Digital security for transport users

Mariska's customer journey in 2023

Travel planner

- Mariska registers on the app and plans a trip to visit her mother
- She enters her personal data, personal preferences and payment details

Shared taxi

- Mariska books the journey and receives a confirmation from the shared taxi in her app
- She gets in the taxi and travels to Amsterdam Central Station
- Her journey can be followed in real time on the app
- The payment for the journey is processed

Public Transport

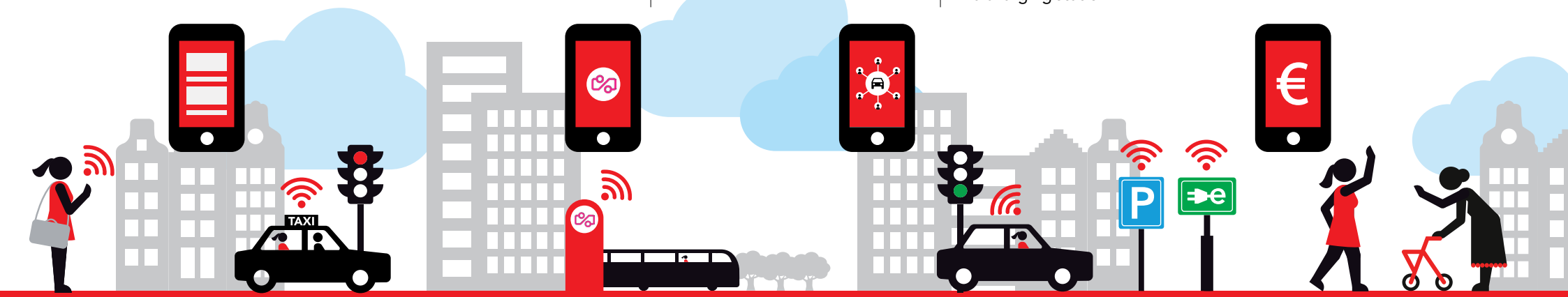
- Mariska takes the train
- An app indicates which train she should take, from which platform it departs, and how long it will take to walk there
- She walks to the station and checks in at the gate
- She travels using public transport and checks out on arrival
- The payment is deducted

Shared car

- In her app Mariska sees where her private shared car is parked
- The car owner accepts the rental
- She opens the car with her phone
- The speed is adjusted to the traffic light timing
- She parks in the car park
- Mariska charges the car at a charging station

Payment

- Mariska has completed the journey and receives a notification
- The payment is deducted in the app
- The platform specifies the cost per modality
- She receives a notification of the cost and her balance



Mariska

It's 2023. Mariska is 45 years old, has two children and lives in Amsterdam.
She works in healthcare and needs to take her children to school.
She also visits her mother in Schiedam, who suffers from health problems.
Mariska books the journey to Schiedam via a MaaS provider.

Digital security for transport users

Privacy & cyber security risks

Travel planner

Algorithm

- → Concentration of supply due to algorithm
- → Prediction of behaviour of transport user using collected data
- → Creation of personas based on transport user data

Shared taxi

- → Quality and reliability of data supplied by providers is inadequate
- → Transport user's anonymity is not guaranteed
- → Use of Bluetooth (contravenes GDPR)
- → Sensitivity of data communication from apps to vehicle and cloud

Public transport

- → Weaknesses in use of passwords for traffic light control from traffic control centres
- → Inadequate protocols and processes for data and user protection in internal organisation
- → Public transport shares virtually no data
- → Mariska's travel preferences are sold to third parties

Shared car

Hacking of vehicle

- → Car theft
- → Control of vehicle by taking over control system (route/braking/speed)
- → Use of data

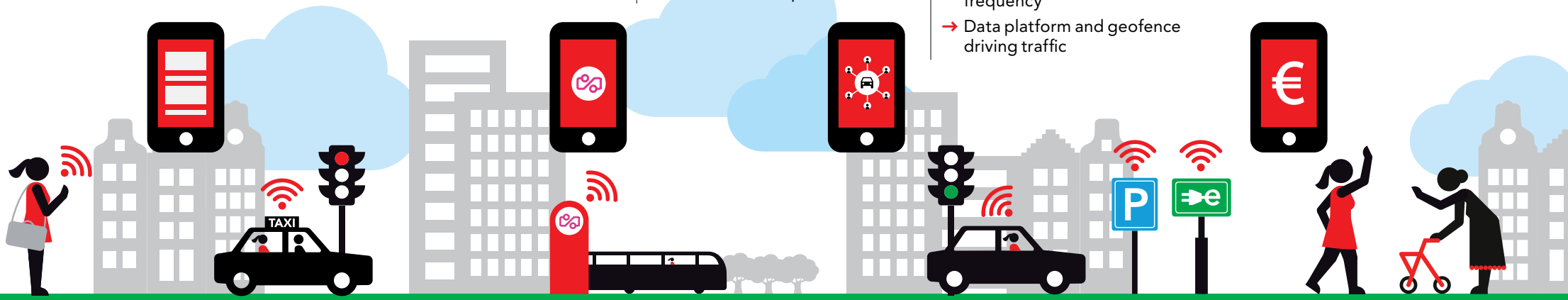
Hacking of infrastructure

- → Taking control of traffic lights resulting in dangerous situations
- → Manipulation of traffic signal frequency
- → Data platform and geofence driving traffic

Payment

Abuse of PDS2 (new financial law)

- → Companies obtain financial data of customers
- → Financial operators in position of power
- → Sensitive to phishing



Risk management

Algorithm determines behaviour

- → Audit of algorithm and IT
- → Set requirements for algorithm
- → Make codes open source
- → Implement and enforce GDPR and Government Baseline Information Security (BIO)
- → Update reference architecture (GDPR)

Data misuse

- → Prevent misuse by establishing rules for data use
- → (Digitally) enforce rules and make audits

Hacking of systems

- → Set up reporting hotline for data abuse
- → Establish incident procedure
- → Transparency regarding hacking for chain partners

Geofencing

- → Distribute traffic based on:
  - Air quality
  - Congestion and crowding
  - Accessibility
  - Physical and digital security of vehicles
  - Braking distance
  - Speed
  - Log times

Exclusion of market mechanism

- → Information on implications of Payment Service Directive 2 (PDS2)
- → Design of standards for data sharing
- → Transparency for users

Examples

Chicago Car2Go app hacked
→ 100 cars missing

Car2Go is a car-sharing app from Chicago. After a hack around 100 cars were stolen. The cars could be opened using the hacked app.

Lime scooters hacked
→ Sexually suggestive messages sent to users

In Australia, electric kick scooters were hacked and sexual remarks sent to users via the speech software.

Hacker remotely kills car engines → GSP tracking app hacked

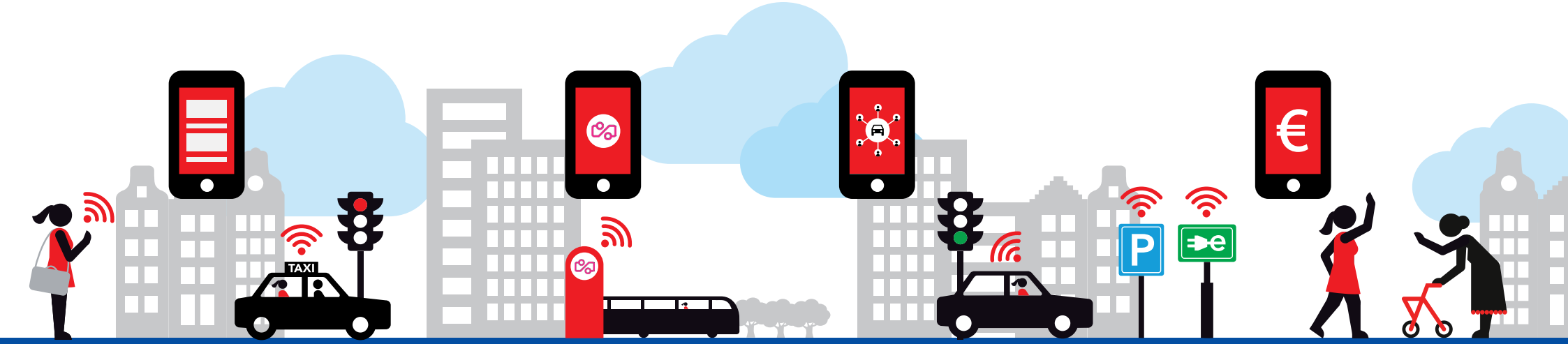
Thousands of user accounts for a GPS tracking app were hacked. The hacker could see the location of the vehicle and control it by turning the engine on and off.

Data from crashed Tesla not wiped → Personal data made public

When crashed Teslas end up on the scrapheap, their data isn't wiped. The data is not encrypted and contains details of the owner, mobile devices and videos of the crash.

Traffic lights and cameras hacked
→ Traffic manipulated

Inspired by the movies *Die Hard* and *Oceans 11*, hackers succeeded in manipulating traffic lights and cameras. They accessed the lights and cameras using drones and via an ethernet connection.



Rapid growth in cyberattacks on smart mobility 2010-2018

Privacy and cybersecurity affect the entire mobility chain due to increasing digitisation.
Nationally there is little knowledge and capacity to guarantee effective digital security.