EUROCITIES principles on citizen data

March 2019

Introduction

A growing number of citizen data sets are generated every day in cities. This data has significant social, scientific and economic value for society. Unfortunately, current business models do not allow full access and use of this data, preventing local companies, academics, governments and citizens from participating in and benefitting from socially responsible innovation.

The principles outlined below recognise data generated by citizens as a valuable public asset while preserving and reinforcing citizens' rights. The principles cover protection and privacy measures, transparency and accountability dimensions but also ethical and social responsibility aspects. They propose ways to better collect, manage, access and use citizens data while preventing or minimising all forms of inequalities.

The aim is to give guidance to European local governments on how to use data-generated knowledge to improve urban life and preserve European values through scientific, civic, social, economic and democratic progress. This includes putting in place mechanisms and practices to give citizens control over their data. These principles are also useful as good practice for companies and potential inspiration for future EU policies and legislation.

These principles were initiated by Barcelona, Edinburgh, Eindhoven, Ghent and Zaragoza and further developed by the EUROCITIES Knowledge Society Forum.

Definition

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

[1] The term 'citizens' in this context means both the origin of data, which is mostly related to citizen activities (how we communicate, move, consume, etc) but also the ultimate guardians of the data.

[2] 'Citizen data' is more comprehensive than open data, which mainly relates to non-personal data. Although we recognise that European local governments, as public bodies, need to continue to move towards open data, this is not the subject of these principles.

Citizen data principles

1. *Citizen data as a public asset of and for each individual:* citizen data must be recognised as a public and individual asset and shall be solely used in the public interest.

2. *Public value:* local governments recognise, support and adhere to the principle that use of citizen data generates tangible benefits for citizens and society. Using data-generated knowledge has the potential to improve our cities through scientific, civic, social, economic and democratic progress.

3. *Citizens as data guardians:* governments have the responsibility and have to ensure citizens can have access to and manage their data (e.g. MyData), as well as influence how it is collected and used.

4. *Protection and privacy:* if citizen data contain personal data, the General Data Protection Regulation (GDPR) will apply. Storage, management, processing and use of data that involves privacy or safety risks should be done in accordance with the relevant EU and national legislation.

5. *Transparency and accountability:* transparent, understandable and accountable measures on which, when, where and for what purpose data is sourced, collected and managed should be put in place when generating data in public space. This includes both manual and automated methods, such as artificial intelligence and decision-making tools.

6. *Citizen data sharing and governance:* anonymised data should be shared between relevant stakeholders with the common goal of maximising 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 artificial intelligence, 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 acknowledged and guaranteed through standardisation, open interfaces, open data models and open protocols to facilitate data sharing and re-use.

9. *Ethical and social responsibility:* collecting and combining data may result in unforeseen insights on society or individuals. Parties collecting data in public spaces should ensure they regularly engage citizens to investigate, discuss and agree requirements for any ethical consequences of data collection and adjust their practices to prevent all forms of discrimination based, for example, on gender, age, socio-economic status, ideology, race or religious beliefs.

10. *Local governments as connectors:* city governments are particularly suited to provide the connection between quadruple helix innovation ecosystems and the public and private data silos. They should be given the means to develop and expand city data stores (or knowledge bases) to facilitate this connection.