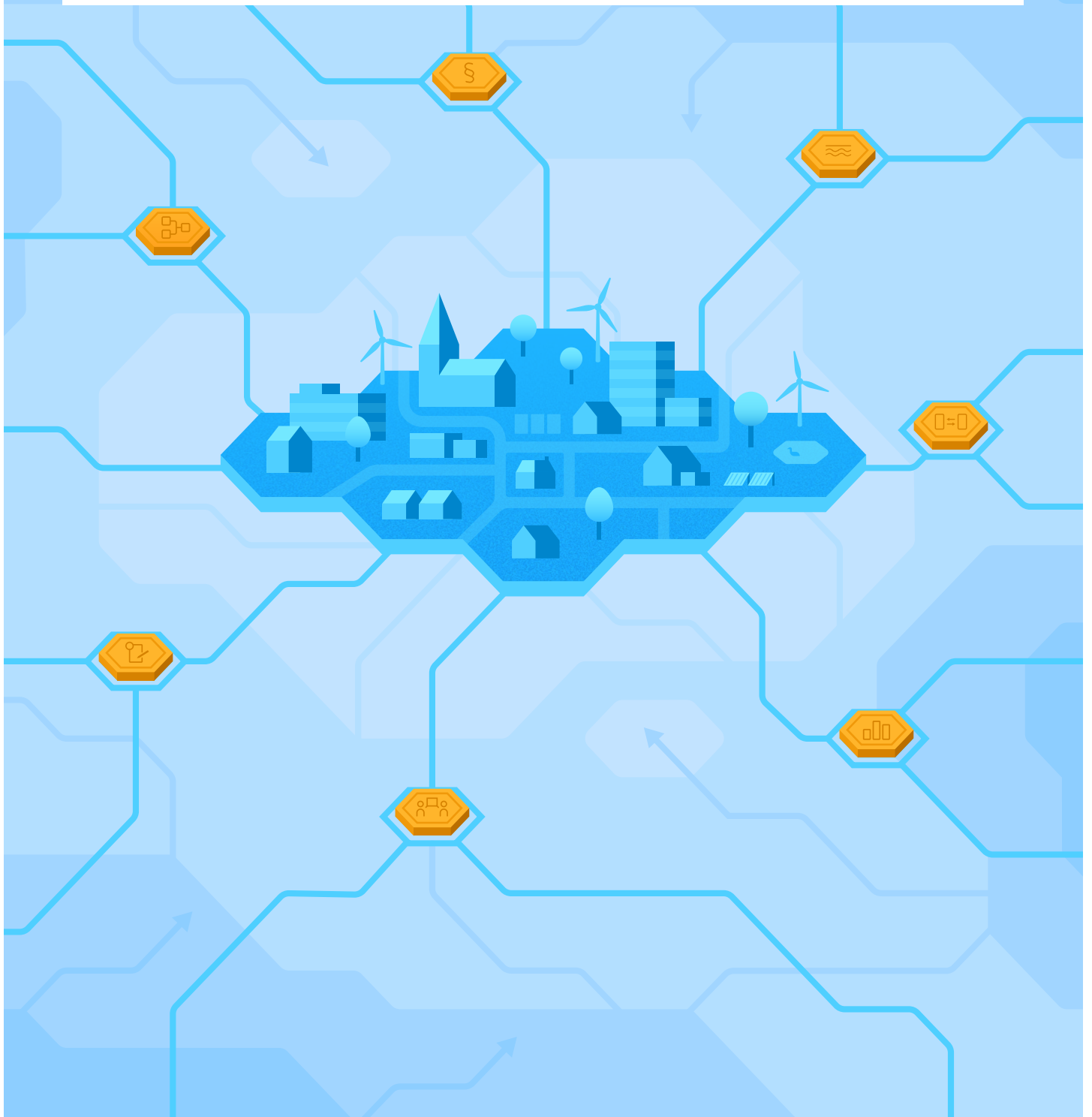


EU Data Act in der kommunalen Praxis

Überblick über den europäischen Rechtsrahmen und strategische Implikationen für die Nutzung externer Daten in Kommunen



© Bertelsmann Stiftung, Gütersloh

März 2026

Verlag

Bertelsmann Stiftung

Carl-Bertelsmann-Straße 256, 33311 Gütersloh

bertelsmann-stiftung.de

Verantwortlich

Johanna Neu, Bertelsmann Stiftung

Clara Ruthardt, Bertelsmann Stiftung

Autorin

Veronika Ludwig, Wirtschaftsjuristin, LL.M., CIPP/E, CEO data stewards GmbH

Korrektorat

Rudolf Jan Gajdacz, München

Zitationshinweis

Ludwig, Veronika (2026). EU Data Act in der kommunalen Praxis: Überblick über den europäischen Rechtsrahmen und strategische Implikationen für die Nutzung externer Daten in Kommunen.

Hrsg. Bertelsmann Stiftung. Gütersloh.

Konzept

Diese Analyse wurde im Rahmen des Projekts 'Kommunale Datenkooperationen für das Gemeinwohl' mit Beyond Civic AG erarbeitet.

Gestaltung

Paul Feldkamp, Bielefeld

Bildnachweis

© Paul Feldkamp

Danksagungen

Wir danken Herrn Matthias Niebuhr für den wertvollen fachlichen Austausch und die hilfreichen inhaltlichen Anmerkungen im Rahmen der Erarbeitung dieser Analyse.

ID_2943

DOI 10.11586/2026011

EU Data Act in der kommunalen Praxis

Überblick über den europäischen Rechtsrahmen und strategische Implikationen für die Nutzung externer Daten in Kommunen

Inhaltsverzeichnis

Glossar	5
Executive Summary	6
Einleitung	8
1. EU Data Act, Data Governance Act und Datenschutz-Grundverordnung im Überblick	10
1.1 EU Data Act (DA)	10
1.2 Data Governance Act (DGA)	11
1.3 Datenschutz-Grundverordnung (DSGVO)	12
1.4 Wie DA, DGA und DSGVO ineinandergreifen	12
2. Kommunalen Datenzugang im europäischen Rechtsrahmen	13
2.1 Freiwillige Datenbereitstellung	13
2.1.2 Datenbereitstellung über datenaltruistische Organisationen (Art. 16 ff. DGA)	14
2.1.3 Nutzung von Datenvermittlungsdiensten (Art. 10 ff. DGA)	15
2.1.4 Datenteilen über vernetzte Produkte oder verbundene Dienste (EU Data Act)	16
2.2 Verpflichtende Datenbereitstellung im Ausnahmefall	17
2.2.1 Rechtsgrundlagen und Voraussetzungen nach Art. 14 ff. DA	17
2.2.2 Praktische Herausforderungen bei der verpflichtenden Datenweitergabe nach Art. 14 DA	19
2.3 Das hybride Modell: Freiwilligkeit und Pflicht strategisch kombiniert	20
2.3.1 Zielsetzung	20
2.3.2 Voraussetzungen und Gestaltungsprinzipien	21
2.3.3 Die kommunale Datenplattform als Basisstruktur	22
2.4 Zusammenfassung: Chancen, Bedingungen, Herausforderungen	22
2.4.1 Datenzugänge im Überblick	22
2.4.2 Datenintermediäre und Datenaltruismus-Organisationen	23
2.4.3 Rechts- und Governance-Anforderungen	23
2.4.4 Strategischer Ausblick	24
3. Erfolgsfaktoren für kommunales Verfügbarmachen und Nutzen externer Daten unter dem EU Data Act	25
Frühzeitig handeln – nicht erst im Notfall	25
Motivation schaffen – durch Anreize und greifbare Mehrwerte	25
Vertrauen ermöglichen – durch Kommunikation, Transparenz und Governance	25
Datenkooperationen als strategische Übung etablieren	26
Fazit	26

Glossar

In dieser Analyse werden einige Begriffe verwendet, die sich an die Terminologie des EU Rechts (z. B. EU Data Act, Data Governance Act) anlehnen, aber nicht immer exakt den technischen juristischen Definitionen entsprechen. Für eine bessere Lesbarkeit nutzen wir teils vereinfachte, intuitive Bezeichnungen. Die folgenden Erläuterungen sollen helfen, die Begriffe im Kontext dieser Analyse richtig zu verstehen.

Dateninhaber: Organisationen oder Unternehmen, die Daten sammeln, speichern und kontrollieren und damit der gesetzlichen Pflicht nach EU Data Act unterliegen, die Daten auf Verlangen herauszugeben.

Beispiel: Ein Hersteller vernetzter Fahrzeuge, der Fahr- und Sensordaten seiner Autos auf seinen Servern speichert.

Datengeber:in/Datenhalter:in: werden als datenhaltend beschrieben, wenn es um ihre Rolle als Erzeuger und Verwalter der eigenen Daten geht (sie sammeln, speichern und nutzen ihre Daten selbst), und als datengebend bezeichnet, wenn sie diese Daten Dritten bereitstellen oder eine Weitergabe ermöglichen (z. B. durch Datenspende oder Anweisung an einen Dateninhaber).

Beispiel: Eine Kommune, die Verkehrsdaten mit eigener Sensorik erhebt, ist zunächst datenhaltend. Stellt sie diese Daten einem Forschungsprojekt oder einer anderen Kommune zur Verfügung, wird sie zum datengebenden Akteur.

Datennutzer:in/Datenempfänger:in: Personen oder Organisationen, die Daten von Datengeber:innen erhalten und für ihre Aufgaben nutzen, z. B. für Planung, Steuerung, Evaluation, Forschung oder Serviceangebote.

Beispiel: eine Stadtverwaltung, die von Bürger:innen und Unternehmen bereitgestellte Mobilitätsdaten erhält und auswertet, um den öffentlichen Nahverkehr und Radwege besser zu planen.

Nutzer:in eines Gerätes oder verbundenen Dienstes: Stelle, die ein vernetztes Gerät oder einen verbundenen Dienst einsetzt und dadurch bestimmte Rechte auf Zugang zu den dabei entstehenden Daten haben kann.

Beispiel: eine Kommune, die smarte Straßenlaternen betreibt und vom Hersteller Zugang zu Betriebs- und Umweltdaten verlangen kann.

Executive Summary

Für einen gezielten Ressourceneinsatz und eine sozial gerechte, vorausschauende Stadtentwicklung benötigen Kommunen eine verlässliche Datengrundlage. Entscheidungsrelevante Daten sind für Kommunalverwaltungen jedoch häufig nicht direkt zugänglich, sondern liegen bei Unternehmen, Vereinen, Bürger:innen oder bei Landes- oder Bundeseinrichtungen. Mit dem seit 12. September 2025 anwendbaren EU Data Act (DA) verfolgt die EU das Ziel, bestehende Barrieren beim Datenaustausch abzubauen, die eine effiziente Nutzung von Daten für die Gesellschaft behindern. Daraus ergeben sich für Kommunen neue rechtliche Möglichkeiten, auf Daten zuzugreifen, die bislang überwiegend bei Bürger:innen oder privaten Unternehmen liegen. Zusammen mit bestehenden Regelungen wie dem Data Governance Act (DGA) und der Datenschutz-Grundverordnung (DSGVO) schafft der EU Data Act somit einen neuen Rechtsrahmen für die verbesserte Nutzung externer Daten durch Kommunen – vorausgesetzt, die entsprechenden Strukturen und Prozesse seitens Dateninhabern und Kommunen sind vorbereitet und erprobt.

Das vorliegende Analysepapier untersucht, welche strategischen Implikationen und Chancen der aktuelle europäische Rechtsrahmen für die Nutzung externer Daten durch Kommunen eröffnet. Der EU-Rechtsrahmen sieht grundsätzlich mehrere Zugangswege zu externen Daten vor, die Kommunen nutzen können, darunter:

- **Freiwillige Datenbereitstellung:**
 - **Nutzerbasierte Datenweitergabe (gemäß Kapitel II DA)¹:** Bürger:innen können als Nutzer:innen selbst bestimmen, dass ihre Daten aus vernetzten Geräten oder digitalen Diensten an Kommunen übermittelt werden.
 - **Freiwillige Datenbereitstellung (gemäß DGA):** Der Data Governance Act schafft neue Kooperationsmodelle, um die Nutzarmachung bestehender Datenbestände aus öffentlicher Hand oder von anderen datenhaltenden Akteur:innen (Unternehmen, Bürger:innen) zu fördern.
- **Verpflichtende Datenbereitstellung in Notlagen (gemäß Kapitel V DA):** In Fällen außergewöhnlicher Notwendigkeit, bzw. öffentlicher Notstände können Kommunen Daten direkt von Dateninhabern anfordern.

Basierend auf den rechtlichen Rahmenbedingungen schlägt das Analysepapier die **Einführung eines hybriden Modells für die Nutzung externer Daten durch Kommunen** vor. Ein solches Modell kombiniert freiwillige und verpflichtende Datenzugänge und nutzt so rechtliche, technische und organisatorische Synergien für eine effiziente, gemeinwohlorientierte Datennutzung.

1 Der Vollständigkeit halber sei angemerkt, dass Kommunen berechtigt sind, Daten aus den von der Kommune selbst genutzten vernetzten Geräten oder digitalen Diensten anzufordern. Diese Konstellation steht jedoch nicht im Fokus der vorliegenden Analyse.

Darauf aufbauend identifiziert der Report vier zentrale Erfolgsfaktoren für kommunales Verfügbarmachen und Nutzen externer Daten:

1. **Frühzeitig handeln – nicht erst im Notfall:** Wenn Infrastruktur, Prozesse und Kooperationen schon vor Krisen bestehen, kann im Ernstfall schneller reagiert werden.
2. **Motivation schaffen – durch Anreize und greifbare Mehrwerte:** Die Mehrwerte der Datenbereitstellung sind für Datengeber:innen oft nicht unmittelbar ersichtlich. Werden diese klar vermittelt und nachvollziehbar gemacht, kann ihre Bereitschaft, aktiv mitzuwirken, steigen.
3. **Vertrauen ermöglichen – durch Kommunikation, Transparenz und Governance:** Klar kommunizierte Zwecke, niedrigschwellige Beteiligung und nachvollziehbare Kontrolle erhöhen die Bereitschaft zur Datenteilung. Dazu müssen Rollen zwischen Kommune, Intermediären und Datengeber:innen eindeutig geregelt sein.
4. **Praxisnahe Erprobung:** Pilotprojekte und Experimentierräume („Data Sandboxes“) sind entscheidend, um Modelle technisch, organisatorisch und gesellschaftlich zu testen.

Mit dem EU Data Act, in Kombination mit dem Data Governance Act verfügen Kommunen über ein strategisch nutzbares Instrumentarium, um mehr externe Daten für kommunale Entscheidungsprozesse verfügbar zu machen. Der Schlüssel liegt in frühzeitig aufgebauten und klaren Strukturen und in praktischer Erprobung sowie in der Erkennbarkeit der Mehrwerte für die Datengeber:innen und in der Herstellung einer Vertrauensbasis, damit theoretische Konzepte in konkrete kommunale Praxis übersetzt werden können. Pilotprojekte, datengetriebene Services und Kooperationen mit Intermediären können zudem Erfahrungsräume schaffen, die nicht nur den Alltag verbessern, sondern auch die Resilienz und Reaktionsfähigkeit in Krisen stärken. Kommunen können so zu souveränen Datenakteuren werden, die den Europäischen Rechtsrahmen nutzen, um Innovation und Gemeinwohl gleichsam zu fördern.

Einleitung

Für einen gezielten Ressourceneinsatz und eine vorausschauende, sozial gerechte Stadtentwicklung benötigen Kommunen eine verlässliche Datengrundlage. Entscheidungsrelevante Daten sind jedoch oft nicht direkt zugänglich, sondern liegen bei Unternehmen, zivilgesellschaftlichen Organisationen, Bürger:innen oder bei Landes- oder Bundeseinrichtungen. Werden Daten nur von wenigen Akteuren kontrolliert, bleiben ihr gesellschaftliche Mehrwert und ihr Innovationspotenzial weitgehend ungenutzt.

Im Projekt „Datenkooperationen für das Gemeinwohl“ hat die Bertelsmann Stiftung explorativ untersucht, wie Datenkooperationen zwischen Kommunen und datenhaltenden Organisationen und Bürger:innen ausgestaltet werden müssen, damit sie echten Mehrwert für die Gesellschaft schaffen. Die Datennutzung in Kommunen bewegt sich in einem komplexen europäischen Rechtsrahmen, der jüngst um ein wichtiges Regelwerk erweitert wurde: Seit 12. September 2025 ist der **EU Data Act (DA)** anwendbar² – **doch was bedeutet das für Kommunen?**

In der vorliegenden Analyse zeigen wir: Es ergeben sich neue rechtliche Möglichkeiten. Kommunen können gemäß EU Data Act unter bestimmten Voraussetzungen gezielt externe Daten nutzen – entweder auf Basis einer freiwilligen Weitergabe durch Bürger:innen oder Unternehmen oder in Ausnahmefällen durch gesetzlich geregelten Sonderzugriff.

Der EU Data Act zählt dabei auf ein übergeordnetes gesellschaftliches Ziel ein: Barrieren, die eine optimale Nutzung von Daten zum Nutzen der Gesellschaft behindern, abzubauen. Ergänzend definiert der seit September 2023 wirksame **Data Governance Act (DGA)** die Rahmenbedingungen für freiwilliges Datenteilen und schafft Strukturen für die Zusammenarbeit mit neutralen Datenvermittlungsdiensten oder gemeinwohlorientierten Organisationen, die z. B. Daten erheben, Einwilligungen verwalten und Datentransparenz sicherstellen können. Ein aktueller Vorschlag der Europäischen Kommission im Rahmen des **Digital-Omnibus** könnte künftig eine stärkere Verzahnung von EU Data Act und Data Governance Act ermöglichen und damit die Nutzung und das Teilen von Daten noch kohärenter gestalten. Die **Datenschutz-Grundverordnung (DSGVO)** schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten vor unbefugter Verarbeitung, unberechtigtem Zugriff, Verlust oder Missbrauch und wird daher häufig als Hürde für die Datennutzung und das Datenteilen wahrgenommen. Bei genauer Kenntnis bietet sie jedoch verlässliche Leitlinien für kommunale Strategien und Entscheidungsprozesse und kann im Zusammenspiel mit weiteren Rechtsakten neue Handlungsräume auf kommunaler Ebene eröffnen.

² Am 29.10.2025 wurde der Entwurf des [Durchführungsgesetzes](#) zum EU Data Act vom Bundeskabinett beschlossen.

Ziel dieses Analysepapiers ist es, die rechtlichen und strategischen Rahmenbedingungen aufzuzeigen, unter denen Kommunen externe Daten nutzen können – gerade dann, wenn diese nicht bei öffentlichen Stellen liegen, sondern bei Bürger:innen oder privaten Unternehmen. Im Mittelpunkt stehen die Voraussetzungen, die erfüllt sein müssen, um eine freiwillige oder verpflichtende Bereitstellung solcher Daten zu ermöglichen. Darauf aufbauend wird ein flexibel kombinierbares „hybrides Modell“ vorgestellt, das rechtliche Rahmenbedingungen, technische Infrastruktur und strategische Governance gezielt verbindet, um Kommunen die effiziente, rechts-sichere und gemeinwohlorientierte Nutzung externer Daten zu ermöglichen. Das Papier dient dazu, kommunalen Akteuren Inspiration und Orientierung zu bieten, um relevante rechtliche und organisatorische Fragen im Hinblick auf die Nutzung externer Daten frühzeitig anzugehen. Es soll dazu anregen, Chancen zu erkennen und über mögliche Partnerschaften nachzudenken, z. B. mit anderen Kommunen, Unternehmen, Forschungseinrichtungen oder perspektivisch auch mit neutralen Intermediären.



Digital-Omnibus und Bedeutung für diese Analyse

Das Digital-Omnibus-Paket ist ein Legislativvorschlag der Europäischen Kommission vom 19. November 2025. Es handelt sich derzeit um einen Vorschlag, der noch im europäischen Gesetzgebungsverfahren verhandelt werden wird. Inhalt und Wortlaut des aktuellen Anpassungsvorschlags können sich also noch deutlich ändern. Für die rechtliche Bewertung in dieser Analyse ist deshalb der aktuell geltende Rechtsrahmen maßgeblich. Die Omnibus-Vorschläge werden hier nicht als bestehendes Recht behandelt, sondern lediglich als Hinweis auf mögliche künftige Entwicklungen:

So zielen die aktuellen Änderungsvorschläge zum EU Data Act hauptsächlich auf Klarstellungen, Entlastungen und besseren Schutz von Geschäftsgeheimnissen ab, ohne die grundsätzlichen Nutzerrechte und Datenteilungsmechanismen zu eliminieren. Im Bereich der B2G-Zugriffe (Art. 14, 15 DA) wird eine stärkere Beschränkung auf echte Not- und Ausnahmesituationen vorgeschlagen. Im Data Governance Act sind etwa Erleichterungen für Datenintermediäre und datenaltruistische Organisationen vorgesehen, die auf weniger bürokratische Hürden und vereinfachte Rahmenbedingungen abzielen, um die Etablierung solcher Modelle zu fördern. Insgesamt spricht die im Digital-Omnibus-Paket erkennbare Tendenz dafür, dass die hier formulierten strategischen Empfehlungen für Kommunen bestätigt und in ihrer Relevanz gestärkt werden.

Hinweis: Die Analyse konzentriert sich – neben EU Data Act und Data Governance Act – auf die datenschutzrechtlichen Vorgaben der DSGVO, lässt jedoch weitere kommunal- oder verwaltungsrechtliche Regelungen bewusst außen vor und verzichtet auf eine Prüfung der Datenverarbeitung im Einzelfall auf Basis des „berechtigten Interesses“. Stattdessen wird die Einwilligung der betroffenen Personen als zentrale Grundlage für freiwillige Datenweitergabe betrachtet. Die Analyse bezieht sich dabei auf das bestehende Recht zum Stand 20. Januar 2026.

1. EU Data Act, Data Governance Act und Datenschutz-Grundverordnung im Überblick

Die europäische Datenpolitik verfolgt das Ziel, den Zugang zu und die verantwortungsvolle Nutzung von Daten zu verbessern, um Innovationen zu fördern, die Wettbewerbsfähigkeit zu stärken und gleichzeitig Grundrechte zu schützen. Drei hier relevante, zentrale Rechtsakte bilden dabei das regulatorische Fundament: der EU Data Act (DA), der Data Governance Act (DGA) und die Datenschutz-Grundverordnung (DSGVO). Während die DSGVO den Schutz personenbezogener Daten sichert, schaffen DGA und DA neue Strukturen für Datenteilung, Zugang und Wiederverwendung – auch über rein personenbezogene Daten hinaus. Für Kommunen ergeben sich daraus neue Möglichkeiten der Datennutzung sowie strategische Fragestellungen im Aufbau von Dateninfrastrukturen.

1.1 EU Data Act (DA)

Die Verordnung (EU) 2023/2854 (EU Data Act) ist seit dem 12. September 2025 anwendbar und ergänzt den Data Governance Act, indem sie den Zugang zu Nutzungsdaten aus vernetzten Geräten und digitalen Diensten regelt. Im Fokus stehen Daten, die bei der Anwendung von z. B. Haushaltsgeräten, Industrieanlagen oder smarten Infrastrukturen anfallen. Ziel ist es, die bislang oft exklusiv vom Hersteller kontrollierten Daten für Nutzer:innen und berechnigte Dritte zugänglich zu machen.

Art. 4 Abs. 1 DA schreibt dabei vor, dass Dateninhaber (z. B. Hersteller vernetzter Produkte und Anbieter digitaler Dienste), die Daten auf Anforderung in maschinenlesbarem, interoperablem Format diskriminierungsfrei und ohne unangemessene Verzögerung bereitstellen müssen. Kommunen können vom EU Data Act auf verschiedenen Wegen profitieren:

Freiwillige Weitergabe durch Nutzer:innen (gemäß Art. 5 ff. DA)

Kommunen können als berechnigte Dritte auf Verlangen der Nutzer:innen vernetzter Geräte (z. B. Bürger:innen) Zugang zu entsprechenden Daten erlangen (Art. 5 DA). Die Nutzung durch die Kommune erfolgt auf Grundlage vertraglicher Vereinbarungen:

- zwischen Kommune und Nutzer:innen (Art. 6 Abs. 1 DA) zur Festlegung von Zwecken und Umfang der Datennutzung,
- zwischen Kommune und Dateninhaber (Art. 8 und 9 DA) gemäß vertraglich festgelegten Bedingungen.

Sonderzugriff in Notlagen (gemäß Art. 14 ff. DA)

Öffentliche Stellen können in Fällen außergewöhnlicher Notwendigkeit („exceptional need“) auf Daten privater Akteur:innen zugreifen – auch ohne Zustimmung der betroffenen Personen oder Unternehmen. Der EU Data Act unterscheidet dabei zwischen öffentlichen Notlagen („public emergencies“), etwa bei unmittelbaren Krisen oder Gefahrenlagen, und anderen Fällen außergewöhnlicher Notwendigkeit, in denen Daten erforderlich sind, um Aufgaben im öffentlichen Interesse zu erfüllen. Jeder Zugriff muss verhältnismäßig, zweckgebunden und technisch gesichert erfolgen; Geschäftsgeheimnisse der Dateninhaber:innen sind dabei unter allen Umständen zu respektieren (Art. 5 Abs. 9–11 DA).

Nutzung eigener Datenzugangsrechte (gemäß Art. 5 DA)

Der Vollständigkeit halber sei darauf hingewiesen, dass auch Kommunen direkt oder durch kommunale Betriebe (z. B. Stadtwerke) Infrastrukturen betreiben, die durch den Einsatz vernetzter Produkte Daten über ihre Nutzung generieren und damit selbst als Nutzer Zugangsrechte gegenüber Dateninhabern geltend machen können. Beispiele sind Anlagen der Energieerzeugung, Gebäudetechnik oder Fahrzeugflotten (z. B. ÖPNV oder Bauhöfe). Die Nutzung dieser Daten steht jedoch nicht im Fokus dieser Analyse.

1.2 Data Governance Act (DGA)

Die Verordnung (EU) 2022/868 (Data Governance Act) ist seit September 2023 anwendbar. Sie zielt darauf ab, das freiwillige Teilen von Daten zu erleichtern und dabei Vertrauen, Transparenz und Rechtssicherheit zu gewährleisten. Der DGA verpflichtet nicht zur Bereitstellung von Daten, sondern definiert neue Kooperationsmodelle, um bestehende Datenbestände aus öffentlicher Hand, von Unternehmen und anderen datenhaltenden Akteuren besser nutzbar zu machen.

Für Kommunen eröffnet der DGA perspektivisch die Möglichkeit, mit Vermittlungsdiensten oder datenaltruistischen Organisationen zu kooperieren, ohne sämtliche Anforderungen und Infrastrukturen eigenständig umsetzen zu müssen. Der DGA unterscheidet drei zentrale Modelle:

Weiterverwendung von Daten öffentlicher Stellen (Art. 3–9 DGA)

Daten, die öffentliche Stellen bereits halten, können unter bestimmten Bedingungen Dritten zur Verfügung gestellt werden – beispielsweise anonymisierte Mobilitätsdaten zur Verkehrsplanung. Dabei sind die bestehenden Vorgaben zum Datenschutz (DSGVO) sowie Geheimhaltungs- und Transparenzvorgaben uneingeschränkt einzuhalten.

Datenvermittlungsdienste (Art. 10–15 DGA)

Sogenannte „Data Intermediaries“ agieren als neutrale Vermittler zwischen Datengeber:innen (Bürger:innen, Unternehmen, öffentliche Stellen) und Datennutzer:innen. Sie gewährleisten rechtlich und technisch konforme Datenflüsse, ohne eigene wirtschaftliche Interessen an den Daten zu verfolgen. Wesentliche Aufgaben umfassen Einwilligungsmanagement, Zugriffskontrolle, Sicherheitsmechanismen und Transparenzvorgaben (Art. 12 DGA).

Datenaltruismus (Art. 16–25 DGA)

Bürger:innen und Unternehmen können ihre Daten freiwillig für Zwecke des Gemeinwohls bereitstellen („Datenspende“), etwa für Forschung oder staatliche Maßnahmen wie die Verbesserung des Verkehrs, der öffentlichen Gesundheit und der Bekämpfung des Klimawandels. Die empfangenden Organisationen müssen gemeinnützig agieren, dürfen keine kommerziellen Interessen verfolgen und werden in einem EU-Register geführt. Bislang ist das Konzept noch in einer frühen Entwicklungsphase, reale Anwendungsbeispiele sind rar (siehe auch Kapitel 2.1.2).

1.3 Datenschutz-Grundverordnung (DSGVO)

Die Verordnung (EU) 2016/679 (kurz DSGVO) bildet das zentrale Schutzregime für personenbezogene Daten in Europa. Sie regelt, wann und wie personenbezogene Daten verarbeitet werden dürfen, und verankert Grundprinzipien wie Zweckbindung, Datenminimierung, Transparenz, Sicherheit und Rechenschaftspflicht. Für Kommunen als datenverarbeitende Stellen bedeutet dies insbesondere:

- **Rechtsgrundlage:** Jede Verarbeitung von Personendaten erfordert eine Rechtsgrundlage (z. B. eine Einwilligung oder eine gesetzliche Grundlage)
- **Informationspflichten:** Betroffene müssen über Art, Zweck und Empfänger der Datenverarbeitung transparent informiert werden.
- **Technische und organisatorische Maßnahmen:** Datenschutz ist durch Maßnahmen wie Anonymisierung, Pseudonymisierung oder Zugriffskontrollen dauerhaft sicherzustellen.
- **Speicherbegrenzung:** Daten dürfen nicht unbegrenzt gespeichert werden; die Aufbewahrungsdauer richtet sich nach Zweck und Rechtsgrundlage.

Diese Anforderungen sind für jede kommunale Datennutzung von zentraler Bedeutung – sowohl beim Aufbau eigener Datenplattformen als auch bei Kooperationen mit Dritten. Sie beeinflussen deren technische, organisatorische und rechtliche Ausgestaltung maßgeblich und stellen ein zentrales strategisches Entscheidungskriterium dar.

1.4 Wie DA, DGA und DSGVO ineinandergreifen

Während der Data Governance Act (DGA) freiwillige Datenweitergaben über klar definierte Governance-Modelle ermöglicht, schafft der EU Data Act (DA) die rechtliche Grundlage für die Nutzung eigener oder nutzerbasierter Datenzugangsrechte und Datenzugriffe in Fällen von Notlagen. Für Kommunen ergibt sich daraus ein übergreifender europäischer Rahmen, der die Nutzung externer Daten rechtlich einbettet – sei es über freiwillige Kooperationen, die Nutzung von Datenvermittlungsdiensten oder, in Notlagen, über gesetzlich geregelte Zugriffsrechte.

Der Data Governance Act zielt darauf ab, organisatorische und vertrauensbildende Strukturen zu schaffen, etwa durch neutrale Datenmittler, Regelungen zur Weitergabe öffentlicher Daten und das Konzept datenaltruistischer Organisationen. Der EU Data Act ergänzt diese Ansätze, indem er festlegt, unter welchen Voraussetzungen Daten verpflichtend bereitgestellt werden müssen. Allerdings bleibt die praktische Umsetzung dieser Verpflichtungen – insbesondere bei Datenteilung in Fällen außergewöhnlicher Notwendigkeit – bislang offen. Der Begriff ist weit gefasst und es fehlen noch klare Verfahren und Zuständigkeitsregelungen, was die Anwendung in der Praxis bislang erschwert. Die Datenschutz-Grundverordnung (DSGVO) bildet dabei den verbindlichen Rahmen für den Umgang mit personenbezogenen Daten und bleibt auch bei der Anwendung von DGA und DA uneingeschränkt maßgeblich.

2. Kommunalen Datenzugang im europäischen Rechtsrahmen

Kommunen bewegen sich beim Erheben und Verarbeiten von Daten im Spannungsfeld zwischen Datenschutz und der Notwendigkeit gemeinwohlorientierter Datennutzung. Maßgeblich sind hier die Einhaltung der Datenschutz-Grundverordnung (DSGVO) sowie die neuen Möglichkeiten und Pflichten durch den EU Data Act (DA) und Data Governance Act (DGA).

Eine wesentliche rechtliche Fragestellung beim Datenteilen ist zunächst, ob und inwieweit personenbezogene Daten betroffen sind. Die Erhebung, Verarbeitung und Weitergabe personenbezogener Daten (auch durch Kommunen) ist nur zulässig, wenn eine Rechtsgrundlage besteht, z. B. eine konkrete gesetzliche Ermächtigung oder eine informierte, freiwillige Einwilligung der betroffenen Person. Die maßgebliche Grundlage bildet die Datenschutz-Grundverordnung, insbesondere Art. 6 Abs. 1, ergänzt durch nationale Gesetze wie das Landesdatenschutzgesetz (LDSG) und einschlägige kommunale Regelungen. Innerhalb der DSGVO gelten zudem unterschiedlich strenge Anforderungen: Besonders sensible Kategorien personenbezogener Daten wie etwa Gesundheitsdaten oder Daten zur ethnischen Herkunft unterliegen zusätzlichen Schutzvorschriften und dürfen nur in Ausnahmefällen verarbeitet werden (Art. 9 DSGVO). Auch vermeintlich harmlose Daten können je nach Kontext als personenbezogen gelten, etwa wenn durch Kombination Rückschlüsse auf Einzelpersonen möglich werden. Nicht-personenbezogene Daten – etwa Sensordaten ohne Personenbezug – können grundsätzlich deutlich freier geteilt und genutzt werden. Gleichwohl gelten auch hier rechtliche Rahmenbedingungen z. B. aus dem EU Data Act oder branchenspezifischen Vorschriften wie der Schutz von Geschäfts- oder Betriebsgeheimnissen.

Wenn Kommunen Daten nutzen möchten, die außerhalb der Verwaltung entstehen, so etwa bei Mobilitätsanbietern, Zahlungsdienstleistern oder direkt bei den Bürger:innen, dann stehen ihnen verschiedene Ansätze offen. In den folgenden Abschnitten werden verschiedene Modelle vorgestellt und es wird aufgezeigt, welche rechtlichen Spielräume und Grenzen dabei jeweils zu beachten sind.

2.1 Freiwillige Datenbereitstellung

2.1.1 Die kommunale Datenplattform

Datenplattformen sind technische und organisatorische Infrastrukturen, mit denen sich verschiedene Formen der Datenerhebung und -nutzung operativ umsetzen lassen. Sie können für Kommunen eine zentrale Rolle spielen, wenn es beispielsweise darum geht, direkt von Bürger:innen, Unternehmen oder anderen Stellen zur Verfügung gestellte Daten auf der Basis von Einwilligungen oder im Rahmen der kommunalen Aufgabenerfüllung zu verarbeiten. Die Kommune kann eine eigene Plattform aufbauen oder bestehende Plattformen nutzen, über die Bürger:innen, Unternehmen oder öffentliche Stellen ihre Daten direkt für gemeinwohlorientierte Zwecke bereitstellen können – etwa für eine bessere Verkehrsplanung oder bedarfsgerechte Versorgungsangebote.

Die Plattform stellt dabei nicht nur die notwendige IT-Infrastruktur bereit – etwa für Speicherung, Zugriffskontrolle, Schnittstellenmanagement und Datenverarbeitung –, sondern ermöglicht auch die Umsetzung der rechtlichen Anforderungen wie Datenschutz, Informationspflichten, Widerrufsmöglichkeiten, Zweckbindung oder Löschung.

Sie schafft damit die Voraussetzungen für ein systematisches Einwilligungsmanagement, die Absicherung von Zugriffsrechten sowie für Maßnahmen zur Gewährleistung von Datensicherheit und Vertraulichkeit.

Mit einer eigenen Datenplattform übernimmt die Kommune allerdings die vollständige Verantwortung sowohl für das datenschutzrechtlich erforderliche Einwilligungsmanagement als auch für die technische Umsetzung und Kommunikation. Gerade Letzteres ist entscheidend: Die Kommune muss das Vertrauen der Menschen gewinnen, indem sie offenlegt, welche Daten zu welchem Zweck verarbeitet werden und welchen konkreten Nutzen dies für das Gemeinwohl hat.

Alternativ zum Aufbau einer eigenen kommunalen Datenplattform für die Datenerhebung und -nutzung können Kommunen auf bestehende Lösungen und Kooperationen zurückgreifen, die technische Standards, Interoperabilität und Governance-Strukturen bereits integriert haben. Diese Plattformmodelle reduzieren Entwicklungsaufwand und -kosten und bieten einen niedrighschwelligeren Einstieg in eine kommunal vernetzte Nutzung von Informationen.



Technische Anforderungen an nachhaltiges Datenteilen – Impulse aus dem EU Data Act (DA)

Auch wenn Daten – rein technisch betrachtet – durchaus über einfache Kanäle wie E-Mail übermittelt werden könnten, ist dies aus datenschutzrechtlicher, technischer und organisatorischer Sicht keineswegs empfehlenswert. Solche Wege bieten weder ausreichende Sicherheit noch eine nachvollziehbare Protokollierung. Zudem erfordert der Austausch von Daten in der Regel die Einhaltung bestimmter Standards (z. B. technische und semantische). Der Aufbau bzw. die Nutzung einer geeigneten technischen Infrastruktur ist daher nicht nur eine Frage der rechtlichen Absicherung, sondern die Voraussetzung dafür, Daten nachhaltig, effizient und wiederverwendbar nutzbar zu machen.

Der EU Data Act liefert hierzu wichtige Hinweise: Er konkretisiert, welche Maßnahmen notwendig sind, um Datenteilen rechtlich zulässig, technisch möglich und langfristig nutzbar zu gestalten. So schreibt die Verordnung in Art. 5 Abs. 1, 7 und Art. 11 vor, dass Daten maschinenlesbar, zugänglich und nutzbar zur Verfügung gestellt werden müssen – bei gleichzeitiger Wahrung von Datenschutz und Geschäftsgeheimnissen. Eine besondere Rolle spielt dabei die Interoperabilität: Standardisierte Schnittstellen und exportierbare Datenformate sollen verhindern, dass Lock-in-Effekte entstehen, und sicherstellen, dass Daten auch über Systemgrenzen hinweg wiederverwendet werden können. Dies betrifft nicht nur die technische Ebene, sondern auch semantische und organisatorische Standards. Für Kommunen und andere datenverarbeitende Akteure bedeutet dies: Die Anforderungen des EU Data Act bieten eine Orientierung, wie sich Datenerhebung, -austausch und -auswertung langfristig gestalten lassen.

Gerade im kommunalen Bereich müssen diese Prinzipien nicht zwingend durch den Aufbau einer vollständig eigenen Datenplattform erfüllt werden. In Deutschland haben sich inzwischen offene und praxisorientierte Modelle etabliert, die zeigen, dass viele Städte und Regionen auf modulare, interoperable und kooperative Infrastrukturen setzen können, um bestehende Datenbestände sicher und rechtssicher zu teilen. Während einige Plattformmodelle primär auf die strukturierte Vernetzung und den sicheren Austausch bereits vorhandener kommunaler Daten ausgerichtet sind, zielen andere Konzepte stärker auf die fortlaufende Integration und Nutzung externer Datenquellen ab, um kommunale Prozesse datengetrieben weiterzuentwickeln.

Beispiele sind das Projekt „Connected Urban Twins (CUT)“³, die interkommunale Datenplattform des Projekts „SmartWendelerLand“⁴ und die „CIVITAS/CORE-Gemeinschaft“⁵.

Zudem gibt es eine Reihe kostenfreier und kostenpflichtiger „Software as a Service“-Angebote (SaaS-Angebote) sowie Open-Source-Anwendungen am Markt und in Entwicklung, wie etwa den Urban Stack der Stadt Gütersloh⁶. Dies zeigt, dass deutsche Kommunen nicht (ausschließlich) auf Eigenentwicklungen angewiesen sind, um datenbasierte Strategien umzusetzen.

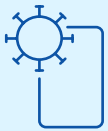
2.1.2 Datenbereitstellung über datenaltruistische Organisationen (Art. 16 ff. DGA)

Wie in Kapitel 1 zu den gesetzlichen Grundlagen dargestellt, eröffnet der Data Governance Act Kommunen theoretisch neue Möglichkeiten, auf freiwillig bereitgestellte Daten zuzugreifen. Zwei zentrale Mechanismen stehen dabei im Vordergrund: Datenaltruistische Organisationen und Datenvermittlungsdienste (Intermediäre). Für Kommunen lohnt es sich, beide Ansätze unter dem Gesichtspunkt der praktischen Umsetzung und strategischen Chancen zu betrachten.

Das Modell „Datenaltruistische Organisationen“ eignet sich, wie bereits in Kapitel 1.2 erläutert, insbesondere für die Verarbeitung sensibler personenbezogener Daten im Rahmen gemeinwohlorientierter Projekte – etwa in der öffentlichen Gesundheitsförderung, der Sozialplanung oder der Umweltbeobachtung.



Beispiele für datenaltruistische Projekte:



Corona-Datenspende-App (Betrieb im Mai 2023 abgeschaltet): Vom Robert Koch-Institut initiiert, ermöglichte sie die Sammlung von Gesundheits- und Bewegungsdaten freiwilliger Nutzer:innen, um die Ausbreitung von COVID-19 besser zu verstehen und die Forschung zu unterstützen. Die Daten wurden anonymisiert und ausschließlich zu gemeinwohlorientierten Zwecken genutzt. Siehe auch [hier](#).



Smart Citizen: Ein internationales Projekt, das Bürger:innen befähigt, Umweltdaten wie Luftqualität oder Lärmpegel zu erfassen und offen bereitzustellen. Die Plattform fördert so die freiwillige Datenspende für Umwelt- und Klimaschutzprojekte. Siehe auch [hier](#).

Ob sich datenaltruistische Ansätze etablieren und als praktikable Modelle durchsetzen, ist offen.⁷ Ein Vorhaben der EU-Kommission, ein Regelwerk („Rulebook“) zu erstellen, das zusätzliche Informationen zu den Pflichten anerkannter datenaltruistischer Organisationen nach dem Data Governance Act enthalten sollte, wurde vorerst zurückgestellt. Das geplante Regelwerk sollte unter anderem Vorgaben zu Informationspflichten, technischen und Sicherheitsanforderungen sowie Empfehlungen zu Interoperabilitätsstandards umfassen. Siehe auch [hier](#).

3 Weitere Informationen zum Projekt „Connected Urban Twins“

4 Weitere Informationen zum Projekt „SmartWendelerLand“

5 Weitere Informationen zur „CIVITAS/CORE-Gemeinschaft“

6 Weitere Informationen zu „Urban Stack“

7 Zum Stand der Veröffentlichung waren keine Organisationen als datenaltruistische Organisationen im EU-Register registriert. Siehe auch: [EU-Register der anerkannten datenaltruistischen Organisationen | Gestaltung der digitalen Zukunft Europas](#)

Aus kommunaler Perspektive läge der Mehrwert insbesondere darin, zentrale Aufgaben rund um die Einholung und Verwaltung von Einwilligungen sowie die operative Datenverarbeitung an spezialisierte datenaltruistische Organisationen und Datenvermittlungsdienste auszulagern. Diese Organisationen übernehmen das gesamte Einwilligungsmanagement, sorgen für Transparenz gegenüber den betroffenen Personen und tragen die Verantwortung für eine datenschutzkonforme Verarbeitung der von ihnen geführten personenbezogenen Daten. Erhält die Kommune ausschließlich hinreichend aggregierte, anonymisierte oder anderweitig nicht personenbezogene Auswertungen und nutzt sie diese für ihre Aufgabenwahrnehmung, dann tritt sie für die zugelieferten Ergebnisse nicht als Verantwortliche für die zugrunde liegenden personenbezogenen Verarbeitungen auf – ein klarer Vorteil, insbesondere bei komplexen oder ressourcensensiblen Vorhaben.

Da die Zwecke dieser Organisationen auf die Förderung des Gemeinwohls ausgerichtet sein müssen, wären solche Kooperationen vor allem dort sinnvoll, wo kein unmittelbarer kommerzieller Nutzen angestrebt wird, sondern die Nutzung der Daten dem öffentlichen Interesse und dem Gemeinwohl dient.

2.1.3 Nutzung von Datenvermittlungsdiensten (Art. 10 ff. DGA)

Datenvermittlungsdienste nach dem DGA (vgl. Kapitel 1.2) sind Anbieter, die zwischen Datengeber:innen und Datennutzer:innen eine technische und organisatorische Brücke schlagen. Sie stellen Plattformen oder Infrastrukturen bereit, über die Daten unter klaren Rahmenbedingungen geteilt werden können, etwa über Schnittstellen, Datenräume oder Portale. Sie dürfen zwar auf kommerzieller Basis arbeiten, müssen jedoch neutral bleiben und dürfen – im Gegensatz etwa zu Datengenossenschaften – keine eigenen wirtschaftlichen Interessen an der Datennutzung verfolgen.



Datenvermittlungsdienste: Bereit für die Praxis?

Datenvermittlungsdienste im Sinne des Data Governance Act (DGA) befinden sich derzeit noch in einer frühen Umsetzungsphase. Der rechtliche Rahmen ist mit klaren Vorgaben zu Neutralität, Zweckbindung und Transparenz geschaffen, doch die praktische Ausgestaltung und Etablierung tragfähiger Betreiberstrukturen steht noch am Anfang.

Der Markt ist bislang durch Pilotprojekte und Forschungsinitiativen geprägt. Operative Intermediäre, die bereits vollständig den Anforderungen des Data Governance Act entsprechen, sind derzeit nur vereinzelt vorhanden. Herausforderungen bestehen insbesondere in der Entwicklung nachhaltiger Geschäftsmodelle, die Neutralität und Wirtschaftlichkeit miteinander vereinbaren, sowie in der technischen und organisatorischen Integration in bestehende Datenräume und Verwaltungsstrukturen.

Für Kommunen bedeutet dies, dass Datenvermittlungsdienste ein hohes zukünftiges Potenzial für den rechtssicheren und standardisierten Austausch von Daten mit externen Partnern bieten, derzeit jedoch noch keinen flächendeckend verfügbaren Standard darstellen. Entsprechende Kooperationen sollten daher als Entwicklungs- oder Pilotvorhaben verstanden und mit Blick auf Reifegrad, Zuständigkeiten und Governance sorgfältig gestaltet werden.

Für Kommunen eröffnet die Zusammenarbeit mit Datenvermittlungsdiensten erhebliche Chancen: Sie erhalten Zugang zu einer breiten Vielfalt an freiwillig bereitgestellten Daten – von Unternehmen, anderen öffentlichen Stellen oder Forschungseinrichtungen. Anders als datenaltuistische Organisationen, die meist auf gemeinwohl-orientierte Zwecke und freiwillig gespendete Daten beschränkt sind, können Datenvermittlungsdienste einen effizienten und flexiblen Austausch unterschiedlichster Daten ermöglichen. Das erweitert die Handlungsmöglichkeiten auch von Kommunen erheblich und schafft die Grundlage für innovative, datengetriebene Projekte.

Darüber hinaus können Vermittlungsdienste eine wichtige Rolle bei der Sicherung von Rechtskonformität, Transparenz und Standardisierung, z. B. im Bereich der technischen Sicherheit oder der Umsetzung von Einwilligungsprozessen übernehmen.

2.1.4 Datenteilen über vernetzte Produkte oder verbundene Dienste (EU Data Act)

Eine weitere Möglichkeit der Nutzung freiwillig geteilter Daten eröffnet der EU Data Act über Art. 5 (vgl. Kapitel 1.1). Bürger:innen und Organisationen, die vernetzte Produkte oder verbundene Dienste wie z. B. Smart-Home-Anwendungen, Smartwatches, Fahrzeugtelematiksysteme oder Cloud-basierte Funktionsanwendungen nutzen (Nutzer:innen), können die bei der Nutzung dieser Produkte entstehenden Daten von den jeweiligen Dateninhabern, wie Geräteherstellern und Anbietern der damit verbundenen digitalen Dienste, direkt an Dritte – darunter auch Kommunen – weiterleiten lassen.

Die Entscheidung über eine solche Datenfreigabe liegt allein bei den Nutzer:innen; der EU Data Act verpflichtet lediglich die Dateninhaber, diese Weitergabe technisch und rechtlich zu ermöglichen und sicherzustellen, dass sie unter fairen, angemessenen und nichtdiskriminierenden Bedingungen erfolgt.



Neue Spielräume durch den EU Data Act?

Unternehmen oder Organisationen konnten bereits vor dem Inkrafttreten des EU Data Act unabhängig von einer Nutzeranweisung eigenständig entscheiden, bestimmte Daten zu teilen, etwa zu Forschungs-, Kooperations- oder Innovationszwecken.

In der Praxis ist ein solcher Austausch jedoch häufig gescheitert: an fehlender Transparenz über die Verfügbarkeit von Daten, an mangelnden Anreizen sowie am wirtschaftlichen Aufwand für die Bereitstellung. Der EU Data Act greift dieses Problem auf, indem er verbindliche, transparente Rahmenbedingungen für den Datenaustausch schafft, insbesondere klare Zugangs- und Weitergaberechte zugunsten der Nutzer:innen vernetzter Produkte festlegt, Anreize über faire (FRAND)Vergütungsregeln (Fair, Reasonable and Non-Discriminatory) setzt, Missbrauch und unfaire Vertragsklauseln einschränkt und so den wirtschaftlichen Aufwand sowie die Unsicherheit beim Teilen von Daten deutlich reduziert.

Für Kommunen eröffnet sich damit ein zusätzlicher Spielraum: Neben den neuen, nutzerbasierten Datenzugangsrechten und entsprechenden Pflichten für Dateninhaber nach dem EU Data Act bleiben die bereits bestehenden Möglichkeiten freiwilliger Datenweitergabe bestehen und erhalten durch die klareren rechtlichen Rahmenbedingungen zusätzliche Rechtssicherheit. Beides zusammen kann neue Formen datenbasierter Zusammenarbeit schaffen.

Der Ablauf ist dabei klar geregelt: Nutzer:innen geben nach Art. 5 Abs. 1 DA eine ausdrückliche Weisung an den Dateninhaber (etwa den Hersteller oder Anbieter der damit verbundenen digitalen Dienste), die Daten an die Kommune zu geben. Für Kommunen hat dieses Verfahren einen entscheidenden Vorteil: Die rechtliche Verantwortung für die Einhaltung von z. B. datenschutzrechtlichen Vorgaben bei der Übergabe verbleibt beim Dateninhaber (Art. 5 und 8 DA) und Kommunen erhalten die Daten ohne eigenes rechtliches Risiko – zumindest, wenn diese anonymisierte oder pseudonymisierte Daten ohne Schlüssel bekommen. Wichtig ist allerdings: Dieser Weg setzt immer die aktive Mitwirkung der Nutzer:innen voraus. Kommunen können die Übertragung nicht selbst veranlassen, sondern sind darauf angewiesen, dass z. B. Bürger:innen und Unternehmen ihr Recht nach Art. 5 DA nutzen und die Weitergabe durch den Datenhalter initiieren.

Auch hier soll der Vollständigkeit halber angemerkt werden, dass die Kommune – als Nutzer vernetzter Geräte oder digitaler Dienste – das datenhaltende Unternehmen anweisen kann, die durch ihre Nutzung entstandenen Daten an die Kommune selbst herauszugeben.

2.2 Verpflichtende Datenbereitstellung im Ausnahmefall

2.2.1 Rechtsgrundlagen und Voraussetzungen nach Art. 14 ff. DA

Wie in Kapitel 1.1 beschrieben, sieht der EU Data Act (Art. 14 bis 22) neben freiwilligen, nutzerbasierten Modellen auch Situationen vor, in denen Unternehmen verpflichtet werden können, Daten an öffentliche Stellen weiterzugeben. Dies ist jedoch ausschließlich in Ausnahmefällen vorgesehen. Solche „außergewöhnlichen Notwendigkeiten“ liegen gemäß Art. 15 DA etwa dann vor, wenn es um den Schutz der öffentlichen Sicherheit, der Gesundheit oder um die Bewältigung von Krisen wie Naturkatastrophen oder Pandemien geht und die dafür notwendigen Daten nicht rechtzeitig und wirksam anderweitig beschafft werden können.

In solchen Fällen dürfen öffentliche Stellen Daten von privaten Dateninhabern anfordern, allerdings nur unter strengen Voraussetzungen. Die anfragende Stelle muss darlegen:

- warum genau diese Daten notwendig sind,
- zu welchem konkreten Zweck sie verwendet werden sollen,
- für welche Dauer sie benötigt werden und
- wie personenbezogene oder vertrauliche Informationen geschützt werden, falls auf solche Daten nicht verzichtet werden kann.

Zudem ist zu begründen, warum gerade dieser Dateninhaber angesprochen wird – etwa, weil er als einziger über die relevanten Informationen verfügt. Diese Form der verpflichtenden Datenbereitstellung ist somit stark begrenzt: sowohl in Bezug auf die konkrete Notsituation als auch hinsichtlich des Zweckes, des Umfangs und der Dauer der Datennutzung.



Haben Datenhalter einen Anspruch auf Entschädigung?

Anspruch auf Entschädigung für die Bereitstellung der Daten gemäß DA:

- **In akuten Notlagen** (Art. 15 Abs. 1 lit. a DA) erfolgt die Bereitstellung unentgeltlich – mit der Ausnahme, dass Kleinst- oder Kleinunternehmen eine Entschädigung verlangen dürfen (Art. 20 Abs. 1 Satz 2 DA).
- Außerhalb akuter Notlagen können Unternehmen in Fällen der **außergewöhnlichen Notwendigkeit** (Art. 15 Abs. 1 lit. b DA) eine faire Entschädigung verlangen, die sich an den tatsächlichen technischen und organisatorischen Aufwänden orientiert, z. B. für Anonymisierung oder Pseudonymisierung (Art. 20 Abs. 2 DA).
- Wird eine Datenbereitstellung zur **Erstellung amtlicher Statistiken** angefragt, kann die Entschädigung entfallen, sofern nationales Recht dies vorsieht (Art. 20 Abs. 4 DA).

Damit gilt: Eine Entgeltlichkeit kommt nur in eng definierten Ausnahmen außerhalb einer Notlage in Betracht. In klassischen Krisensituationen, wie einer Naturkatastrophe oder einer Pandemie, ist die Datenbereitstellung grundsätzlich unentgeltlich – mit wenigen, klar begrenzten Ausnahmen.

2.2.2 Praktische Herausforderungen bei der verpflichtenden Datenweitergabe nach Art. 14 DA

Wenngleich der EU Data Act unter bestimmten Voraussetzungen eine verpflichtende Datenweitergabe durch Unternehmen an öffentliche Stellen vorsieht, kann die praktische Umsetzung herausfordernd sein:

Identifikation relevanter Datenquellen

Öffentliche Stellen wissen möglicherweise nicht, welche Unternehmen relevante Daten besitzen, solange Verzeichnisse, Klassifizierungen oder transparente Metadaten zur Datenverfügbarkeit fehlen. Auch Unternehmen selbst können unsicher sein, ob ihre Daten im konkreten Fall tatsächlich relevant sind, insbesondere ohne ein gemeinsames Begriffs- und Zweckverständnis.

Zeitverzug durch rechtliche Nachweispflichten

Behörden müssen die außergewöhnliche Notwendigkeit im öffentlichen Interesse nachweisen und darlegen, warum Daten nicht anderweitig verfügbar sind und warum gerade dieses Unternehmen verpflichtet werden soll. Da die außergewöhnliche Notwendigkeit unter dem EU Data Act unterschiedlich ausgelegt werden kann, bleibt im Zweifelsfall unklar, ob der konkrete Fall tatsächlich darunterfällt. Beides kann insbesondere in zeitkritischen Situationen zu Verzögerungen führen.

Fehlende organisatorische Ansprechstrukturen

Viele Unternehmen haben keine klar definierten internen Zuständigkeiten für derartige behördliche Anfragen. Fehlen zudem Rahmenvereinbarungen oder standardisierte Vertragsklauseln, steigt die Sorge vor Haftungsrisiken, Verletzungen von Geschäftsgeheimnissen oder Reputationsschäden. Dies führt häufig zu Reibungsverlusten oder Verzögerungen.

Fehlende Interoperabilität und technische Schnittstellen

Ohne geeignete technische Infrastruktur beim Datenempfänger und standardisierte oder getestete Übermittlungswege zwischen öffentlicher Stelle und Datenhalter:in können proprietäre Datenformate, fehlende Semantik oder fehlende Application Programming Interfaces (APIs) die automatisierte Datenübertragung erschweren. Bei fehlender Vorkonfiguration entsteht zusätzlicher Aufwand bei der technischen Integration und Umwandlung der Daten.

Datenschutz und Geheimhaltung

Personenbezogene und sensible Daten unterliegen weiterhin strikt der Datenschutz-Grundverordnung (DSGVO). Gleichzeitig müssen vertrauliche Informationen und Geschäftsgeheimnisse geschützt werden. Auch bei Notfallzugriffen sind Zweckbindung, Sicherheitsvorkehrungen und Nachweispflichten einzuhalten, was zusätzliche Abstimmungen zwischen Datenhalter:innen und Kommunen erforderlich macht. Zudem verlangt der EU Data Act (gemäß Art. 17 Abs. 2 lit. e), dass personenbezogene Daten vor einer Weitergabe anonymisiert oder pseudonymisiert werden müssen.

Fehlende operationelle Vorgaben und Zuständigkeiten

In Ermangelung eines von der EU-Kommission in Art. 17 Abs. 6 DA vorgesehene Musterverfahrens für Datenanforderungen fehlt öffentlichen Stellen ein klarer Rahmen, wie sie Daten im Notfall formell anfordern und koordinieren können. Da insbesondere Zuständigkeiten und Abläufe innerhalb der Verwaltung unklar bleiben, werden Kommunen künftig eigene Verfahren und Ansprechstrukturen definieren müssen, um im Bedarfsfall handlungsfähig zu sein.

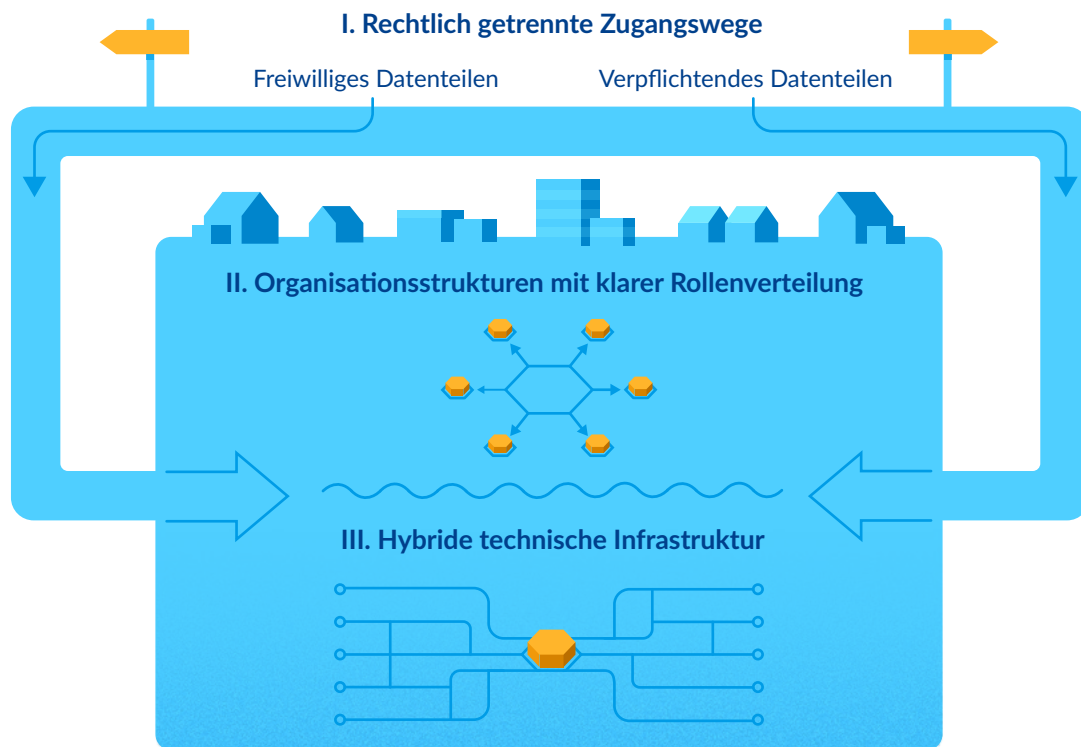
2.3 Das hybride Modell: Freiwilligkeit und Pflicht strategisch kombiniert

Sowohl freiwilliges Datenteilen als auch verpflichtende Datenzugänge stoßen in der kommunalen Praxis auf Hürden. Freiwillige Modelle erfordern viel Engagement und Kooperation von Bürger:innen oder datenhaltenden Organisationen, während verpflichtende Zugriffe nach dem EU Data Act nur in klar definierten Ausnahmesituationen möglich sind. Technisch und organisatorisch bestehen bei beiden Ansätzen viele Überschneidungen: Die gleiche Infrastruktur kann für beide Ansätze genutzt werden und rechtliche Vorgaben lassen sich stärker zusammendenken. Ein zukunftsorientierter Ansatz für Kommunen besteht daher darin, freiwillige und verpflichtende Zugänge auf Basis gemeinsamer technischer und organisatorischer Strukturen zu kombinieren.

2.3.1 Zielsetzung

Ein hybrides Modell verfolgt das Ziel, Dateninfrastrukturen so zu gestalten, dass sie sowohl im Alltag für freiwillige Kooperationen als auch in Krisensituationen für gesetzlich verpflichtende Datenzugriffe nutzbar sind (Abbildung 1). Diese doppelte Nutzbarkeit steigert die Effizienz, reduziert den Umsetzungsaufwand im Ernstfall und sichert die langfristige Datenverfügbarkeit für kommunale Aufgaben.

ABBILDUNG 1 Hybrides Modell



Hybrides Modell: Sowohl bei technischer Infrastruktur als auch bei rechtlichen und organisatorischen Rahmenbedingungen können Synergien genutzt werden, indem verpflichtendes und freiwilliges Datenteilen zusammengedacht werden.

Quelle: eigene Darstellung

| BertelsmannStiftung

2.3.2 Voraussetzungen und Gestaltungsprinzipien

Ein funktionierendes hybrides Modell stützt sich auf drei Säulen:

I. Rechtlich getrennte Zugangswege

Da freiwillige und verpflichtende Zugriffe unterschiedliche Rechtsgrundlagen haben (z. B. Einwilligung vs. Art. 15 DA), müssen technische und organisatorische Maßnahmen eine klare Trennung sicherstellen, z. B. über separate Verarbeitungsumgebungen oder logisch getrennte Zugriffspfade. Auch Widerrufsrechte und Zweckbindungen müssen individuell abgebildet werden können.

II. Governance und Rollenklarheit

Das hybride Modell erfordert klar definierte Zuständigkeiten zwischen Kommune, Dateninhabern, Intermediären und ggf. datenaltruistischen Organisationen. Zuständigkeiten und Verantwortlichkeiten für Sicherheit, Informationspflichten, Fehlerbehandlung oder Auskunftersuchen müssen vertraglich, technisch und prozessual verankert sein.

III. Hybride technische Infrastruktur

Eine zentrale technische Infrastruktur muss den Zugriff auf unterschiedliche Datenquellen ermöglichen, unabhängig davon, ob diese auf Einwilligungen oder gesetzlichen Anspruchsgrundlagen beruhen. Wesentlich ist die Abbildung zentraler datenschutzrelevanter Funktionen wie Einwilligungsmanagement, Zugriffskontrolle, Protokollierung, Anonymisierung und ggf. rollenbasierter Zugriffsrechte. Dabei sollten Standards so gewählt werden, dass sie sowohl Alltagsdatenflüsse als auch Notfallszenarien abdecken.

2.3.3 Die kommunale Datenplattform als Basisstruktur

Ob eine Kommune eine eigene Plattform betreibt oder mit externen Intermediären kooperiert, hängt von Ressourcen, Zielen und Komplexität des Datenvorhabens ab. In jedem Fall bildet die Plattform das Rückgrat für kontinuierliche und krisenfeste Datennutzung. Sie ermöglicht eine abgestufte, zweckgebundene Nutzung verschiedener Datenarten und somit unterschiedliche Kooperationsformen, z. B. mit direkt beteiligten Bürger:innen, Datenvermittlungsdiensten und datenaltruistischen Organisationen.

Da im Vorfeld oft unklar ist, welche Daten im Notfall benötigt werden, erlaubt eine flexibel konzipierte Infrastruktur, schneller und gezielter zu reagieren. Eine kommunale Plattform dient somit nicht nur als technisch-organisatorische Lösung, sondern auch als strategischer Ansatz zur Absicherung kommunaler Handlungsfähigkeit.

2.3.4 Datenschutzrechtliche Anforderungen als strategischer Entscheidungsfaktor

Die datenschutzrechtliche Einordnung ist zentral für die Ausgestaltung eines hybriden Modells. Sie beeinflusst, ob eine Kommune selbst als datenschutzrechtlich Verantwortliche agiert, z. B. beim Betrieb einer eigenen Plattform, oder ob Intermediäre oder datenaltruistische Organisationen durch eigene Datenerhebung und -verarbeitung diese Rolle übernehmen und der Kommune lediglich aggregierte bzw. anonymisierte Ergebnisse zur Verfügung stellen.

Die Anforderungen der Datenschutz-Grundverordnung wirken sich auch auf die technische Architektur der Plattform und das jeweilige Governance-Modell aus. Je nach Modell liegt die datenschutzrechtliche Verantwortung bei der Kommune selbst oder bei kooperierenden Dritten. Eine bewusste Entscheidung darüber, welche Kontroll- und Verantwortungsbereiche bei der Kommune verbleiben und welche an Partner übertragen werden, ist daher erforderlich.

2.4 Zusammenfassung: Chancen, Bedingungen, Herausforderungen

Kommunen stehen vor der Herausforderung, eine zunehmend komplexe Datenlandschaft rechtssicher, technisch tragfähig und im Sinne des Gemeinwohls zu erschließen. Die Analyse zeigt, dass der europäische Rechtsrahmen – insbesondere durch den EU Data Act und Data Governance Act – verschiedene Zugangspfade und -modelle bietet, jedoch keine Standardlösung vorgibt. Kommunen benötigen daher auf sie zugeschnittene Strategien, die juristische Anforderungen, technische Machbarkeit und gesellschaftliche Akzeptanz zusammenführen.

2.4.1 Datenzugänge im Überblick

Kommunen können auf unterschiedliche Weise auf Daten zugreifen:

- freiwillige Bereitstellungen durch Unternehmen oder Bürger:innen, z. B. Daten vernetzter Produkte über eigene Datenplattformen,
- Kooperationen mit anderen Kommunen oder regionalen Partnern zur gemeinsamen Datennutzung,
- Zusammenarbeit mit gemeinnützigen datenaltruistischen Organisationen oder Datenvermittlungsdiensten gemäß Data Governance Act, deren Modelle gesetzlich vorgesehen, in der Praxis jedoch erst im Aufbau sind,

- projektbezogene oder vertraglich geregelte Partnerschaften mit privatwirtschaftlichen Datenhalter:innen, etwa im Rahmen gemeinsamer Anwendungen oder Innovationsprojekte,
- verpflichtender Datenzugriff in Ausnahmefällen nach Art. 14 ff. DA.

Jeder Datenzugang ist mit eigenen Voraussetzungen, Risiken und rechtlichen Pflichten verbunden. Besonders der gesetzlich verpflichtende Zugang bringt einen hohen Nachweisaufwand mit und erfordert umfassende Kenntnisse der Datenlandschaft sowie technische und organisatorische Vorkehrungen. Ohne vorherige Abstimmung und vorbereitende Maßnahmen seitens der Kommunen und der Datenhalter:in ist dieser rechtliche Zugang deshalb nur begrenzt wirksam.

2.4.2 Datenintermediäre und Datenaltruismus-Organisationen

Der Data Governance Act führt neue Modelle für den Datenaustausch ein – neutrale Datenvermittlungsdienste und gemeinnützige Datenaltruismus-Organisationen. Beide sollen künftig dazu beitragen, Datenteilung auf einer vertrauenswürdigen, transparenten Grundlage zu ermöglichen und faire Zugänge zu fördern. Noch handelt es sich um junge Strukturen, die sich in der Praxis erst entwickeln und deren institutionelle Verankerung in vielen Mitgliedstaaten, auch in Deutschland, noch aussteht. Für Kommunen ist es dennoch sinnvoll, diese Entwicklungen zu verfolgen: Sie könnten mittelfristig eine wichtige Rolle spielen, um sektorübergreifende Datennutzungen und Kooperationen auf eine stabile rechtliche und organisatorische Basis zu stellen.

2.4.3 Rechts- und Governance-Anforderungen

Ein zentrales Entscheidungskriterium für alle Datenzugangswege ist die datenschutzrechtliche Verantwortung: Sie bestimmt, wer die Hoheit über die Datenverarbeitung hat, wer Informationspflichten erfüllen muss und wer für die Sicherheit der Daten haftet. Bei freiwillig bereitgestellten personenbezogenen Daten kann dies zu erheblichem organisatorischem Aufwand führen, insbesondere bei Verwaltung von Einwilligungen, Widerrufen und technischen Nutzungsbegrenzungen

Kommunen müssen daher strategisch abwägen, ob sie diese Verantwortung selbst tragen, z. B. beim Betrieb einer eigenen Plattform, oder ob sie Aufgaben an vertrauenswürdige Partner delegieren. In beiden Fällen müssen die Anforderungen der Datenschutz-Grundverordnung erfüllt und in Governance- und Prozessstrukturen verankert sein.

2.4.4 Strategischer Ausblick

Viele der identifizierten komplexen Anforderungen können über technische Lösungen beherrschbar gemacht werden: modulare Architekturen, rollenbasierte Zugriffskonzepte, transparente Protokollierung oder integrierte Anonymisierungsmechanismen unterstützen beispielsweise die Einhaltung des Datenschutzes. Darüber hinaus kann über zentral organisierte Aggregation und Aufbereitung von Daten deren Wiederverwendung, beispielsweise für statistische oder planungsbezogene Zwecke, gesichert werden.

Die Gestaltung kommunaler Datenkooperationen ist jedoch keine rein technische Aufgabe. Sie erfordert strategische Planung, politisches Commitment und nachhaltige Investitionen in Prozesse, Standards und Kompetenzen. Hybride Infrastrukturen können einen wirksamen Rahmen bieten, wenn sie bewusst so aufgebaut werden, dass sie nicht nur im Regelbetrieb, sondern auch in Ausnahmesituationen tragfähig sind.

Neben erkennbaren Mehrwerten für die Datengeber:innen – etwa von Bürger:innen oder Unternehmen – ist ihr Vertrauen entscheidend für reibungsloses Datenteilen. Transparente Kommunikation, individuelle Rückmeldungen, klar definierte Zwecke und einfache Beteiligungsformate erhöhen die Bereitschaft zur Datenfreigabe nachhaltig. Langfristige Partnerschaften mit vertrauenswürdigen Intermediären sichern zudem Skalierbarkeit, Rechtssicherheit sowie die Qualität der Daten und ihrer Nutzung. Auf dieser Basis können Kommunen als souveräne Datenakteure auftreten, die das Potenzial freiwilliger und verpflichtender Datenströme zum Wohl der Allgemeinheit verantwortlich und vorausschauend nutzen.

3. Erfolgsfaktoren für kommunales Verfügbarmachen und Nutzen externer Daten unter dem EU Data Act

Kommunen, die ihre datenpolitische Handlungsfähigkeit stärken und gesellschaftlich relevante Daten nutzbar machen wollen, stehen vor komplexen, aber gestaltbaren Aufgaben. Die Analyse zeigt: Es gibt zahlreiche Datenquellen, Zugangswege und Kooperationsmodelle, die jeweils spezifische Anforderungen mit sich bringen. Freiwillige Datenbereitstellungen durch Bürger:innen oder Unternehmen eröffnen große Potenziale, erfordern aber Vertrauen und Motivation. Auch in Ausnahmefällen, etwa bei Notlagen im Sinne des EU Data Act, müssen technische, organisatorische und rechtliche Strukturen vorhanden sein, um Daten verlässlich, rechtssicher und gemeinwohlorientiert zu nutzen. Daraus ergeben sich zentrale strategische Empfehlungen:

Frühzeitig handeln – nicht erst im Notfall

Die Implementierung von Dateninfrastrukturen kann eine längere Vorlaufzeit erfordern. Effektive Nutzung im Krisenfall setzt Vorsorge in ruhigen Zeiten voraus. Frühzeitige Kooperationen mit potenziellen Datenpartnern, ob Unternehmen, anderen Kommunen, Intermediären oder zivilgesellschaftlichen Organisationen, schaffen Grundlagen, die im Ernstfall schnell aktiviert werden können. Kommunen sollten technische und organisatorische Infrastrukturen mitdenken, etwa in Form einer hybriden Datenarchitektur, die freiwillige und verpflichtende Datenflüsse getrennt verarbeitet, klare Rollenverteilungen vorsieht und datenschutzrechtliche Anforderungen (Einwilligung, Informationspflichten, Löschkonzepte) von Beginn an berücksichtigt.

Motivation schaffen – durch Anreize und greifbare Mehrwerte

Entscheidend ist die Frage: Warum sollten Bürger:innen oder Organisationen ihre Daten teilen? Abgesehen von den verpflichtenden Datenherausgabepflichten im Rahmen des EU Data Act (Art. 14 ff.) müssen Bürger:innen konkrete individuelle oder gesellschaftliche Mehrwerte erkennen können, z. B. bessere Verkehrsplanung oder gezielte Services. Auch Unternehmen und andere datenhaltende Organisationen benötigen nachvollziehbare Anreize, etwa ökonomische Vorteile durch Datennutzung oder -kombination oder reputationale Mehrwerte durch sichtbares Gemeinwohlangagement („Datenspende“). Bereits das Austesten verpflichtender Datenzugänge kann motivierend wirken. Grundsätzlich sollten Prozesse niedrigschwellig, komfortabel und transparent sein, sodass die Nutzer:innen jederzeit Kontrolle über die Datenfreigabe behalten.

Vertrauen ermöglichen – durch Kommunikation, Transparenz und Governance

Freiwillige Datenbereitstellung funktioniert nur, wenn Bürger:innen oder Organisationen wissen, was mit ihren Daten passiert und warum sie benötigt werden. Die Akzeptanz hängt stark von Transparenz über Zwecke, Zugriffe und Nutzen ab. Kommunen sollten daher begleitende Kommunikationsmaßnahmen einsetzen, z. B. Informationskampagnen, niedrigschwellige Beteiligungsformate oder Pilotprojekte, die konkrete Anwendungen sichtbar machen. Gleichzeitig sind Governance-Strukturen notwendig, die Zuständigkeiten klar regeln, Missbrauch verhindern und Mitbestimmung ermöglichen.

Datenkooperationen als strategische Übung etablieren

Partnerschaften mit Dateninhabern sollten nicht nur situativ entstehen, sondern als strategisches Lernfeld genutzt werden. Besonders interkommunale Kooperationen und projektbasierte Partnerschaften bieten die Chance, gemeinsame Standards, rechtliche Vereinbarungen und technische Prozesse einzuüben, etwa zur Einwilligungserfassung, Zweckbindung oder sicheren Datenübermittlung. Zukünftig können auch neutrale Datenvermittlungsdienste oder Datenaltruismus-Organisationen nach dem Data Governance Act eine Rolle spielen, befinden sich derzeit aber noch im Aufbau. Frühzeitige Erfahrungen aus freiwilligen Kooperationen helfen Kommunen, solche neuen Modelle später gezielt zu nutzen. Gelebte Kooperationen zahlen sich insbesondere in Krisen- oder Ausnahmesituationen aus, wenn Abläufe bekannt und Rollen bereits eingeübt sind.

Fazit

Die EU-Gesetzgebung verschafft Kommunen große Gestaltungsmöglichkeiten und rechtliche Orientierung, um externe Daten gezielt für kommunale Aufgaben einzusetzen. Die Vielzahl potenzieller Datenquellen, die rechtlichen Rahmenbedingungen aus EU Data Act, Data Governance Act und Datenschutz-Grundverordnung sowie die Verantwortung bei direkter Datenerhebung über eigene Datenplattformen erfordern vorausschauende Planung, klare Governance-Strukturen und strategische Kompetenz. Besonders spannend bleibt, welche Synergien der Digital-Omnibus der Europäischen Union zwischen den verschiedenen Rechtsvorschriften aufzeigen und künftig besser miteinander verbinden wird.

Für Kommunen zeigt sich, dass die verpflichtende Datenweitergabe nach Art. 14 DA ohne vorbereitende Kooperationen, gemeinsame Standards oder vertrauensbildende Maßnahmen komplex und störungsanfällig sein kann. Strategisch sinnvoll ist es daher, bereits im Vorfeld freiwillige Kooperationsmodelle und Dateninfrastrukturen aufzubauen, um im Krisenfall schneller und effektiver agieren zu können. Frühzeitig aufgebaute, tragfähige Partnerschaften, gut konzipierte und anpassungsfähige technische Infrastrukturen sowie transparente Kommunikationsmaßnahmen sind entscheidend, um eine handlungsfähige Kommune zu schaffen, die Daten sowohl im Alltagsbetrieb als auch in Krisensituationen rechtssicher, effizient und gemeinwohlorientiert nutzen kann.

Rechtlicher Hinweis

Die vorliegende Analyse gibt einen strukturierten Überblick über geltende Rahmenbedingungen, mögliche Handlungsoptionen sowie rechtliche und organisatorische Aspekte im Kontext kommunaler Datennutzung. Sie soll zur Orientierung und Einordnung beitragen. Für die Beurteilung konkreter Einzelfälle bzw. konkreter Use Cases ist stets qualifizierter fachlicher Rat einzuholen. Die Analyse berücksichtigt den Rechtsstand zum Zeitpunkt der Erstellung des Dokuments im Januar 2026.

Adresse | Kontakt

Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
Telefon +49 5241 81-0
bertelsmann-stiftung.de

Johanna Neu
Project Manager
Zentrum für Nachhaltige Kommunen
Telefon +49 5241 81-81331
johanna.neu@bertelsmann-stiftung.de

Clara Ruthardt
Project Manager
Digitalisierung und Gemeinwohl
Telefon: +49 30 275788-189
clara.ruthardt@bertelsmann-stiftung.de