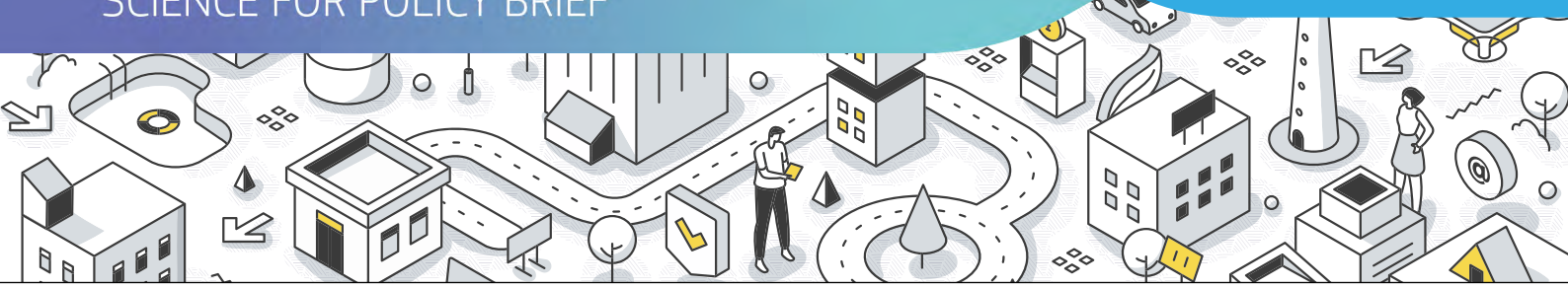
JRC138657

European Commission

SCIENCE FOR POLICY BRIEF



Data sovereignty for local governments. Enablers and considerations

HIGHLIGHTS

- **New data governance approaches are needed to counteract power imbalances** originating from the collection, use and control of large amounts of public-interest data by private companies.
- Big data collection by private companies can be an asset for local governments **appropriate governance** is set in place to **make data of public interest available**.
- **Data sovereignty for local governments** concerns their **authority and autonomy** to determine how data of public interest collected in the city can be accessed, managed, shared and used.
- **Data sovereignty clauses** (DSCs) are mandatory data-sharing provisions established by local governments to ensure access to data of public interest that is collected by companies under contractual or legal agreements with the local administration.
- **To improve the implementation and efficacy of DSCs**, organisational, technical and legal dimensions should be considered (e.g., standardised contracts and clauses, specialised data intermediaries, Privacy Enhancing Technologies, FAIR standards and transparency reporting).

Data sovereignty for local governments refers to a capacity to control and/or access data, and to foster a digital transformation aligned with societal values and EU Commission political priorities. Data sovereignty clauses are an instrument that local governments may use to compel companies to share data of public interest. Albeit promising, little is known about the peculiarities of this instrument and how it has been implemented so far. This policy brief aims at filling the gap by systematising existing knowledge and providing policy-relevant recommendations for its wider implementation.

THE DATA SOVEREIGNTY ISSUE

Data sovereignty as an EU policy objective

As part of the broader notion of technological sovereignty, data sovereignty is a prominent policy priority of the European Commission. If technological sovereignty refers to the right and ability of an entity (country, region, organisation, etc.) to develop, control, and utilise critical technologies without dependence on external entities, data sovereignty refers more specifically to the right and ability of an entity (an individual, a company, an organisation) to be in control of how their data - or data about them - are collected, stored, processed, accessed or shared. Both concepts emphasise a pursuit of **autonomy**, **control** and **security** for technology and data within a given jurisdiction or entity.

Joint Research Centre

Data sovereignty stands as one of the central pillars of the **European strategy for data** and of Common European data spaces [1], which aim to create a single market for data in Europe and to increase data access and re-use for both economic development and societal benefit. Within this context, data sovereignty implies greater control of data by European businesses, researchers and public administrations. This, in turn, is expected to generate **growth**, **innovation** and **better decision-making**, placing Europe as a leader in the data economy and society. To achieve greater data sovereignty, the European Commission has outlined policies and investments for establishing Common European Data Spaces that support data availability within and between different sectors, as well as across Member States in Europe, such as high-quality industrial data or health data [2].

Data sovereignty also concerns privacy and autonomy over personal data. In this regard, the **General Data Protection Regulation (GDPR)** increases control by European citizens and residents over their personal data, by ensuring that personal data collected within EU borders are handled in **accordance with privacy standards**, while safeguarding the rights and freedoms of individuals.

Finally, data sovereignty objectives could support the development of artificial intelligence (AI) in Europe. Given its focus on greater data availability, accessibility and autonomy, data sovereignty promotes higher control over data by European entities, thus **reducing reliance on foreign Big Tech** or on third countries as a source of data for AI. Overall, it has implications for how data are collected, including as concerns the granularity and representativity of data. This might generate **higher quality datasets** for the training of AI systems, providing resources for European start-ups, and supporting transparency and accountability over the data used to train AI systems.

Data sovereignty as data control and self-determination for different actors

The concept of data sovereignty is used in various contexts and can refer to different values and entities, comprising individuals, communities, organisations and countries. Its overarching meaning relates to control and self-determination over the handling of data that those entities contribute to generating, and thus implies their participation in data governance [3, 4]. It can be understood as a right, an ability, or an outcome of legislation, or as a means for accessing data [3]. Among the various notions captured by this term, the following can be identified according to the actors that are referred to:

- **Data sovereignty for businesses** entails the right and ability of companies to **maintain control** over how their data are used, empowering them to manage data as an economic asset and leverage its potential for innovation This implies **self-determination over** how, when and at what price others may use their data across the value chain - such as through a cloud service or by entering an EU data space - as well as safeguarding user data and ensuring they are employed in accordance with defined rules [1].
- **Data sovereignty for the individual** is intended as having the right and ability to **control one's own data**, such as for users/consumers of IoT products, inhabitants of a city or for medical patients. This notion underscores that data belongs to the individuals that generated the data (i.e., data subjects), beyond the providers or institutions that collected it. It implies, for instance, giving citizens access to their personal data that has been collected by a municipal government, and it enables them to have a certain degree of control over the ways these data are shared and used - such as choosing to reveal selected information about themselves, instead of their full identities, when interacting with city council services [5].

- **Data sovereignty for countries and public entities** is understood as the right and ability for such entities to **control and manage data generated under their jurisdictions**, while limiting the accessibility of this data to others and ensuring sensitive data remains private and protected. In this context, data sovereignty can also be the result of legislation, for instance concerning issues of national defence and/or the location of data storage in the cloud and the rights of governments to access such data.
- **Data sovereignty for indigenous peoples** is understood as the right and ability of such populations to govern the **collection, ownership, and use of data** about their communities, lands, and resources [6]. Debated mainly in countries with significant indigenous populations (e.g. such as Australia, USA and Canada), this type of data sovereignty is expected to enhance self-determination of indigenous peoples, giving them the power to **hold countries and companies accountable** for respecting their rights.

Data sovereignty for cities and local administrations

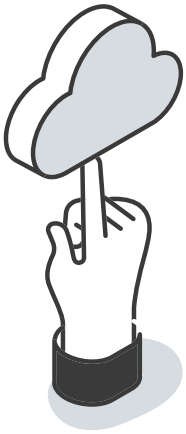
In this context, data sovereignty refers to the right and ability of a local administration to control public interest data produced in the city or locality. This includes certain data collected by private entities on various aspects of urban life, such as public transportation usage, energy consumption, waste management, public service uptake, and citizen behaviour.

The concept of data sovereignty at the local level suggests, on the one hand, that local administrations should have

the **authority** to determine how data of public interest are collected, processed, shared, and used and that, on the other hand, they also have the **autonomy** to access these data without being entirely dependent on external companies or foreign entities[1]. There is a public interest justification for cities to regain data sovereignty by accessing data from the private sector, which is linked to the public value that can be obtained as a result of sharing them with the local administration and eventually with third parties. To preserve data sovereignty, municipalities should also be able to protect citizens' privacy rights and ensure the security of such data. Although this policy brief mentions only local administrations and the city level, the same concepts and instruments could be extended and applied at the metropolitan and regional scale.

Bearing in mind that access to data alone does not guarantee impact and value, data sovereignty could **enhance how local governments use data to perform and improve/enhance their functions**, supporting the development of better public administration and services and thus improving citizens' quality of life. Wider access and ability to control data of public interest by a city could enhance local **innovation** both within and beyond the public sector, such as by fostering the development of digital tools and AI applications (e.g. third-party apps for service integration or citizen monitoring of city events), as well as of innovative solutions that draw from a wide range of data to address societal challenges more effectively.

Cities, which are playing an important role in pursuing innovative agendas in data governance [7], can foster data sovereignty implementing policies to make certain categories/types of urban data 'available by default' [8, p.1]. Through data sovereignty clauses, local governments could **use their legislative and contractual bargaining power** to require private data holders to share public interest data that they have collected so that it can be used for the benefit of city residents and society at large. Yet, this should occur in a manner such that businesses can also maintain control over their data when sharing it with government entities, so that data sovereignty of both companies (i.e., privacy, security, commercial confidentiality and intellectual property rights) and of public entities is ensured.



Data sovereignty for local governments refers to the authority and autonomy to control data of public interest produced in the city, with the goal of improving public services and spurring innovation.

1. A certain degree of dependence might still exist, especially in terms of connectivity and storage where private operators often own and manage part of the infrastructure employed by public entities.

DATA SOVEREIGNTY CLAUSES

Why are data sovereignty clauses relevant?

A large amount of urban data with a public interest dimension is collected by private companies, including ICT corporations, firms providing smart cities technologies, and businesses running public services through public-private partnerships. Local governments frequently lack access to these data, which remain controlled by the private entities, leading to significant power imbalances in data governance. Although local governments commonly contract private companies to deliver or operate public services, data generated in these settings are usually not accessible or reusable outside the narrow contractual context.

To overcome this problem, public sector bodies might establish data sovereignty clauses (DSCs) demanding that data of public interest that are collected by a service provider are available and accessible, in a privacy-compliant way, to a local authority. In this context, **data access does not necessarily imply the transfer of data**; it can also refer to other forms of information exchange, such as 'data visiting,' where data remain in their original premises. Overall, DSCs can enhance local governments' power in data governance by **empowering public bodies to set the terms** for accessing private sector data of public interest that is collected in public spaces, through public infrastructure, or during the delivery of public services.

Defining data sovereignty clauses

With data sovereignty clauses (DSCs) we refer to **mandatory data-sharing clauses** established by local governments to secure **access** to data of public interest produced within the city.

Not all kinds of data can be subjected to these clauses. In fact, such clauses are more likely to be imposed on companies that have a **contractual relationship or legal agreement with a local administration**; these may be either government-owned companies or private companies. Examples include public transport, waste management, water supply, and ride-sharing companies. These entities collect data as a by-product of running a service or business in the city.

Imposing DSCs on public interest data collected by technology companies, such as digital platforms and telecom companies, could be more challenging, although they rely on public infrastructures and might need a licence to operate in which data sharing clauses could eventually be included [5].

Under the umbrella of DSCs fall different initiatives established by local public authorities to compel companies to share public-interest data with them. According to a recent publication [10], cities can **implement DSCs using different instruments**, such as:

- clauses imposed through public procurement processes, for instance included in a **call for tenders, requiring companies to share data produced** during the implementation of their services with the local authorities;
- **clauses included in licence terms agreed** between a city and organisations that operate services or run businesses within the city;
- terms and conditions set by local governments as **requirements for obtaining public financing** or funding.

The implementation of DSCs by cities has been limited so far due to a **series of challenges**.

- A first type of challenge relates to **public sector capacity**. It derives from the lack of skills, infrastructures and human resources available within public sector organisations to establish data sharing agreements and to process and analyse the resulting data assets. Cities might not want to implement DSCs because of the additional costs and liabilities that come with being provided with massive amounts of data from private providers [7, 10].
- A second challenge originates from **companies' unwillingness to share data** due to fear of losing competitive advantage in the market by sharing strategic information, or of creating concerns among individuals about sharing their data or compromising personal data and involuntarily breaching data protection regulations. These tensions become more prominent in cases where companies dominate a particular market and create so-called 'data monopolies', such as for Uber in some American cities, or Airbnb in several European cities [11]. An additional challenge exists with companies traded on the US stock market (as is the case for several of the Big Tech players), because the U.S. Securities and Exchange Commission prevents those companies from sharing information that can influence their stock price [12].

Data sovereignty clauses are not the only instrument available to access public interest data collected by private entities. Local administrations can also adopt **complementary governance or legal instruments** to enhance their data sovereignty [12, 13, 14]. For instance, by:

- establishing voluntary (win-win) **partnerships with private sector companies** that are willing to share their data at no cost for objectives of mutual interest;
- benefiting from **corporate social responsibility initiatives**, through which businesses make data available at no cost for objectives of public interest;
- acquiring data directly through **procurement agreements** with data holders.

Another option for cities would be to leverage the **mechanism in the EU Data Act**[2] through which public sector bodies should be able to access private sector data in situations of exceptional need, for example in the case of public emergencies, and for public interest purposes (only applies to non-personal data) [12].

DSCs, however, deserve particular attention as they could offer local governments a **practical** and relatively **affordable** way to access data of public interest that is collected by businesses. DSCs could be implemented 'by default' in contracts and licensing agreements that are already in place between public and private entities. The same binding clauses can be included in each contract a city has with service providers to avoid preferential treatment, allowing the reuse of the same data sharing contract with different entities [8, 10]. Furthermore, DSCs are inexpensive as they allow access to data without additional costs, as compared to cases where data must be acquired from data holders through procurements. Finally, DSCs do not only facilitate data sharing, but they also allow local governments to keep control of the modalities through which data are shared. Differently from other mechanisms, they could offer a **systematic** 'way for city governments to get access to private sector data of public interest, both in organisational and legal terms, since the same rules apply for different contractors and across departments. [...] Local authorities [...] can specify in advance the format for exchanging information' [13].

IN PRACTICE

The implementation of DSCs by local public entities is currently limited, yet there have been a few initiatives and negotiations that can be studied. While mobility companies are a typical use case, as explained below, other relevant actors in this field are government-owned companies providing public services and digital platforms that collect information useful to monitor tourism and crowds in urban spaces (e.g., mobile phone operators and AirBnB).

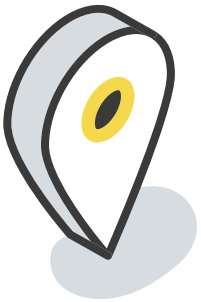
The city of **Barcelona** has been a precursor of a 'new wave of urban data politics' that promoted an alternative vision of smart cities based on data sovereignty and digital rights [15]. From 2015 with the election of the mayor Ada Colau and under the lead of Francesca Bria as CTIO, several projects were conducted concerning the way data are managed and used in and by the city. Among the various initiatives, the City Hall introduced data sovereignty clauses in all public service contracts with private sector providers. The city revised the procurement deals in public procurement contracts imposing a mandatory obligation so that any supplier to the local administration had to share data gathered while delivering their services in machine-readable format. The overall idea

2. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN

was to return to the public domain data of public interest collected by private operators, while at the same time preserving privacy and security [16]. Although most of the clauses referred to data generated by contracted public services, the city also explored widening the scope of such clauses to data of public interest collected by other private operators, such as telecom providers or shared mobility operators, with details to be established in specific contracts or as conditions for licences or concessions [15].

Following this precursor, other European cities have also been working in the direction of negotiating or implementing DSCs. For instance, **Rennes** in France, **Porto** in Portugal and **Florence** in Italy have explored the use of data sovereignty clauses to ensure systematic access to data in their urban and municipal data platforms [12].

Examples from the mobility sector



Innovative forms of mobility are increasingly appearing in cities with connected apps and platforms that allow the shared use of transport means (such as bikes, scooters and cars). In most cases, city authorities provide permission for private companies to operate in the city and use its public space to run their business; in other cases, they might issue procurement contracts to have these additional services included in their mobility offer. While the data generated by these transport vehicles (e.g., origin-destination) can be highly useful for the planning and management of transport at the city level, most of the companies retain sole control of, and access to, these data. In such cases, the use of DSCs could improve access to mobility data by local governments.

Relevant examples in this regard include the **Netherlands**-based project 'City Data Specification – Mobility (CDS-M)' in which a group of cities developed a sample contract for shared mobility operators to provide anonymised data to the local administration (**Box 1**). Another initiative has been established by the Transport authority of **London**, whereby public tender contracts for e-scooter companies include specific data sharing requirements (**Box 2**). In the Municipality of **Florence**, an exclusive licence was granted to a single smart bike provider to manage the municipal bike sharing service, with the obligation to share data collected with the municipality (**Box 3**).

Box 1. Netherlands cities: sample contract for shared mobility operators to provide anonymised data to the local administration

A group of cities in the Netherlands - including Amsterdam, Utrecht, Groningen, Eindhoven and Rotterdam - has joined forces to systematise urban data sharing in the context of the project 'City Data Specification – Mobility (CDS-M)'. The initiative proposes data sharing standards for private shared mobility operators (shared bicycles, scooters and cars), which can be adopted and applied by any local authority.

The project developed a **publicly accessible procedure** for the secure exchange of mobility data in compliance with relevant legal frameworks based on ethical principles. It produced downloadable documents and ready-made contracts including sample contract term (in Dutch) for a licence to 'include in the permit, concession, or APV what the conditions are for secure data exchange'.

The document outlines provisions for a **municipal policy rule** or regulation based on the General Administrative Law Act (APV) and establishes **obligations for providers** of shared mobility services to provide anonymised data to the local administration. The requirements stipulate that mobility providers must automatically provide **information** on the actual location of each shared vehicle offered for rent within the city at least once per hour; that the provided data should not include the ID of individual shared vehicles, and that the aggregated data on the usage of shared vehicles must be provided at least once per day.

Box 2. London: tender for shared mobility operators with requirement to share relevant data with the transport authority

The Transport for London authority (TfL) has undertaken several efforts to encourage data sharing from various mobility operators in the city such as e-scooter companies or providers of public charge points for electric vehicles. For example, TfL issued a **tender** for a trial scheme of e-scooter mobility services in 2021, **which included a requirement for operators to share data about vehicle usage and other trial data**. This was reflected in the tender specifications and formalized through data sharing agreements that were signed after the award of the contracts. Accordingly, e-scooter operators were required to share data with TfL and participating Boroughs for the purpose of operational, compliance and evaluation purposes as well as research and monitoring.

In instances mandated by TfL, operators were required **to provide data through APIs in 'near real-time'** and in accordance with appropriate standards. However, operators also had to ensure that the data shared with authorities were **anonymised in compliance with GDPR regulations, to protect the privacy of individuals**. Among the data sharing requirements, the following **information** were mandatory for the operators to share with the transport authority and Borough: routing of each trip, trip start and end data, total distance, trip time, maximum speed, location of scooters, aggregate age band and gender of users, incidents information, among others.

Box 3. Municipality of Florence: licence for smart bike operator with requirement to share data with Municipality

In 2017, the Municipality of Florence launched a free-flowing bike-sharing service using pedal-powered **'smart bikes'**. In 2021, an **exclusive licence was granted to a single provider** to manage the service, **with the obligation to share the data collected**.

The operator of the bike-sharing service **must collect data in the interests of several parties**: the **individual user**, e.g., to indicate the means of transport available in the surroundings; **other users**, e.g., to ensure that the stations are not empty, or to offer profiled tariffs in order to penalise bad behaviour (e.g. returning bicycles outside the stations), or to encourage virtuous behaviour (e.g., returning a bicycle left outside the station); and **the Municipality**. In this context, the operator collects both individual anonymised data on each bicycle and its use (such as the time and place of pick-up and drop-off, the user ID, the route taken), as well as aggregated data on the number of bicycles, users, rides.

The purpose of sharing the data is to enable the public administration to monitor the bike-sharing service, but also to develop other integrated mobility services, allowing users to consult the offer in real time, book, purchase and use a variety of means of transport. In addition, the municipality can use the data collected to develop the public transport network more efficiently and implement effective coverage throughout the territory. The data are used to improve public policies and develop new ones, following a **bottom-up** approach that values user input and cooperation with the private operator.

ENABLING SOVEREIGNTY: WAY FORWARD

According to the existing limited literature, certain steps could be taken to enhance the implementation of DSCs among local governments. For instance, the following enablers could be considered:

- **Organisational:**

  Adopt a more systematic approach to reduce the effort involved in data sharing. Implementing a use case repository, with standardised contracts and clauses, would assist cities, while also offering the flexibility to tailor solutions to their specific needs [19].

  Rely on specialised data intermediaries to make data sharing more manageable. These intermediaries can provide legal, technical, and organisational tools for data sharing, mediating between cities and private companies. [10, 12].

- **Legal:**

  Ensure transparent reporting on the use of these data for public purposes by governments.

  Explore the use and implementation of Smart Contracts that would allow companies to retain ownership and control of data, while enabling local governments to access and use data for public purposes.

- **Technological:**

  Utilise Privacy Enhancing Technologies and alternative approaches that enable the use of data directly at its source (e.g., data 'visiting'), ensuring data security and optimising resource efficiency.

  Incorporate FAIR principles & standards from the outset, including interoperability aspects in the design stage of projects to ensure seamless processing and utilisation of data across various services and providers within a city.

Future lines of research

According to the gaps we have identified in the literature, the following aspects and research questions could be addressed in future science for policy studies about DSCs and related issues:

- **How to efficiently negotiate and implement DSCs at the local level?** Which requirements should be established? When and how should they be included in procurement contracts and licences to operate? Which stakeholders should be involved in their implementation? What could be the facilitation role of data intermediaries?
- **To what extent and when are DSCs currently used by cities?** What can we learn from the state of the art? What are the enablers for adopting data sovereignty clauses at the local level?
- **What similar instruments are implemented at other levels of government** (regional, national and transnational) to access private-sector data of public interest, for instance in sectors such as health, research, or energy?
- **How can data from Big Tech platforms and telecommunication companies** be accessed through DSCs? To what extent is the bargaining power strong of cities and local authorities strong enough to contract with large tech companies? What could support their effort (e.g., alliances of cities, EU-level provisions)?
- **What is the relation of DSCs with current EU data policies and legislation?** What will be the role of the Data Act (applicable from September 2025) in enhancing data sovereignty in cities?[3] What could be the role of entities under the Data Governance Act, such as data altruism organisations and data intermediaries? What is the impact of the Interoperable Europe Act?

3. These questions will be addressed by the project Data Ally hosted at the Copernicus Institute of Sustainable Development of Utrecht University https://data-ally.sites.uu.nl/

REFERENCES

[1] Farrell, E.; Minghini, M.;Kotsev, A.; Soler-Garrido, J.; Tapsall, B.; Micheli, M.; Posada, M.; Signorelli, S.; Tartaro, A.; Bernal, J.; Vespe, M.; Di Leo, M.; Carballa-Smichowski, B.; Smith, R.; Schade, S.; Pogorzelska K.; Gabrielli, L.; De Marchi, D., *European Data Spaces: Scientific insights into data sharing and utilisation at scale*, Publications Office of the European Union, Luxembourg, 2023.

[2] European Commission. *Commission staff working document - Report on the state of the Digital Decade 2023*. 2023. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023SC0570

[3] Hummel P, Braun M, Tretter M, Dabrock P. 'Data sovereignty: A review'. *Big Data & Society*. 2021 Jan; 8(1).

[4] Von Scherenberg, Franziska, Malte Hellmeier, and Boris Otto. 'Data Sovereignty in Information Systems'. *Electronic Markets* 34, no. 1 (December 2024): 15.

[5] Bass, T., Sutherland, E. and Symons, T., Reclaiming the smart city: *Personal data, trust and the new commons*, 2018, https://media.nesta.org.uk/documents/DECODE-2018_report-smart-cities.pdf

[6] Kukutai, T., & Taylor, J. (2016). 'Data sovereignty for indigenous peoples: current practice and future needs'. *In Indigenous data sovereignty: Toward an agenda.* ANU Press.

[7] Fernandez-Monge, F., Barns, S., Kattel, R., & Bria, F. (2024). 'Reclaiming data for improved city governance: Barcelona's New Data Deal'. *Urban Studies*, 61(7), 1291-1307.

[8] von Grafenstein, M. (2023). The New Hanse: Data sharing between public and private actors in the public interest. *A first legal assessment toward a legal blueprint.* The New Institute. https://thenew.institute/en/media/data-sharing-between-public-and-private-actors-in-the-public-interest

SUGGESTED CITATION

Micheli M., Thabit S., Signorelli S., Farrell E., Kotsev A. (2024). Data sovereignty for local governments. Considerations and enablers. Science for Policy Brief. European Commission - Joint Research Centre, JRC.

ACKNOWLEDGEMENTS

The authors would like to thank Fernando Monge (Bloomberg Harvard City Leadership Initiative/ Institute of Innovation and Public Purpose at UCL), Iryna Susha (University of Utrecht) and Chiara Venturini (Eurocities) for their insightful feedback on an earlier draft of this document. Their expertise and suggestions significantly enhanced this Policy Brief. The authors are also grateful to Andrea Simoncini, Giuseppe Mobilio, Erik Longo, Matteo Giannelli (Università degli Studi di Firenze), and Ricardo Vitorino (Ubiwhere) for their availability and informative conversations that provided valuable material for the Policy Brief.

DISCLAIMER

The views expressed are purely those of the authors and may not in any circumstances be regarded as stating an official position of the European Commission.

COPYRIGHT