



## EUROCITIES principles on citizen data

### Introduction

Every day a growing number of data sets are generated in the digital public sphere. This data has an enormous intrinsic social, scientific and economic value for society as a whole. Unfortunately, current business models do not allow full access and use of this data, blocking local companies, academics, governments and citizens to participate in and benefit from socially responsible innovation.

The set of principles outlined below recognise data generated by citizens as a valuable public asset while preserving and reinforcing citizens' rights on them. The aim of these principles is to offer guidance to European local governments on how to use data generated knowledge to improve urban life and preserve European values through scientific, civic, economic and democratic progress. The principles also have the potential to shape future EU policies and legislations in this area.

The principles were initiated by the cities of Barcelona, Edinburgh, Eindhoven, Ghent and Zaragoza and developed by the EUROCITIES knowledge society forum.

### Definition

Citizen data<sup>1</sup> is personal and non-personal data, directly or indirectly generated in the digital public sphere, using digital technologies and collected through different infrastructures (IoT, telecom networks, payment systems, cameras, social networks, etc). This data is traced, collected, measured, stored, used and managed both by public and private entities (according to the General Data Protection Regulation)<sup>2</sup>.

---

<sup>1</sup> The term « citizens » here means both the origin of data, which is mostly related to citizen activities (how we communicate, move, consume, etc) but also the ultimate custodians over those data.

<sup>2</sup> Citizen data refers to a much wider sphere than open data, which mainly relates to non-personal data. Although we recognize that European local governments, as public bodies, need to pursue its path towards open data, this is not strictly the subject of these principles.

## Principles on citizen data

1. *Citizen data as a public asset*: citizen data must be recognized as a public asset, and shall be therefore solely used in the public interest;
2. *Public value*: local governments recognise, support and adhere to the principle that use of citizen data generate tangible benefits for citizens and society as a whole. There is untapped potential yet to be recognised and understood to use data-generated knowledge to improve our cities through scientific, civic, economic and institutional organizations;
3. *Citizens as data custodians*: governments have the responsibility and act to ensure citizens can have access to and manage their data, as well as influence how it is collected and used;
4. *Protection and privacy*: if citizen data contains personal data, the General Data Protection Regulation will apply. Storage, management and use of data that involve privacy or safety risks should be done in accordance with EU and national legislation;
5. *Transparency and accountability*: when generating data in public space, transparent, understandable and accountable measures on which, when, where and for what purpose data is sourced, collected and managed should be put in place; This includes both manual and automated methods, such as Artificial Intelligence and decision-making tools.
6. *Citizen Data Sharing and Governance*: anonymized data should be shared between relevant agents with the common goal of maximizing public value, subject to national and EU legislation. However, safeguards (e.g. synthetic data) must be identified and put in place to avoid, wherever possible, the risk of individuals or profiles being identified through use of new data analysis technologies (e.g. mining, use of AI, aggregation of data sets or data linking).
7. *Quality*: the quality of the data should be preserved. Those who use and share data have the responsibility to ensure the integrity, authenticity, consistency and accuracy of data;
8. *Interoperability*: the importance of data interoperability should be recognised and guaranteed through standardisation, open interfaces and protocols to facilitate data sharing and re-use;
9. *Ethical and social responsibility*: collecting and combining data may result in unforeseen insights to society or individuals. Parties collecting data in public spaces should have ongoing engagement with citizens to investigate, discuss and agree requirements for any ethical consequences of data collection and, if necessary, adjust their practices accordingly;
10. *Citizen Data Connectors*: city governments are especially suited to provide the connection between the quadruple helix innovation ecosystems and the public and private data silos. They should be given the means to means to develop and expand city data stores (or knowledge bases) to facilitate this. (to be further discussed).