



DKSR

Data Competence
for Cities and Regions

KNOWLEDGE PRODUCT



INTRODUCTION

Data sovereignty in public contracts: Self-determined access to data

This introduction to the topic of data sovereignty in public contracts will help you in sovereignly structuring data exchange between your municipality and the private sector by setting contractual specifications.



You have questions? Feel free to reach out to us
anytime via square@dksr.city!

Data sovereignty in public contracts: Self-determined access to data

Innovative data-based approaches can be used by cities and municipalities to provide for the general welfare of people. However, in a world where the majority of data is in the hands of the private sector, how can cities gain access to datasets and ensure that they are used to advance their vision? Some examples of strategies that cities have used to gain access to third-party data include buying data, trading data, promoting voluntary data sharing, creating data partnership agreements, and including data sharing clauses in public contracts and public procurement. This guidance document will look at this latest point and provide you with key information on city contracts and how they can help your city to not only gain access, but also to sustain a long-term exchange of data with the private sector.

As third parties are often tasked to provide services for cities, data is generated in the course of these operations. Traditional supplier contracts usually do not refer to this data and leave its ownership and use rights in the hands of the third party. As result, municipalities often find themselves in the unfortunate position of having to pay twice: first for using a service and then again for purchasing the data. To avoid this, municipalities should pay close attention to the wording, standard terms and specific clauses of contracts and ensure that they include clauses on how data will be shared, accessed, protected and processed.

Ideally, the aspect of data ownership and data access should be included in the supplementary contractual conditions for the procurement of IT services, or EVB-IT. Nevertheless, since this process can be quite complex and lengthy, some cities have collaborated on the topic. This can be seen in the joint work of the cities of Bonn and Münster for developing wordings to specify the awarding of contracts and the handling of data. The result includes clauses that define data rights, copyright, and right of use. It also includes clauses to enable access to generated and processed data, as well as ensuring the technical data access via API¹. Some other examples of approaches taken by cities to ensure data access through contracts include:



Barcelona: Barcelona has developed procurement guidelines that focus on data sovereignty. All the contracts of the city administration as well as those in which the city participates (with majority-ownership) contain clauses pertaining data sovereignty². These include access to critical data, as well as its integration to the urban data platform. The city has included extensive training to project managers on how to include the clauses in tenders and contracts. An example of this approach can be seen in the contract entered between the city and the bike-sharing provider Bicing. The data that is generated through this provider's mobile application is fed into the data platform and used to improve traffic in the city.

¹ Want to get inspiration? You can see the clause concerning data access for the city of Münster here <https://github.com/od-ms/datennutzungsklauseln-muster/blob/main/MUSTERKLAUSELN.md>

² Access to the full text on data sovereignty in Barcelona can be found here <https://www.barcelona.cat/digitalstandards/en/tech-sovereignty/0.1/policy>



Guadalajara: The operator of streetlights in Guadalajara is required to provide real-time data on streetlights in the FIWARE urban data platform of the city. Based on the data from sensors placed in the street lights and defined KPIs, city managers can measure the service level of the provider and adjust payments accordingly.



Hamburg: the city introduced contracting wording to control and regulate e-trekking services. It includes data access through via a REST API and its input in the internal city data platform. Hamburg specifies the data sets to be provided and their frequency. The wording also includes privacy measures and data protection regulation clauses³. To protect privacy of users, location data and relevant information should be provided for the device (e.g. scooter, bicycle) rather than the user.

Example of a data provision clause:

All data generated during the time and for the purpose of the contract must... ..

- ...Be provided to the municipality for no additional costs or licences ...werden in voller Granularität (wenn möglich in Echtzeit) und über eine geeignete API bereitgestellt.
- ...Be interoperable and provided in a mutually agreed data format [specify] which ...corresponds to the [e.g. Berlin] data standard [add reference].
- Be provided in full granularity (real time if possible) and via a suitable API

[The city] shall be granted a non-exclusive, worldwide, royalty-free right of use to the data as to the protected and unprotected results arising from the provision of the service for the purpose of application on which the contract is based.



Do you already know which contractual clauses are necessary to regulate data access and data sovereignty for your city or municipality in agreements with service providers?

If not, it's time to address the issue! We would be happy to schedule a free consultation with you to find out how we can help. Simply contact us at square@dksr.city

³ The data access contractual specifications of the city of Hamburg can be seen here <https://www.hamburg.de/contentblob/12739712/7242056ae13651f702172cbc2adb4281/data/2019-06-20-plev-vereinbarung-hamburg-final.pdf>