

Data sources in the city



What?

This cardset will **support** you in the development and organisation of Datawalks. The cards are part of the **manual** that allows interested parties to create their own Datawalk.

Use

You can use the data source cards as **background information** when preparing your Datawalk, but also during the Datawalk itself. If a particular data source is not (visibly) present in your city or municipality, you can use the data source cards **for illustration purposes** during the walk.

Disclaimer: The information and examples given on the data source cards pertain to Belgian cases and context. They can be different in other countries.

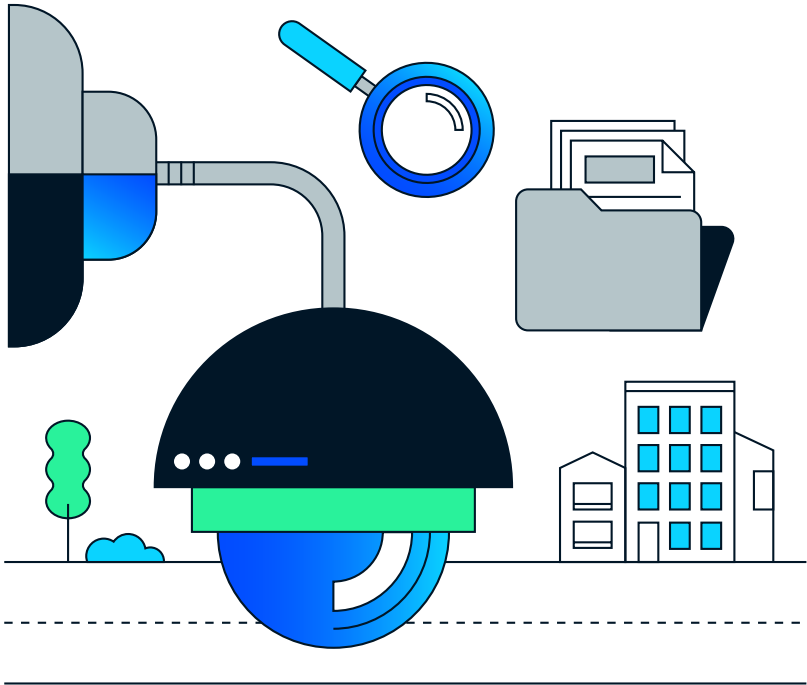
Keen to find out more?

These data source cards include a **brief description** of what each service in a smart city entails. If you are **interested in learning more and looking for references**, visit the website of the Knowledge Centre Data & Society.



data-en-maatschappij.ai/en/tools/datawalk-handleiding

DATA SOURCE



01100011

**Monitoring cameras in
public spaces
(non-ANPR)**


What?

Public cameras used by **local or federal police and city departments** to monitor public order.



Use

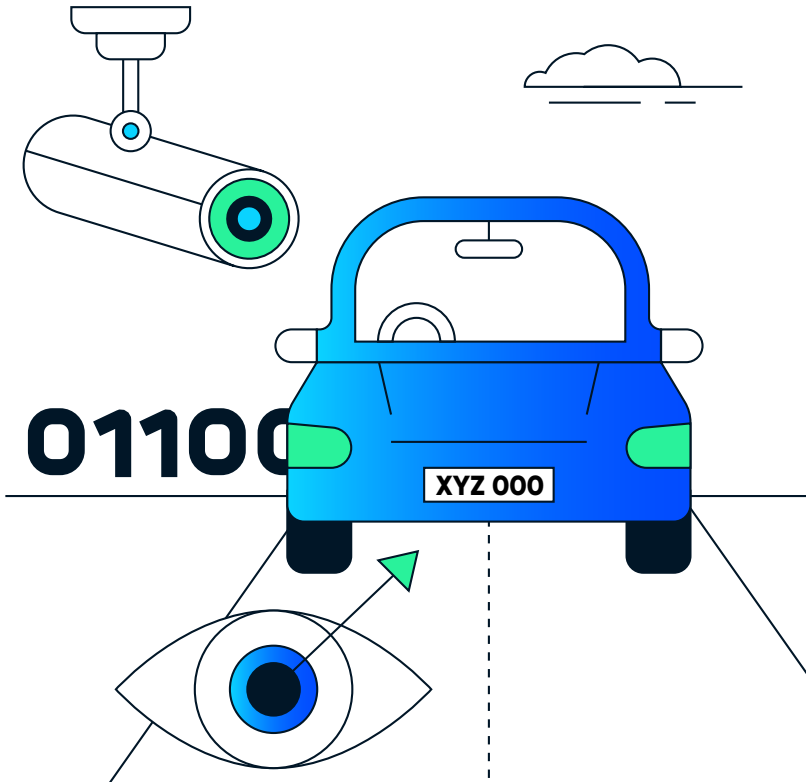
These types of cameras can **monitor** locations **live**, for example to identify suspicious behaviour or keep an eye on large crowds. They can often be controlled manually, off-site, by law enforcement authorities. These cameras can also be equipped with **object recognition** for automated monitoring (such as counting or tracking vehicles or persons, or detecting suspicious behaviour). The **regulations** on the use of cameras in public spaces in Belgium are laid down in the **Act on the Police Service** and the **Camera Act**, among others.



Data

Camera images contain **personal data**, which is processed under the legal basis 'public interest', among others. The Belgian Act on the Police Service stipulates that **citizens** should be **informed about the use of cameras** as they enter the municipality or city. The regulations also depend heavily on whether the **images are recorded and/or retained**, and whether **object recognition** is used.


DATA SOURCE



Automatic Number Plate Recognition cameras (ANPR cameras)


What?

These target-specific cameras use an **object recognition algorithm** that can recognise and 'read' **number plates**.



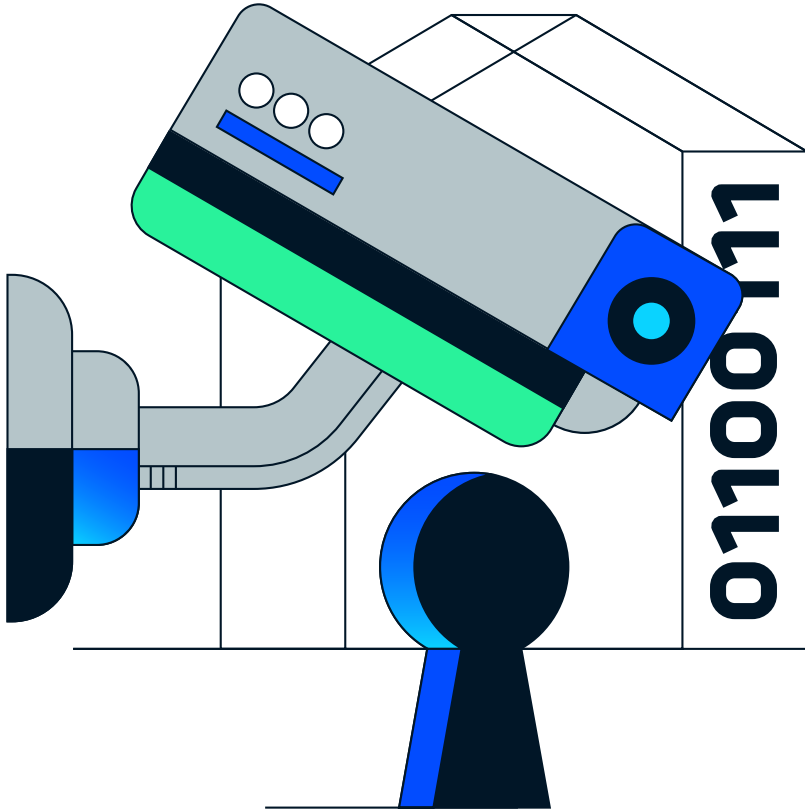
Use

These cameras are generally installed on a **fixed location**. They are used both by public bodies and private stakeholders for various **purposes**: access management (car-free zones, parking garages ...), route and speed checks, fraud checks (car insurance, car inspection ...) or to map suspicious movements (drug trafficking, ...).



Data


The cameras take **photos or video clips** of passing **vehicles**. The object recognition algorithm 'looks for' the **shape of a number plate and reads the numbers and letters**. Depending on the type and functionality of the camera, the video images are either processed **locally** (on the camera itself) **or** on a **central server**. With local processing, the read number plates are passed on to the operators in text format, rather than the full (video) images, which may feature other elements (such as persons or the brand and type of car).



**Private
security cameras**

What?


These cameras are used for surveillance in **private spaces**, including shops, restaurants, offices and private homes.



Use

These cameras are installed to prevent burglary or theft, for access control etc. They are available in a **variety of set-ups** and can be equipped with **object recognition** to automatically identify persons or behaviours. They can also be located **at the border between public and private spaces**. An example is a doorbell equipped with a camera at the front door of a home.

The regulations surrounding the use of these cameras are governed in Belgium by the **Camera Act** and are subject to the specifications included in this legislation. Among other things, the owner must 1) declare the camera, 2) keep a record of imaging activities, and 3) display a pictogram at the entrance to the monitored place.



Data

The **data collected and processed varies greatly** between cameras. Filming can be **continuous or only triggered by movement**, the recording **may or may not be saved**, ... **Object recognition** can generate additional data, anonymous or otherwise, about persons or events. From a legal perspective, this type of camera may **only record private property** and it **may not film any part of the public road, or only a limited part of it**. Since the camera is in a private space, any data processing is done on the basis of **legitimate interest**.



Telecommunication masts and telecom data


What?

A telecommunication mast is a **tall structure equipped with antennas** belonging to **telecom companies**, among others. It enables you to make calls and surf the web with your mobile phone, for example.



Use

Telecommunication masts are crucial in providing **communication services**. Telecom providers offer the resulting **telecom data** to, for example, city authorities in an **aggregated and pseudonymised format**. This may include information such as the number of unique visitors to a city, the duration of their visit, or the geographic origin of the visitors.



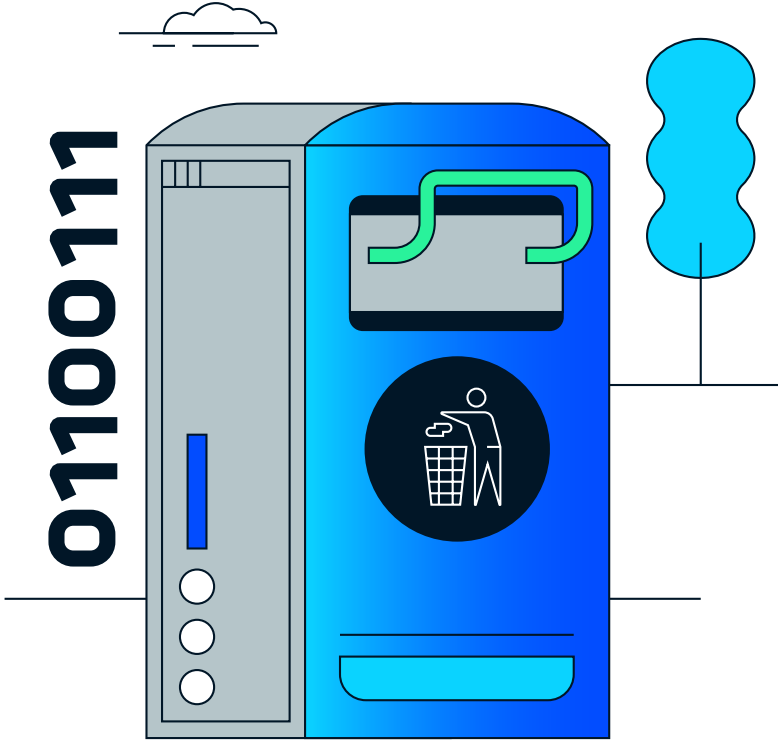
Data

Telecom data contains a lot of **sensitive information**. Since your mobile phone is equipped with a SIM card and you use telecom services, the provider can find out **where you are, who you are in contact with**, etc. at any time. However, they do not have access to the **content of the communication**. There are currently discussions in Belgium on how long telecom operators should and may keep this data (data retention law).

To comply with privacy regulations, only pseudonymised, aggregated data are included in the reports. This network data is based on the **logging of mobile phone signals** and generalisation via **extrapolation** based on the market share held by the different telecom providers.

To safeguard **privacy**, the reports can only contain data on **groups of at least 30 people**. The data on groups of fewer than 30 people are combined into a single category. Re-identification of individuals based on the reports is not easy and not allowed.


DATA SOURCE



Smart bin


What?

This waste bin is equipped with **sensors** that can **measure how full it is** in order to compress the waste locally and optimise waste collection through efficient grouping of collection rounds in specific areas.



Use

A waste bin with sensors measures the contents of the bin and provides **useful information to organise waste collection more efficiently**. Bins for household waste allow residents to deposit their waste whenever they want. They are charged based on the amount of waste they have produced. This service is usually available in highly urbanised areas, and often also in locations where waste collection is complicated for various reasons (for example due to narrow streets).

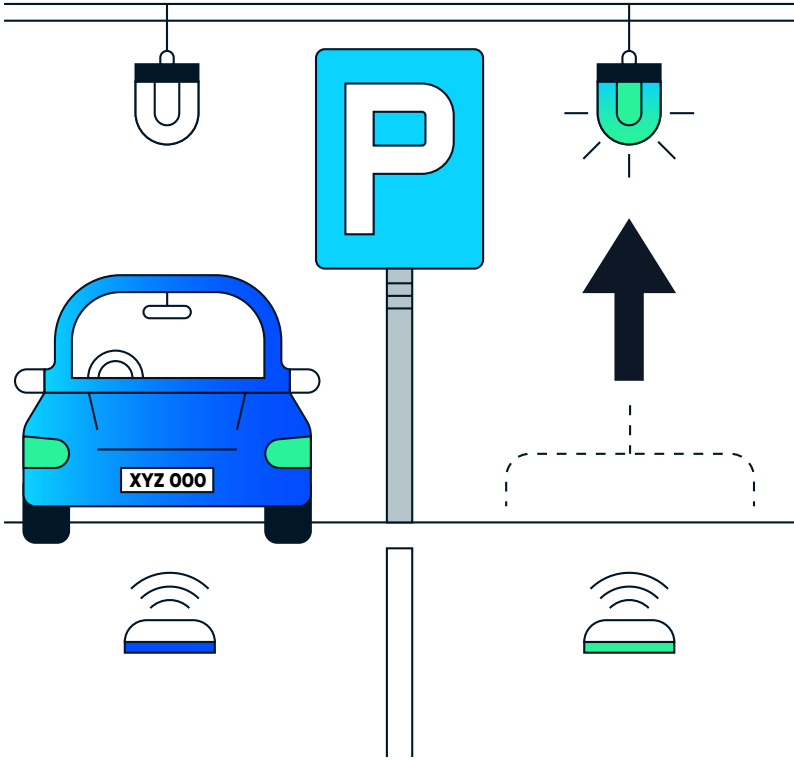


Data

Data insights gathered from smart waste bins can **support urban policies on (household) waste in several ways**. The data collected can be used to map out **more efficient and environmentally-friendly routes and collection times**.

As for household waste bins, sometimes **personal data** are linked to the waste the individual leaves in the bin so as to calculate the charges due based on their waste production. This data may include the nature of the waste, the quantity and the time of its disposal.


DATA SOURCE



Parking space sensors

What?


These **sensors** record whether a parking space is occupied and if so, how long the vehicle has been there. Vehicle registration can be done using **different types of sensor techniques** such as magnets, lasers or cameras. Often the sensors are embedded in the road surface or attached near the parking spot.



Use

Parking facilities use these sensors in different ways. They can **track which parking spaces are occupied**, as well as the frequency of occupancy, the **time** someone occupies a particular space, etc.

A specific example is the use of these sensors to organise **free short-term parking** in highly urbanised areas. When a vehicle exceeds the permitted parking time, a parking attendant is notified to determine the violation.



Data

These sensors collect **a limited amount of non-personal data**. The sensor only registers whether or not the parking space is occupied and logs any changes, possibly with a timestamp.


DATA SOURCE



Parking meters


What?

Parking meters allow you to **pay** for the use of a **parking space**.



Use

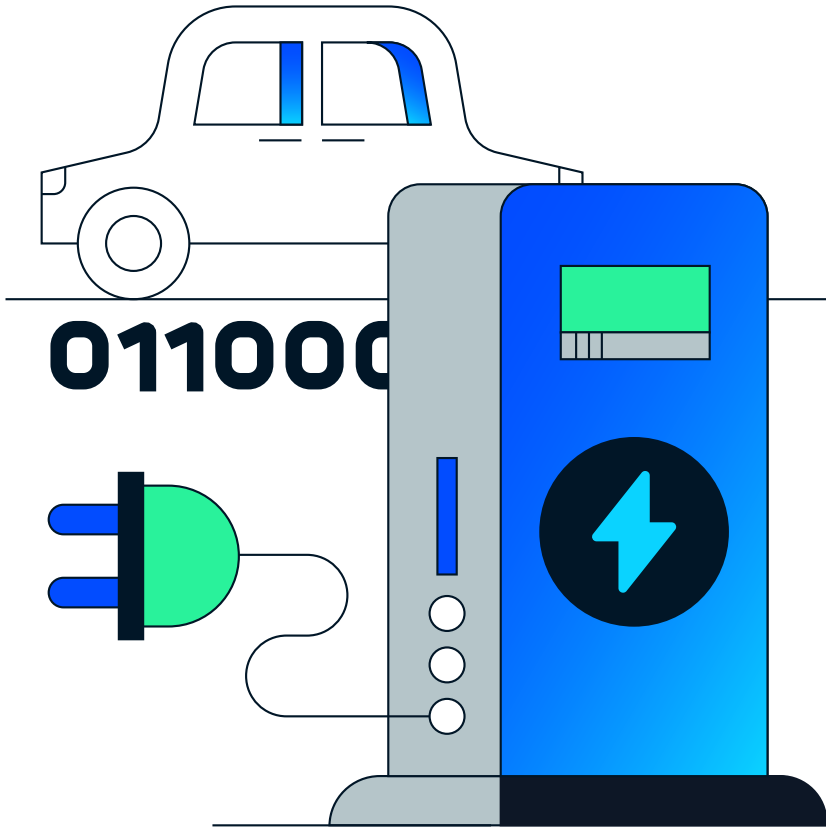
When it comes to parking meters, **printed tickets** (which you place behind the windscreen of your vehicle) are increasingly being replaced by **paperless alternatives**. These payment terminals work with **different forms of registration**. You can make use of a mobile app, send your number plate via SMS, or enter it at a parking meter.



Data

These data sources record the **time of arrival and departure**. This data can be linked to your **number plate or the data you shared when creating an account** in an app, such as the brand and model of your vehicle, your place of residence, etc.

DATA SOURCE



Charging stations for electric vehicles


What?

These are **charging stations for electric vehicles** such as cars and bicycles.



Use

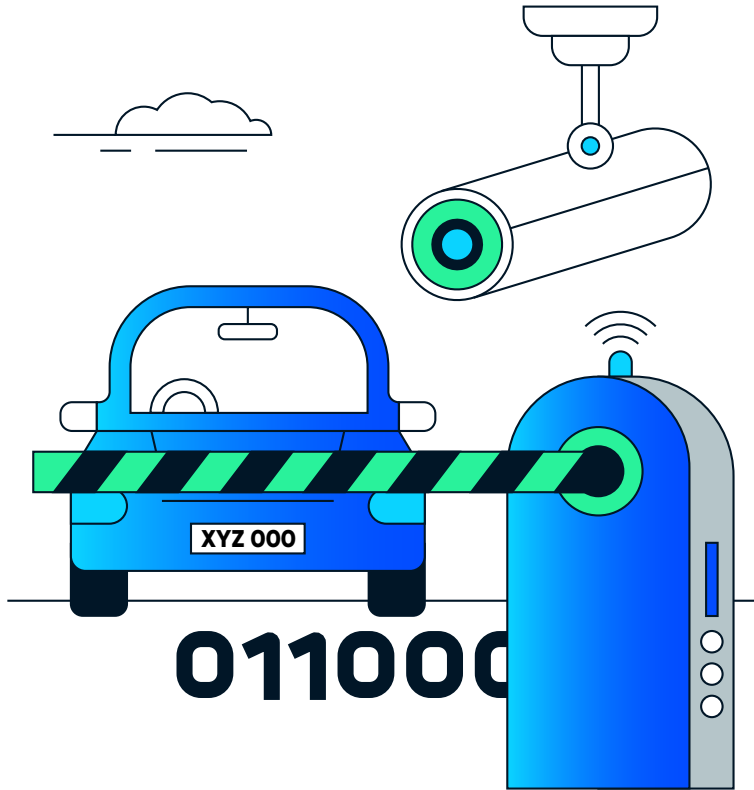
You can charge your vehicle at a public charging station by plugging it in and paying with a bank card. Charging station providers sometimes work with a **membership**, allowing you to buy a certain amount of electricity for a fixed fee or issuing invoices at set times. Usually these charging stations are **managed by private providers**.



Data

The **cost** is calculated based on the **start and end time** of the charging and **the amount of electricity you have been supplied with**. The charging cable also establishes a **data connection between the vehicle and the charging station**. In this way, the vehicle can communicate how many kilowatts the charging station should supply. In the process, information on the brand and model of the vehicle, for example, can also be exchanged.


DATA SOURCE



Access control


What?

Locations with **restricted access** may be closed off by means of retractable bollards or barriers, among others. These can only be opened with the correct **verification data**.



Use

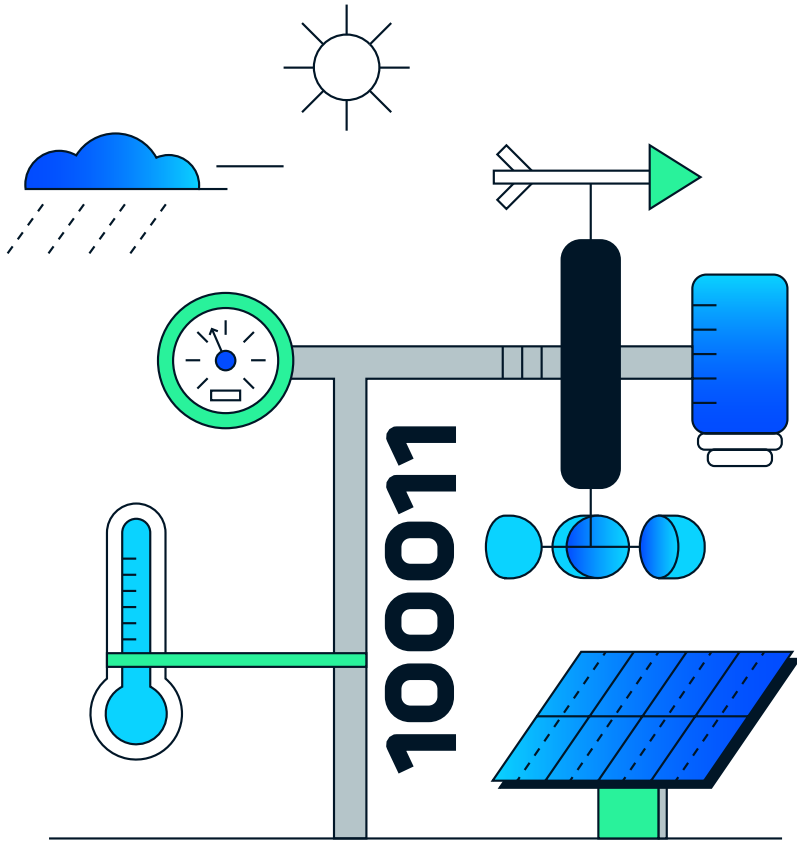
Access authorisation can be granted **in different ways**: with an ANPR camera for number plate verification, by scanning a badge or access card, with a code entered via a keypad, ...



Data

The **data collected varies depending on the verification method**. Verification via ANPR may involve recording the time and location of the access request, as well as registering the vehicle. This registration is also possible using an access code or badge, which can only be traced back to a specific person if the code or badge is personalised and therefore different for each user.


DATA SOURCE



Weather stations


What?

In addition to the official weather stations of meteorological institutes, some cities also have **smaller weather stations**. These make **less precise measurements** but map the weather **in more (localised) detail**.



Use

These weather stations are used to monitor **differences in weather in different parts of the city**, which helps **respond more precisely to the effects of the weather**. By placing these stations at different locations across the city, one can investigate in detail which areas have the highest heat concentration, for example. These weather stations may be located on public property, but private organisations or individuals may also be involved as part of **citizen science initiatives**.



Data

The weather stations collect **various weather-related data points** such as temperature, relative humidity, wind and precipitation. This **does not involve any personal data**.


DATA SOURCE



Shared mobility


What?

Shared mobility refers to vehicles that you can use for a **defined period of time** for **personal travel**, without owning the vehicle. It usually refers to electric scooters, bicycles and cars.



Use

Shared mobility solutions are often very prominently offered in cities to diversify the **mobility mix**. They increase the mobility of residents or visitors without the need for them to own their own vehicle. There are often **several providers** of the same type of shared vehicle within a city.



Data

The platform of shared mobility providers collects information such as the users' **personal data**, the **routes travelled** and the **speed driven**. The **business model** of shared mobility providers is based on the payment of usage fees but also on users' data. This combined data can be valuable to gain more **insights** into **mobility trends** within a city. Providers therefore often market the insights they can extract from this data, for example through the analysis of **popular routes and locations**.


DATA SOURCE



Public Wi-Fi


What?

This refers to **Wi-Fi** that citizens can use freely and **free of charge**. It is often offered in crowded public spaces or in libraries and museums.



Use

Cities offer public Wi-Fi to **make the digital world more accessible**, for example to provide access to **certain online (city) services**. Depending on the provider, this public Wi-Fi can be accessed freely (without the use of an account or password) or after registering or creating an account.



Data


The **internet traffic** over a (public) Wi-Fi network can be analysed. The content of messages is not monitored. However, information can be gathered about the apps used to connect to the internet, and the websites that have been visited.



Beacons and sniffers

What?


These are sensors that can be installed in **both public and private spaces** and (attempt to) connect to mobile devices. These sensors use **various technologies, such as Bluetooth or Wi-Fi**.



Use

Beacons and sniffers continuously send out **connection requests** to look for nearby devices. Depending on the settings, a smartphone will respond to these requests with a **personal identification** linked to the device. Using these beacons and sniffers, **locations and routes** of individuals can be mapped.

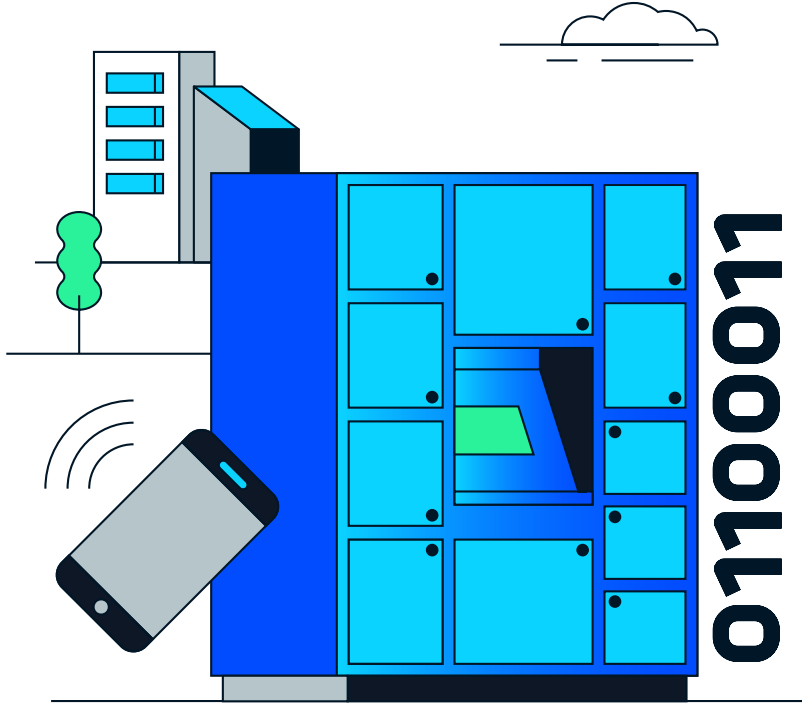
It is also possible to analyse how long a particular device remained near a particular location. **When installed in a shopping centre**, for example, they can analyse which shops get the highest footfall or which products the visitors linger at the longest.



Data

Each individual beacon or sniffer creates an inventory of **all the devices** it has connected to. While the identification codes exchanged do not contain any personal data, such as your name, it is **possible** to use other techniques to find out the **identity of the user**.


DATA SOURCE



Parcel machine

What?

Parcels are stored in these machines and the recipient can **unlock** them **with a (QR) code, for example**. There is often a network of parcel machines, which are distributed across strategic locations in the city.



Use

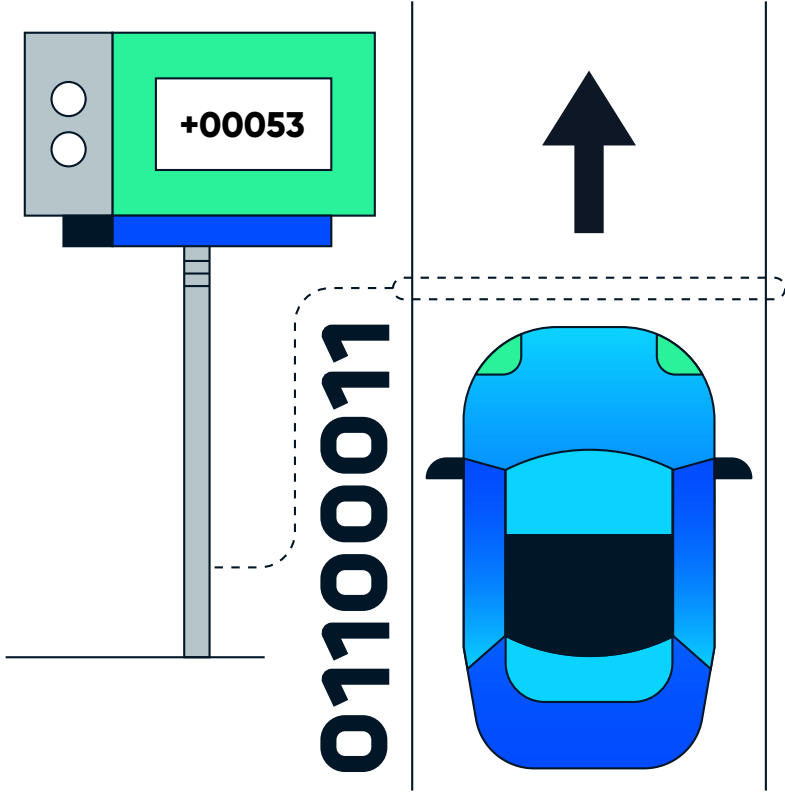
The delivery of parcels in centralised parcel machines **reduces the traffic** and **pollution** associated with deliveries.



Data

When you collect your order, the parcel machine can **record the collection time**. This data can be used to **refill the machine more efficiently**.


DATA SOURCE



Traffic counters

What?


Traffic counters **monitor traffic at a particular location**: which vehicles and how many of them pass along this street? There are **different systems** to record traffic flows. A counting loop is a cable or laser that spans the width of the road surface and can register what kind of vehicle passes by monitoring interruptions. Cameras with object recognition are also used for this purpose.



Use

Traffic counters serve to **support mobility policies**. Therefore, they are **usually installed by (local) governments**.

Citizen science initiatives such as **'Telraam' in Belgium** also engage citizens to get a more detailed picture of traffic flows. As part of this initiative, citizens place a small device behind their window, aimed at passing traffic. The 'Telraam' algorithms can recognise and classify vehicles in the video stream, analysing every vehicle that passes by. Since these **algorithms work locally on the device itself**, only the **numbers** of the vehicle count are **collected** on the 'Telraam' platform.



Data

Traffic counters generally **do not collect personal data**. Even with camera solutions, image analysis is often done on the device itself. Only **the data on the vehicle counts** is transmitted, not the camera images. Traffic counts by means of ANPR cameras are not included in this category (see the data source-card on ANPR cameras for more info).

DATA SOURCE



Acoustic sensors

What?


Acoustic sensors are **microphones** that measure the **sound levels** in crowded places or can use **algorithms** to detect **events** in the sound stream.



Use

Acoustic sensors are used in entertainment areas to detect **noise pollution or specific incidents** (such as brawls).

Their use depends partly on the functionality of the sensor. Simple applications record only when a certain decibel limit is exceeded. More complex applications can use AI to recognise different types of sounds, such as breaking glass, shouting, sirens, gunshots, etc.



Data

Data flows differ greatly according to the **way in which sound data is analysed and potentially categorised**. The analysis of the captured sounds can be done **on the device itself** or **sent over the internet** to a **central server** that analyses the sound clip. In the first case, only the labelled sound data (sound level, event, etc.) is transmitted, which can be organised in a relatively privacy-friendly way. In the second case, every captured sound is transmitted, which is more risky in terms of privacy.