine der möglichen Folgen wäre, dass ein solches Programm für Datenspenden von einem eigens eingerichteten Team verwaltet wird, das alle möglicherweise an der Verwendung der Daten interessierten Beteiligten unterstützt.

---

<sup>19</sup> <https://www.nallian.com/>

### **Datenphilanthropie von Mastercard<sup>20</sup>**

Mastercard ist der Auffassung, dass Organisationen, die für die Verringerung menschlichen Leids kämpfen, ungeachtet ihrer Größe und ihres Einflusses über notwendige Instrumente und Ressourcen verfügen sollten, um auf Daten zuzugreifen und mit ihnen Probleme zu lösen. Das *Mastercard Center for Inclusive Growth* ist entschlossen, diese Lücke durch Daten-Philanthropie zu schließen, indem:

- Daten geteilt werden – beispielsweise durch die Gewährung eines Zugangs zu ihren eigenen Daten (unter vollständiger Gewährleistung des Verbraucherdatenschutzes), um Forschung zu unterstützen;
- Daten-Know-how geteilt wird, wie die gewinnbringende Nutzung internen Fachwissens, um Analysen durchzuführen und die Erkenntnisse einer breiteren Verwendung zuzuführen;
- Fachwissen optimal ausgeschöpft wird, beispielsweise durch Zusammenarbeit mit den Partnern, um zusätzliches Wissen und Kapazitäten bereitzustellen.

- b) **Preisverleihungen:** Bei der Zusammenarbeit zwischen Unternehmen und Behörden können ebenfalls Preise gestiftet werden, die auf Datenanalytik spezialisierte Einzelpersonen und Unternehmen dazu ermutigen würden, für besondere Herausforderungen im öffentlichen Interesse Lösungen zu finden. Denkbar wäre, dass eine staatliche Organisation in Zusammenarbeit mit einem Unternehmen eine Herausforderung definiert, das die zur Lösung einer solchen Herausforderung erforderlichen Daten des Privatsektors bereitstellen würde.

### **Horizont-Preis für Big-Data-Technologien<sup>21</sup>**

Im Rahmen des EU-Finanzierungsprogramms „Horizont 2020“ wurde im Bereich der Big-Data-Technologien ein Preis angekündigt, der dazu beitragen soll, die Nutzung von Energienetzen durch ein präziseres Prognosesystem zu optimieren. Die siegreichen Lösungen werden in der Lage sein müssen, extrem umfangreiche Bestände strukturierter raumbezogener temporärer Datensätze, Zeiterfassungen der Wetterbedingungen und sonstige Daten mit verschiedenen Parametern zu analysieren, die beim Energienetzmanagement Verwendung finden.

- c) **Partnerschaften zwischen Unternehmen und Behörden:** Die Zusammenarbeit zwischen Unternehmen und Behörden kann in Form von Datenpartnerschaften erfolgen. Öffentliche Stellen können mit privaten Unternehmen Vereinbarungen treffen, die auch einen gegenseitigen Datenaustausch unter Einhaltung der PSI-Richtlinie<sup>22</sup> in Bezug auf die mit der Privatwirtschaft geteilten Informationen des öffentlichen Sektors beinhalten können. Das kann auch dem privaten Unternehmen Vorteile verschaffen, weil es aus der Korrelation der Daten des öffentlichen und des privaten Sektors Erkenntnisse gewinnen kann.

<sup>20</sup> <https://mastercardcenter.org/action/call-action-data-philanthropy/>

<sup>21</sup> <http://ec.europa.eu/research/horizonprize/index.cfm?prize=bigdata>

<sup>22</sup> Richtlinie 2003/98/EG des Europäischen Parlaments und des Rates über die Weiterverwendung von Informationen des öffentlichen Sektors (ABl. L 345 vom 31.12.2003, S. 90).

„Assessing the Quality of Mobile Phone Data as a Source of Statistics“ (Bewertung der Qualität von Mobilfunkdaten als Statistikquelle) – eine vom belgischen Statistikamt und Eurostat durchgeführte Studie<sup>23</sup>

In einer vom belgischen Statistikamt und Eurostat gemeinsam durchgeführten Studie wurde das Potenzial von Mobilfunkdaten zur Schätzung der Bevölkerungsdichte aufgezeigt. Ziel war, die Qualität belgischer Mobilfunkdaten (vom größten Netzbetreiber Proximus) mit dem Schwerpunkt auf der tatsächlichen Bevölkerung zu bewerten. Die Mobilfunkdaten wurden dabei auf ihre interne Konsistenz hin überprüft und wichen von den Ergebnissen der belgischen Volkszählung aus dem Jahre 2011 ab, die als Teil des Einwohnermelderegisters permanent aktualisiert wird. Beide Datensätze wurden aus Datenschutzgründen aggregiert.<sup>24</sup> Beide Parteien profitierten von den Ergebnissen der Studie. Einerseits wurde aufgezeigt, dass Mobilfunkdaten gültige und präzise Informationen bereitstellen, die traditionelle Statistiken ergänzen können. Andererseits könnten Mobilfunknetzbetreiber Daten der ansässigen Bevölkerung nutzen, um Schätzungen der Mobilität der Personen für neue Anwendungen zu verbessern, die vom Mobilfunknetzbetreiber angeboten werden.

- d) **Vermittler:** Wenn zwischen einem Unternehmen und einer öffentlichen Stelle keine vorherige Beziehung und kein Vertrauensverhältnis besteht, kann ein Vermittler damit beauftragt werden, die für Zwecke des öffentlichen Interesses erforderlichen Erkenntnisse zu gewinnen.

**Consumer Data Research Centre (CDCR UK)**<sup>25</sup>

Tag für Tag fallen riesige Mengen an Daten über die britischen Verbraucher an, aus denen Organisationen wertvolle Erkenntnisse gewinnen können, um effizienter zu funktionieren. Das CDRC will mit Organisationen zusammenarbeiten, um ihre Daten vertrauenswürdigen Forschern zur Verfügung zu stellen, damit diese Lösungen finden, die das Wirtschaftswachstum erhöhen und die Gesellschaft verbessern.

- e) **„Teilen von Bürgerdaten“:** Einzelpersonen können ermutigt werden, öffentlichen Stellen die Verarbeitung ihrer personenbezogenen Daten zu erlauben, nachdem diese zuvor von einem Privatunternehmen verarbeitet wurden. Dabei ist zu betonen, dass Behörden in diesem Fall ebenfalls die Datenschutzvorschriften einhalten müssen. Die Verarbeitung muss im Einklang mit einer geeigneten Rechtsgrundlage (zum Beispiel Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a oder die Durchführung einer im öffentlichen Interesse liegenden Aufgabe gemäß Artikel 6 Absatz 1 Buchstabe e)

<sup>23</sup> De Meersman et al. (2016): *Assessing the Quality of Mobile Phone Data as a Source of Statistics* (Bewertung der Qualität von Mobilfunkdaten als Statistikquelle), [https://ec.europa.eu/eurostat/cros/system/files/assessing\\_the\\_quality\\_of\\_mobile\\_phone\\_data\\_as\\_a\\_source\\_of\\_statistics\\_q2016.pdf](https://ec.europa.eu/eurostat/cros/system/files/assessing_the_quality_of_mobile_phone_data_as_a_source_of_statistics_q2016.pdf).

<sup>24</sup> Statistikämter unterhalten Verzeichnisse mit personenbezogenen Daten und Unternehmensdaten, doch diese Verzeichnisse können aufgrund des Schutzes personenbezogener Daten und Einschränkungen durch die statistische Geheimhaltung nicht mit anderen Parteien geteilt werden. Gleichwohl können Daten aus dem Privatsektor mit Verzeichnisdaten verknüpft werden, während gleichzeitig die Sicherheit der Daten gewährleistet wird. Als Ergebnis dieser Analyse können aggregierte Statistikergebnisse veröffentlicht werden, die sich nicht bis zu den betroffenen Personen zurückverfolgen lassen.

<sup>25</sup> <https://www.cdrc.ac.uk/>

erfolgen.<sup>26</sup> Ein solches „Teilen von Bürgerdaten“ dürfte funktionieren, wenn zwischen dem Bürger und der öffentlichen Stelle (zum Beispiel der Gemeindeverwaltung des Ortes) entweder eine ausreichend starke Verbindung besteht oder das öffentliche Interesse aus Sicht der Bürger besonders plausibel ist (Bekämpfung bestimmter Krankheiten, Regelung des Verkehrsflusses bei beliebten Veranstaltungen usw.).

#### **4.2 Rechtliche und praktische Überlegungen zur Zusammenarbeit bei der gemeinsamen Datennutzung zwischen Unternehmen und Behörden**

Die folgenden Überlegungen können öffentlichen Stellen und Unternehmen bei der Vorbereitung und/oder Aushandlung von Datennutzungsvereinbarungen helfen:

- a) Öffentliche Stellen sollten ein öffentliches Interesse, die Daten des Privatsektors und die erforderliche Granularität angeben. Daten des Privatsektors, die dem öffentlichen Interesse dienen, können beispielsweise Daten sozialer Medien, Transaktionsdaten oder Daten von Einzelhändlern betreffen. Ebenso können Unternehmen selbst prüfen, ob ihre Daten von öffentlichem Interesse sein könnten, und den Verhandlungsprozess von sich aus beginnen.
- b) Die Parteien sollten dabei interne Herausforderungen und Sachzwänge im Zusammenhang mit der gemeinsamen Datennutzung ermitteln.
  - Öffentliche Stellen und Unternehmen müssen möglicherweise in Wissensmanagement und Datenverwaltung investieren.
  - Unternehmen, die Abteilungen für die gemeinsame Datennutzung einrichten (auch für die gewinnbringende Verwertung von Daten im Geschäftsverkehr zwischen Unternehmen), werden die gemeinsame Datennutzung zwischen Unternehmen und Behörden im Hinblick auf Datenverwaltung, Infrastruktur und die Abfassung von Rechtstexten als weniger kostspielig betrachten. Da die gemeinsame Datennutzung für mehr Unternehmen an Bedeutung gewinnt, dürften Kosten und Aufwand im Rahmen einzelner Kooperationen sinken.
  - Unternehmen und öffentliche Stellen müssen sicherstellen, dass die Bestimmungen der DSGVO und der e-Datenschutz-Richtlinie eingehalten werden (Gewährleistung der Rechtmäßigkeit der Verarbeitung, darunter die Nutzung einer Rechtsgrundlage wie der Einwilligung, die ordnungsgemäße Nutzung von Anonymisierungsverfahren, Vertraulichkeit, Einhaltung der Grundsätze des Datenschutzes durch Technik und der datenschutzfreundlichen Voreinstellungen, die Nutzung datenschutzfreundlicher Auswertungsverfahren und gegebenenfalls Datenschutz-Folgenabschätzungen).
  - Um sicherzustellen, dass die Erkenntnisse repräsentativ sind, und um auswahlbedingte Verzerrungen zu vermeiden, müssen öffentliche Stellen eine sorgfältige Analyse potenzieller Datenquellen vornehmen und die Einschränkungen eines bestimmten Datenanbieters bewerten. Außerdem sollten sie sorgfältig die Datentriangulation, die konstante Beobachtung und Neuausrichtung von Modellen und eine Kombination, beispielsweise mit öffentlichen Konsultationen und Instrumenten, erwägen, um Fakten

---

<sup>26</sup> Sofern sich Behörden auf Artikel 6 Absatz 1 Buchstabe e der DSGVO stützen („die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt“), muss eine solche Rechtsgrundlage im Recht der Union oder des Mitgliedstaats verankert sein. Zudem müssten betroffene Personen bei einem solchen „Teilen von Bürgerdaten“ unmissverständlich informiert werden, auch über das Recht, Einwilligungen zu widerrufen sowie über die potenzielle Weiterverarbeitung ihrer personenbezogenen Daten durch Behörden.

und Auffassungen von Interessenträgern zusammenzutragen, damit Risiken und potenzielle methodenbedingte Einschränkungen der Quellen für Daten des Privatsektors gemindert werden.

- c) Die Parteien müssen dabei die technischen oder praktischen Modalitäten für die gemeinsame Datennutzung wählen, die optimal auf ihre internen Herausforderungen und die Datenverwaltung zugeschnitten sind.
- Indes müssen öffentliche Stellen den Schutz legitimer Geschäftsinteressen (wie vertraulicher Geschäftsinformationen und Geschäftsgeheimnisse) und die Sicherheit des technischen Zugriffs auf Daten des Privatsektors sicherstellen. Daten des Privatsektors, die an öffentliche Stellen übertragen werden, sind als vertrauliche Daten zu behandeln. In den relevanten Infrastrukturen für die Datenverarbeitung ist durch Anmerkungen und Zugangsbeschränkungen deutlich zu machen, dass diese durch festgelegte Ausnahmen abgedeckt sind, wenn die öffentliche Stelle den Rechtsvorschriften über den Zugang zu Dokumenten unterliegt. Dabei sind wirksame Maßnahmen erforderlich, damit die Sicherheit von Netzen und Informationssystemen gewährleistet ist.
  - Darüber hinaus kann es erforderlich sein, dass öffentliche Stellen ihre technischen Kapazitäten und die Fähigkeiten ihrer Mitarbeiter erweitern müssen, um die Möglichkeiten für die Nutzung von Daten des Privatsektors auszuschöpfen.
- d) Im Vertrag sollten die Bedingungen der Umsetzung, die zeitlichen Beschränkungen und die verwendeten spezifischen Datensätze aufgeführt sein.
- Öffentliche Stellen müssen gewährleisten, dass ihre Anfragen nach bestimmten privaten Daten dem Grundsatz der Verhältnismäßigkeit entsprechen und erforderlich sind, um das festgelegte öffentliche Interesse wahrzunehmen. Überdies sollte in der Vereinbarung festgelegt sein, dass die übertragenen Daten nach Erfüllung des öffentlichen Interesses oder dem Ablauf der Laufzeit zu löschen sind. Die Nutzung derselben Daten für ein anderen Zweck sollte Gegenstand einer neuen bzw. geänderten Kooperationsvereinbarung sein.
  - Die Parteien sollten die Bedingungen für die Datenübermittlung auf betrieblicher Ebene festlegen, d. h. das Format der Daten und Metadaten sowie die Qualität, Granularität und Dauer des Zugangs und den Zugangsmodus.
  - Schließlich sollten die Parteien ebenfalls die Vergütung festlegen. In dieser Hinsicht bestehen verschiedene Auffassungen. So sollte die Vergütung auf die anteilmäßige Deckung der Kosten für Generierung, Bewahrung und Verbreitung der Daten beschränkt und nur in Ausnahmefällen mit einer fairen Investitionsrendite verknüpft sein. Zudem sollte die Vergütung höchstens den Kosten für die Verbreitung der Daten entsprechen, wobei zu berücksichtigen ist, dass die Kosten für Generierung und Bewahrung der Daten im vorliegenden Fall möglicherweise bereits durch andere Ertragsströme gedeckt wurden. Die Wahl dieser Möglichkeit könnte an das verfolgte öffentliche Interesse und die Merkmale des sozialen Erfordernisses geknüpft sein, dem sie gerecht werden soll.
  - Um öffentlichen Stellen die erforderlichen Qualitätsbewertungen zu ermöglichen, mit denen potenzielle auswahlbedingte Verzerrungen oder sonstige Qualitätsbeschränkungen festgestellt werden können, die möglicherweise erst nach Abschluss der Vereinbarung zutage treten, sollten datenliefernde Unternehmen nach besten Kräften eine angemessene und verhältnismäßige Unterstützung gewähren, um die Bewertung der Datenqualität für die festgelegten Zwecke zu ermöglichen, darunter

auch über die Möglichkeit, die Daten wann immer angemessen zu prüfen oder auf sonstige Weise zu verifizieren.

- e) Schließlich sollten sich die Parteien auf gemeinsame Leitlinien für die Überwachung der Durchführung des Vertrags verständigen:
  - Denkbar wären ein Verhaltenskodex oder die Anwendung bestehender ethischer Regeln wie des Verhaltenskodex für europäische Statistiken<sup>27</sup>, die Einsetzung eines Koordinierungsausschusses oder die Bestellung eines unabhängigen Prüfers zur Überwachung der Datennutzung.
  - Öffentliche Stellen bieten die notwendigen Garantien, die verhindern, dass die eingesehenen Daten für vertragsfremde Zwecke verwendet werden.
- f) Der Vertrag sollte Haftungsregelungen enthalten, sofern fehlerhafte Daten bereitgestellt werden, die Datenübertragung unterbrochen wird, die Auswertung von geringer Qualität ist, falls diese Auswertung zusammen mit den Datensätzen weitergegeben wird, oder es zu Zerstörung/Verlust oder Veränderungen der Daten (unrechtmäßig oder zufällig) kommt, die Schäden verursachen können.
- g) Überdies sollten im Vertrag das geltende Recht und die Verfahren für die Streitbeilegung festgeschrieben sein.  
Jede Partei sollte den Vertrag kündigen dürfen, wenn ein rechtliches oder technisches Risiko in Bezug auf die Verarbeitung oder die Nutzung der gemeinsam genutzten Daten besteht.
- h) Öffentliche Stellen sollten die Ergebnisse/Erkenntnisse der Zusammenarbeit zwischen Unternehmen und Behörden bekannt machen und – wann immer notwendig oder relevant – Verfahren für öffentliches Feedback einrichten, ohne dabei die Vertraulichkeit der Daten des Privatsektors zu gefährden.

#### **4.3 Technische Mittel zur Einrichtung einer Zusammenarbeit zwischen Unternehmen und Behörden**

Bei einer Zusammenarbeit zwischen Unternehmen und Behörden ist festzulegen, wie die Erkenntnisse aus den Daten des Privatsektors für ein öffentliches Interesse abzuleiten sind. Dies kann die tatsächliche Übertragung von Daten des Privatsektors in die IT-Umgebung der jeweiligen öffentlichen Stelle beinhalten. Dies ist jedoch nicht die einzige Möglichkeit, und es können weitere Verfahren erwogen werden. Dieser Abschnitt enthält einen Überblick über technische Mittel, die als Alternative für die Übertragung von Daten des Privatsektors in die IT-Umgebung der öffentlichen Stelle fungieren können. Diese technischen Verfahren können Regeln für den Zugang zu und die Nutzung von Daten umfassen und gleichzeitig eine vertrauenswürdige und sichere Umgebung für den Austausch von Datensätzen bieten.

- a) **Datenplattformen:** Datenplattformen können eine sichere Umgebung bieten, um Daten zu speichern und zwischen Unternehmen und öffentlichen Stellen auszutauschen. Öffentliche Stellen können durch solche Plattformen standardisierte Daten erhalten, um in Zusammenarbeit mit Unternehmen gemeinsame Datenressourcen einzurichten oder Erkenntnisse zu gewinnen.

---

<sup>27</sup> Bei Vereinbarungen mit Statistikämtern könnte dies der Verhaltenskodex für europäische Statistiken sein, <http://ec.europa.eu/eurostat/web/products-manuals-and-guidelines/-/KS-32-11-955>

### Centre for Big Data Statistics, Niederlande<sup>28</sup>

Das Centre for Big Data Statistics (CBS) arbeitet mit einer Reihe von Organisationen des Privatsektors zusammen, um Daten des Privatsektors zu sammeln und hochwertige Datenvisualisierungen zu erstellen. Da es sich beim CBS um eine staatliche Einrichtung handelt, hat es ebenfalls Zugang zum umfangreichen niederländischen Bestand an staatlichen Daten und Sensordaten, die es zur Gewinnung neuer Erkenntnisse mit diesen neuen Datenquellen zusammenführen kann.

- b) **Datenalgorithmen:** Datenalgorithmen, die direkt bei den Datenbeständen zum Einsatz kommen, können eine Lösung im Hinblick auf Probleme der Sicherheit, des Datenschutzes und der Privatsphäre darstellen. Dabei würde eine der wichtigsten Aspekte der Gewährleistung eines Schutzes personenbezogener Daten und der Privatsphäre eingehalten – d. h. Daten so wenig wie möglich zu verschieben. Bei dieser Lösung wird der Algorithmus innerhalb der IT-Umgebung des Privatunternehmens verankert, wo auch die Auswertung erfolgt. Dabei fließen nur die vom Algorithmus abgeleiteten anonymen Erkenntnisse wieder zur öffentlichen Stelle zurück. Die Schnittstelle zur Datenabfrage und die Analysemöglichkeiten könnten vom Unternehmen und/oder der jeweiligen staatlichen Organisation (oder einem vertrauenswürdigen Vermittler) gemeinsam geschaffen werden.

### The Open Algorithms (OPAL)<sup>29</sup>

Das Projekt ist eine soziotechnologische Innovation, die von der Data-Pop Alliance, dem Imperial College London, dem MIT Media Lab, Orange und dem Weltwirtschaftsforum entwickelt wurde, um Daten des Privatsektors für Zwecke des Gemeinwohls zu nutzen, indem „der Code zu den Daten gesendet wird“, und zwar auf datenschutzfreundliche, vorhersehbare, partizipative, skalierbare und nachhaltige Weise. Der Algorithmus wird dabei von den örtlichen Beiräten für Entwicklungsrichtung und Ethik (CODE) entwickelt, damit er lokalen Anforderungen gerecht wird und lokale Normen einhält, statt externe Perspektiven und Erkenntnisse aufzuzwingen.

- c) **Datenschutzfreundliche Rechentechnik:** In den letzten Jahren wurden mehrere Rechenmodelle für die Durchführung von Operationen mit Daten entwickelt, die vertraulich bleiben müssen. Derartige Modelle ermöglichen es, die gewünschten Ausgabedaten ohne Offenlegung der Eingabedaten zu extrahieren. Aus diesem Grunde können die Rechenvorgänge gemeinsam über mehrere administrative Bereiche (öffentlich oder privat) hinweg erfolgen, ohne dass Daten außerhalb des Unternehmens verschoben werden müssen. Solche Modelle bedeuten einen fundamentalen Paradigmenwechsel von der „gemeinsamen Datennutzung“ hin zur „gemeinsamen Rechentechnik“. Unter den bestehenden datenschutzfreundlichen Rechenverfahren scheint sich die Kategorie des sicheren Mehrparteienrechnens besonders gut für die Datenzusammenarbeit zwischen Unternehmen und Behörden zu eignen. Bestimmte einfache sichere Mehrparteienrechenverfahren sind äußerst skalierbar und leistungsfähig. Einige wenige Unternehmen bieten die Technologie und einschlägige Plattformen bereits an. Es wurden

<sup>28</sup> <https://www.cbs.nl/en-gb/our-services/innovation/big-data>

<sup>29</sup> <http://www.opalproject.org/about-us/>

Studien durchgeführt, in deren Rahmen dieses Verfahren bei der Zusammenarbeit zwischen Unternehmen und Behörden zur Anwendung kam.

### **Sicheres Mehrparteienrechnen<sup>30</sup>**

Das sichere Mehrparteienrechnen (*Secure Multi-party Computation*) ist eine praktische Verschlüsselungsmethode zur Verarbeitung vertraulicher Daten. Fortschritte in der Forschung haben dazu geführt, dass sie in der datenschutzfreundlichen statistischen Analyse Verwendung findet. Im Jahr 2015 führten Statistiker des Estnischen Zentrums für angewandte Forschung (CentAR) eine Untersuchung mithilfe von Massendaten durch, um die Korrelationen zwischen einer Erwerbstätigkeit während des Hochschulstudiums und der Unfähigkeit, das Studium zeitnah abzuschließen, zu erforschen. Dazu wurden die Einkommensteuerdatenbank des estnischen Steuer- und Zollamts und die Datenbank für Hochschulstatistik des Ministeriums für Bildung und Forschung miteinander verknüpft. Datenerhebung, -aufbereitung und -analyse wurden unter Nutzung des sicheren Sharemind-Mehrparteienrechnensystems durchgeführt, das die durchgehende Verschlüsselung im Rahmen der Analyse ermöglichte. Die auf 10 Millionen Steuerunterlagen und eine halbe Million Ausbildungsnachweise gestützte Analyse ist die größte verschlüsselte private Statistikanalyse, die jemals mit echten Daten durchgeführt wurde.

---

<sup>30</sup> Bogdanov (et al.), *Students and Taxes: a Privacy-Preserving Social Study Using Secure Computation*. In: *Proceedings on Privacy Enhancing Technologies*, PoPETs, 2016 (3), S. 117–135, 2016. (Erweiterte Fassung, PDF).