

Wir wissen, wo dein Auto steht

Volksdaten von Volkswagen

**Flüpke
Michael Kreil**

Wo parken Autos?

Na auf Parkplätzen!



»Ich bin der
Anzeigenhauptmeister«

SPIEGEL TV

<https://www.youtube.com/watch?v=bcqbVmC9M5g>

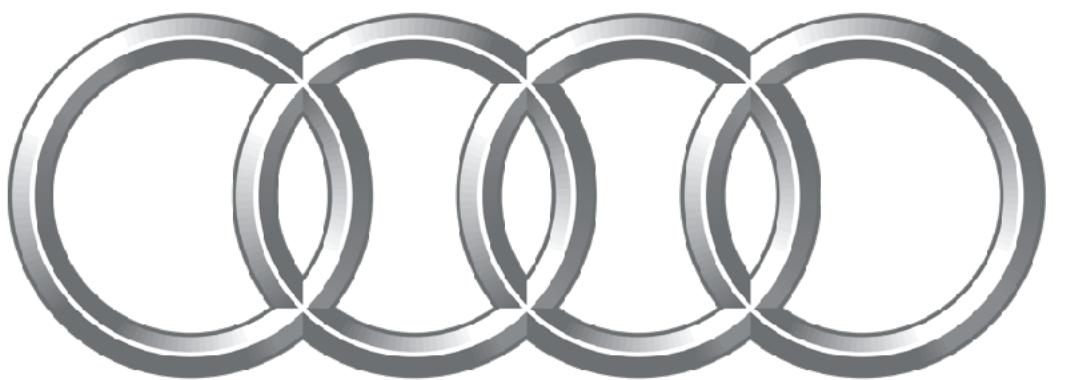
Volkswagen: Datenleck bei
wv - Millionen
Fahrzeugdaten ungeschützt



t. T-Online | 11 minutes ago

Volkswagen AG

Wer ist das?



Audi



ŠKODA



SEAT

Fahrzeugplattformen



<http://bilder.buecher.de/produkte/36/36962/36962902z.jpg>

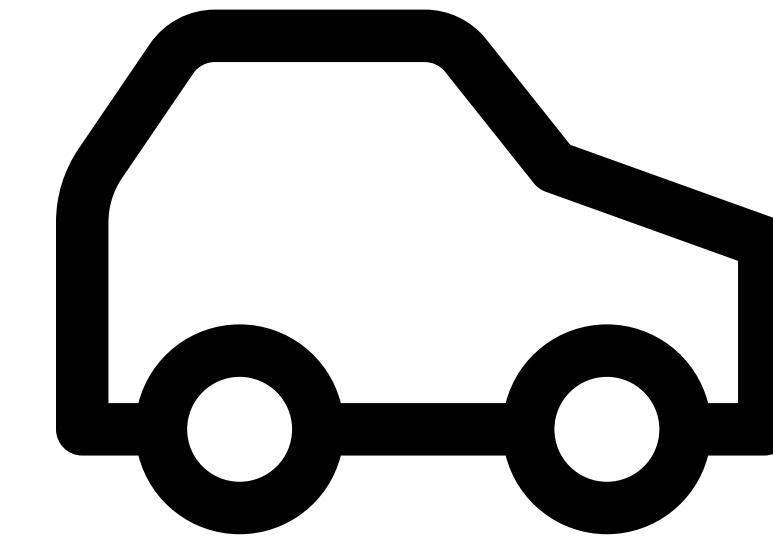
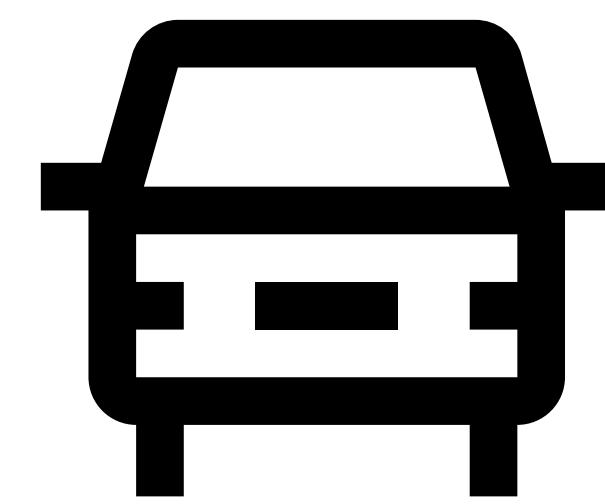
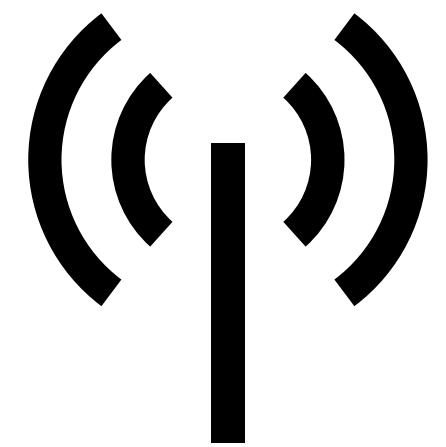
Software

Was kann da schon schief gehen?



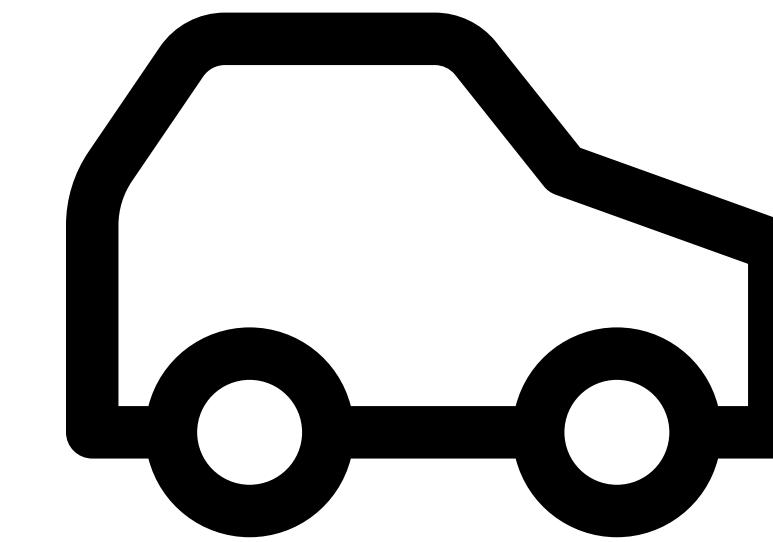
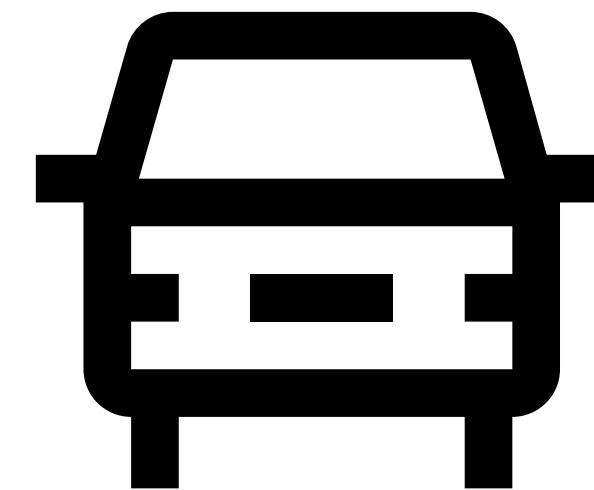
Wer hat uns verraten?

Telemetriedaten!



Wer hat uns verraten?

Telemetriedaten!



Wie hat sich das zugetragen?

Zeit für eine Datenreise



https://commons.wikimedia.org/wiki/File:Travel_agency,_The_Village,_Formby_-_geograph.org.uk_-_1133475.jpg

Navigation subfinder

```
[\$ subfinder -d ccc.de

  _/ \_ / \_ / \_ / \_ / \_ / \_ / \_ / \_
  ( ) / \_ / \_ / \_ / \_ / \_ / \_ / \_ / \_
/_ / \_,/_ . / \_ / \_ / \_ / \_ / \_ / \_ / \_

      projectdiscovery.io

[INF] Current subfinder version v2.6.7 (latest)
[INF] Enumerating subdomains for ccc.de
infra-01.cert.ccc.de
c3a0ac7d.ip.berlin.ccc.de
c3a0ace8.ip.berlin.ccc.de
c3a0adb3.ip.berlin.ccc.de
icon.adventure.koeln.ccc.de
gitlab.hamburg.ccc.de
c3a0ac68.ip.berlin.ccc.de
c3a0ad72.ip.berlin.ccc.de
inv.aachen.ccc.de
build2.darmstadt.ccc.de
www.eh09.hamburg.ccc.de
c3a0acdb.ip.berlin.ccc.de
ns.west.berlin.ccc.de
westkreuz.berlin.ccc.de
jitsi.matrix.aachen.ccc.de
c3a0adc7.ip.berlin.ccc.de
c3a0adec.ip.berlin.ccc.de
tickets.muc.ccc.de
c3a0ad6d.ip.berlin.ccc.de
c3a0adf9.ip.berlin.ccc.de
```

Ortskontrollfahrt

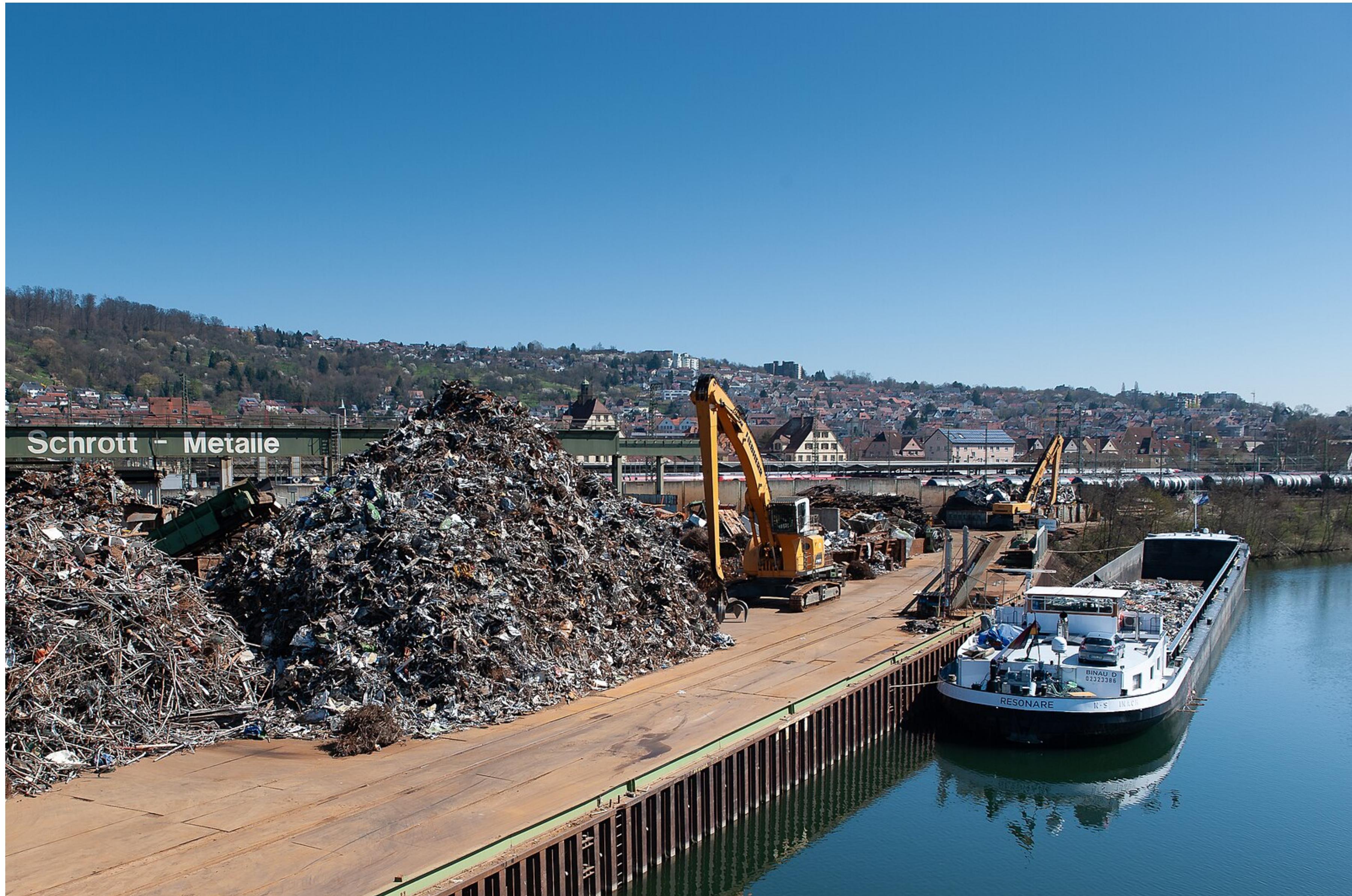
Directory Enumeration

```
$ gobuster dir --url "https://www.ccc.de" --wordlist wordlist.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          https://www.ccc.de
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     wordlist.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/JS/                  (Status: 200) [Size: 10227]
/Js/                  (Status: 200) [Size: 10227]
/js/                  (Status: 200) [Size: 10227]
/admin                (Status: 302) [Size: 99] [--> https://www.ccc.de/de/session/new]
/Admin                (Status: 302) [Size: 99] [--> https://www.ccc.de/de/session/new]
/admin/               (Status: 302) [Size: 99] [--> https://www.ccc.de/de/session/new]
/admin/access_log    (Status: 302) [Size: 99] [--> https://www.ccc.de/en/session/new]
/admin/backups/      (Status: 302) [Size: 99] [--> https://www.ccc.de/de/session/new]
/admin/backup/        (Status: 302) [Size: 99] [--> https://www.ccc.de/de/session/new]
/admin/_dump/         (Status: 302) [Size: 99] [--> https://www.ccc.de/de/session/new]
```

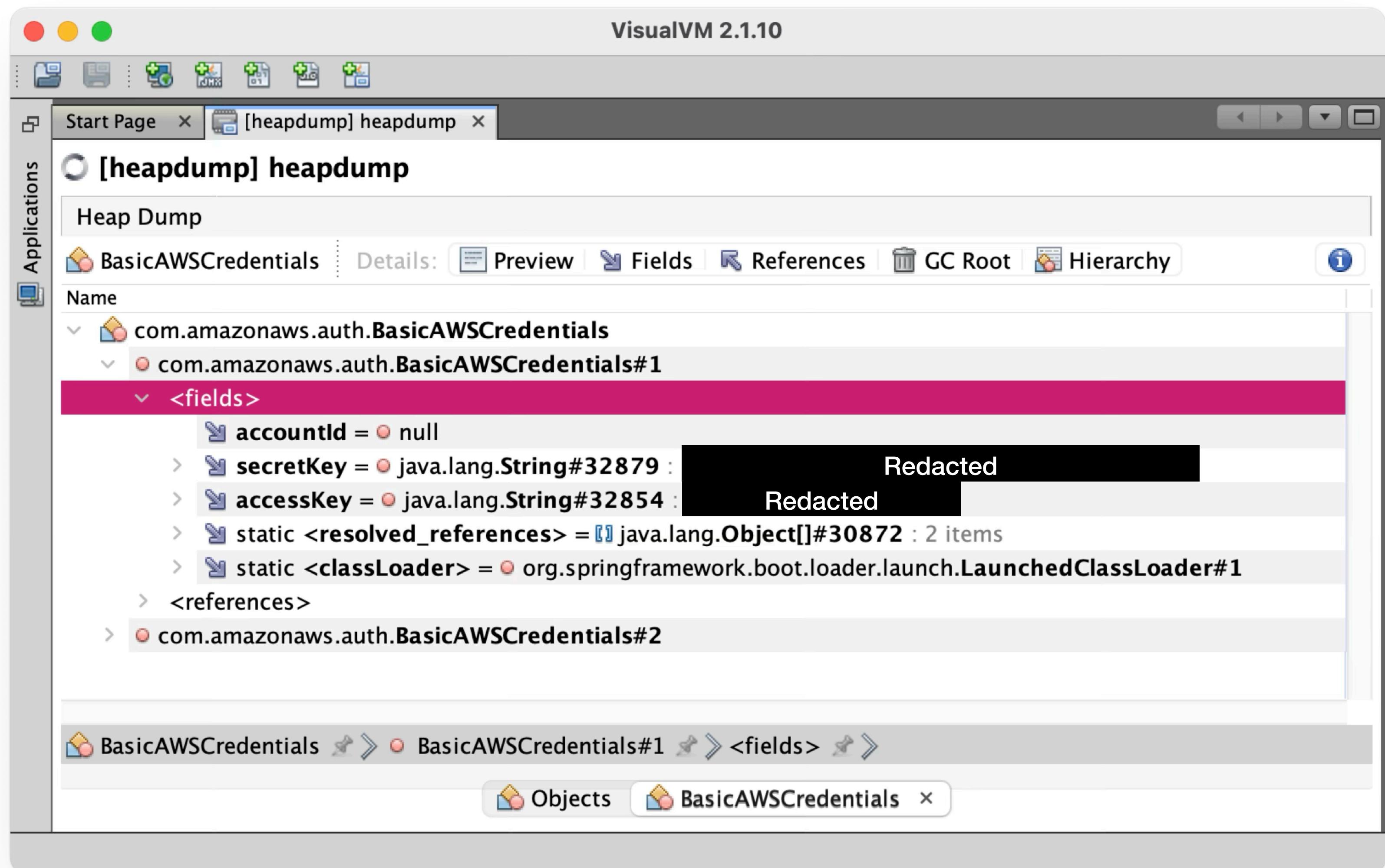


spring[®]

GET /actuator/heapdump



<https://de.wikipedia.org/wiki/Datei:HafenPlochingen-pjt1.jpg>





Angekommen



»Der Zugriff auf die Daten erfolgte in einem sehr komplexen, mehrstufigen Verfahren.«

Volkswagen, gegenüber SPIEGEL

strings

Binäranalysewerkzeug

**CLIENT_ID
CLIENT_SECRET**

Token Exchange

komplexes, mehrstufiges Verfahren?

**»Wir wissen dann alles über das Auto und
Einiges über die Kunden.«**

CEO Volkswagen Financial Services

Schauen wir uns die Daten mal an 

Automobile Vorratsdatenspeicherung

1. User Data

Name

Email

Telefon (teilweise)

2. Enrollment Data

VIN

Model

Year

User ID

3. EV Data

Odometer

Battery Temperature

Battery Status

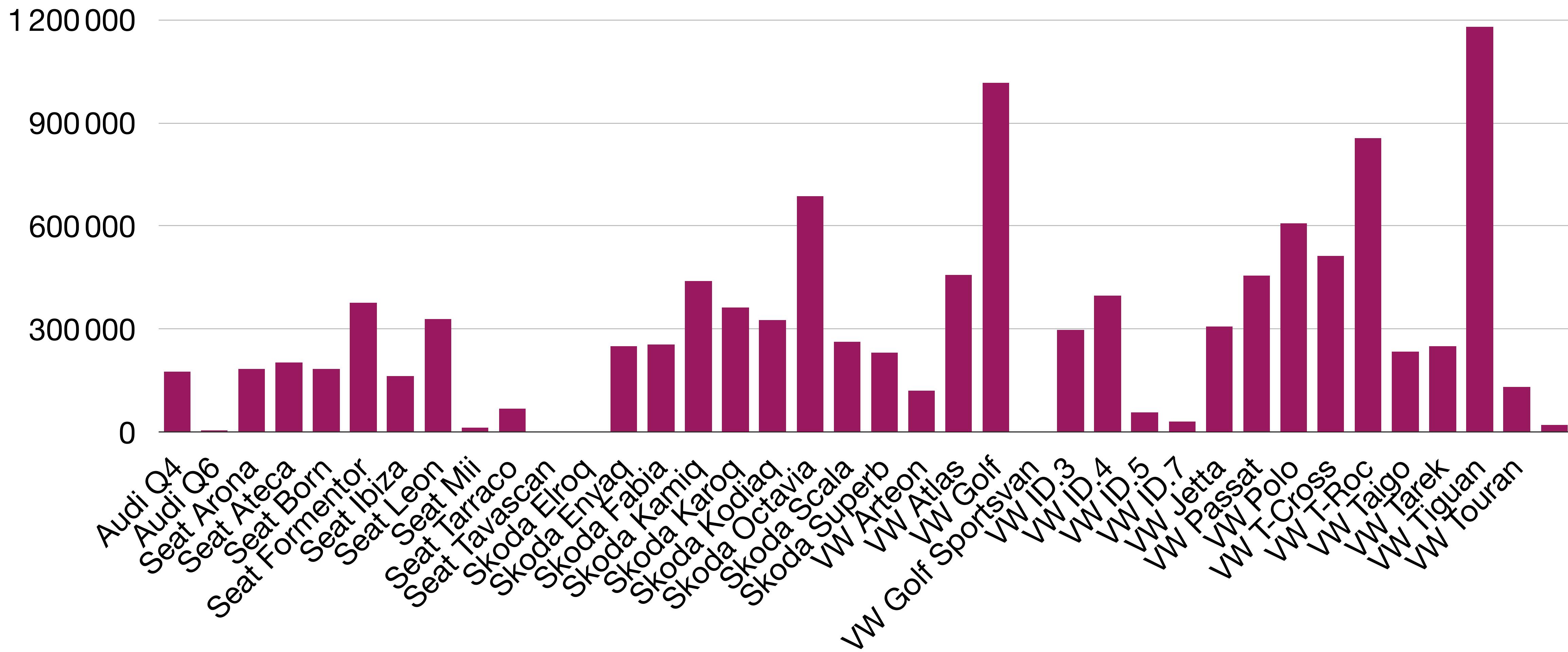
Charging Status

Warning Light Data

1. Enrollment Data

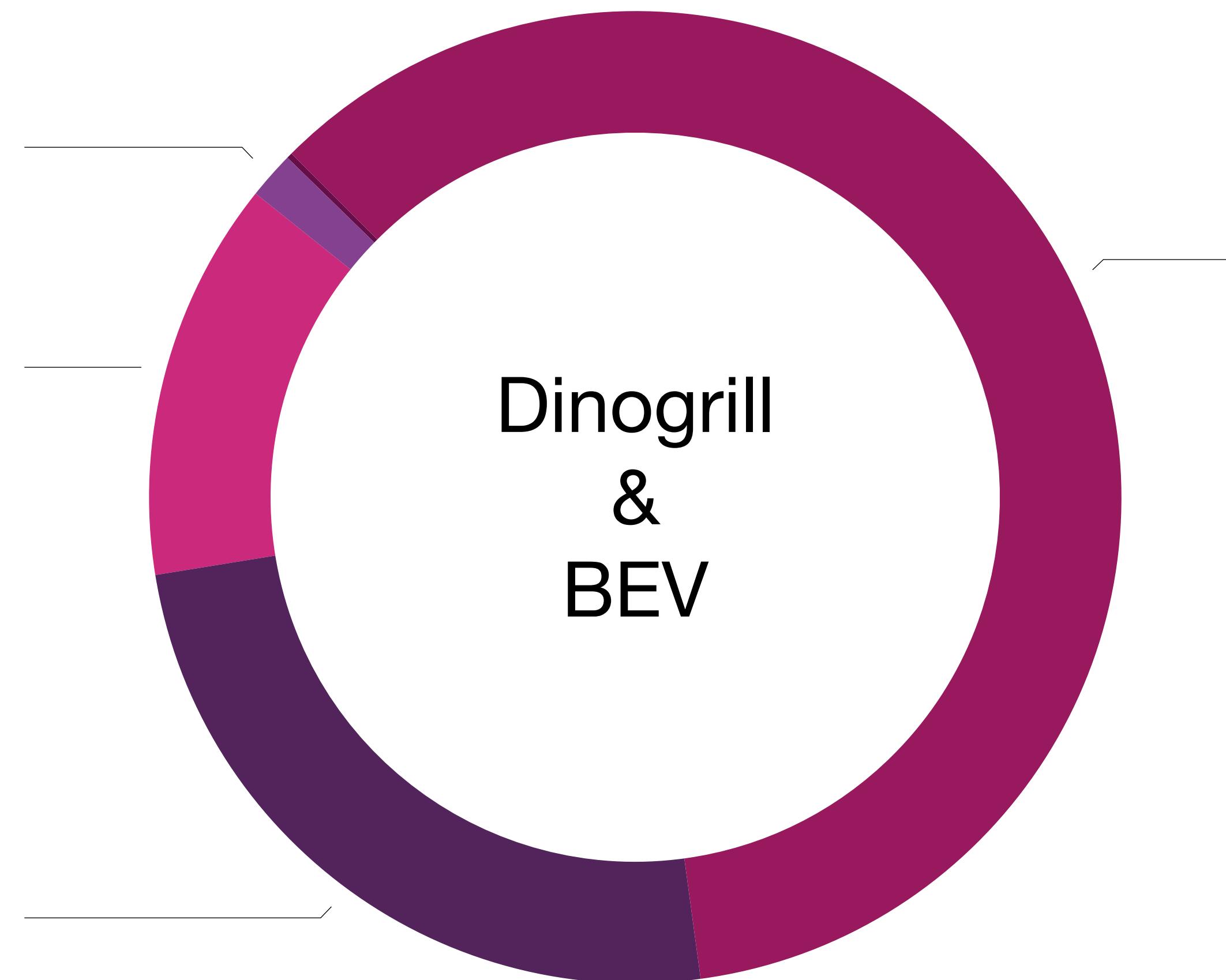
Enrollment Data

Fahrzeugmodelle



Enrollment Data

Fahrzeugmarken



Enrollment Data

Digitalisierungsquote



2. EV Data

"Nur" EV Data?

{audi|skoda|seat|vw}cmp-dataloader-service

- Vermutung: Backups aus größerem Datenpool
- Heapdump und API Endpoints
- VW: "Ladeverhalten und Ladegewohnheiten von Kunden werden genutzt, um Batterien und die dazugehörige Software zu verbessern"

Fleet Interface

der Volkswagen Group, bereitgestellt von der Volkswagen Group Info Services AG

Dateneinblicke, angepasst an Ihre Bedürfnisse.

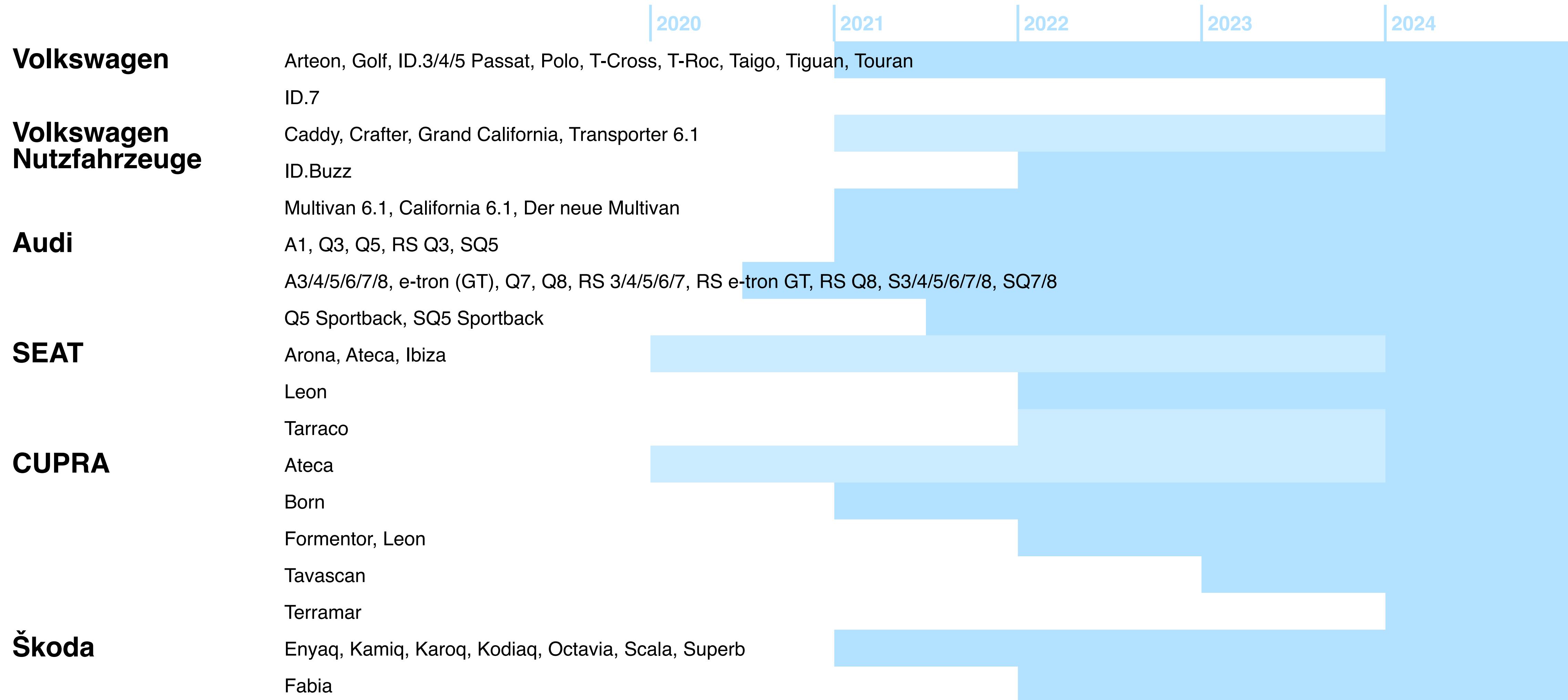
Fleet Interface ermöglicht Ihnen den **Zugriff auf Ihre Fahrzeugdaten** direkt aus dem Flottenmanagementsystem Ihrer Wahl. Sie müssen **keine Telematiklösung nachrüsten.**

Es ist einfach, zugänglich und **angepasst an Ihre Bedürfnisse.**

KONTAKT AUFNEHMEN

LOGIN

Unterstütze Marken und Modelle



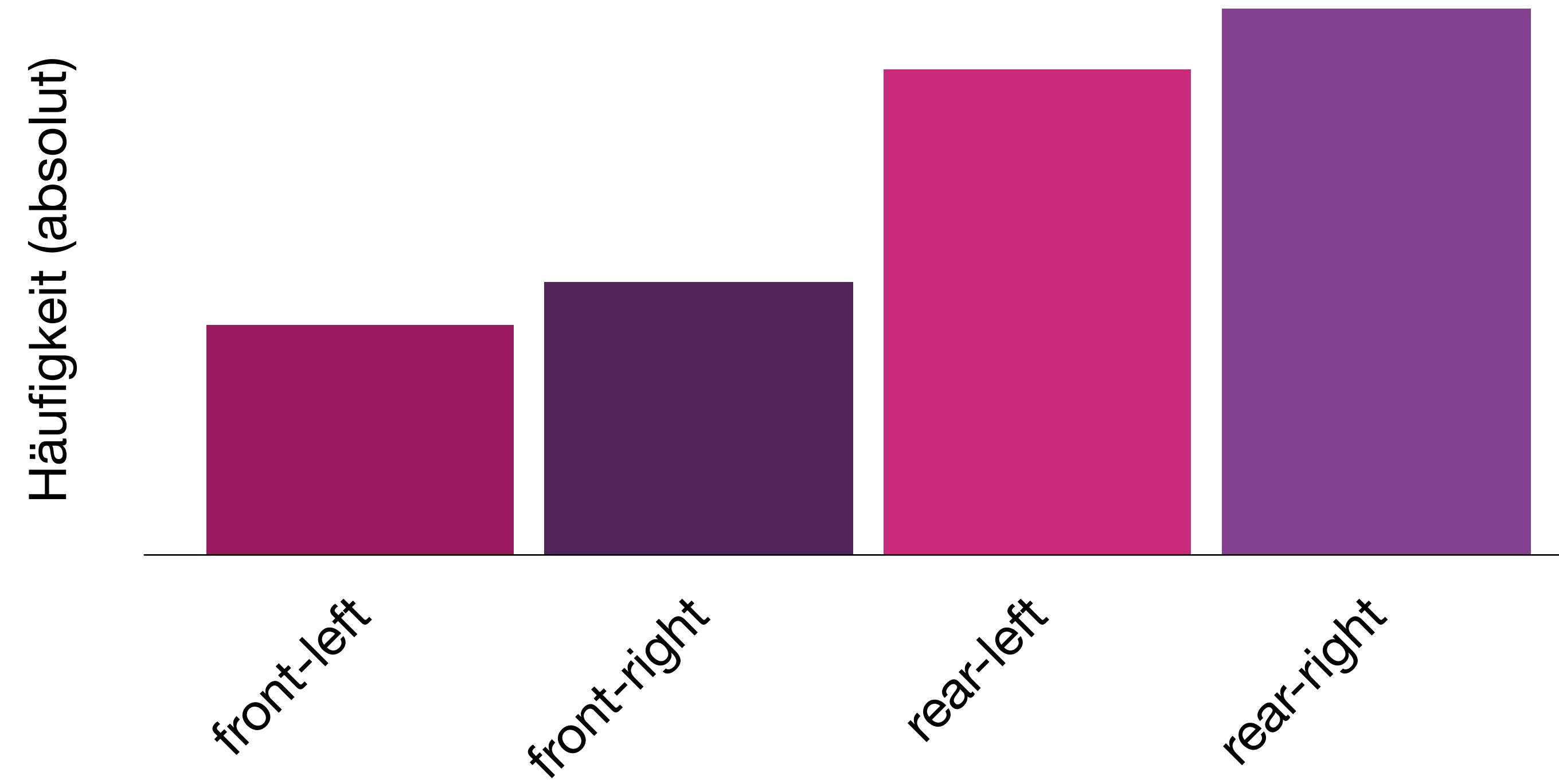
EV Data

VWs Feldbeobachtung

- Battery Status Data
- Charging Status Data
- Plug Status Data
- Ignition Events
- Warning Light Data

Warning Light Data

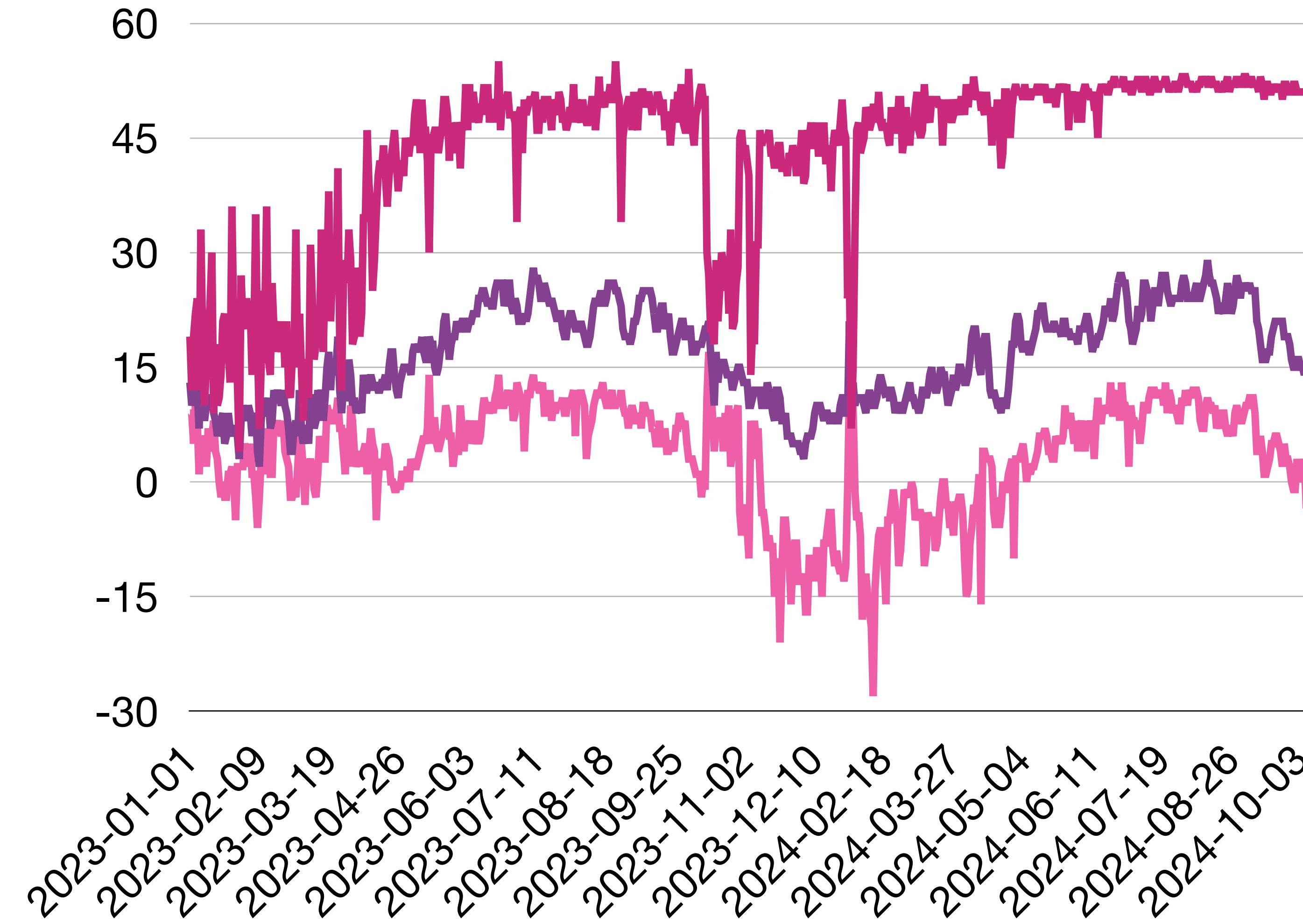
"Loss of pressure"



45x

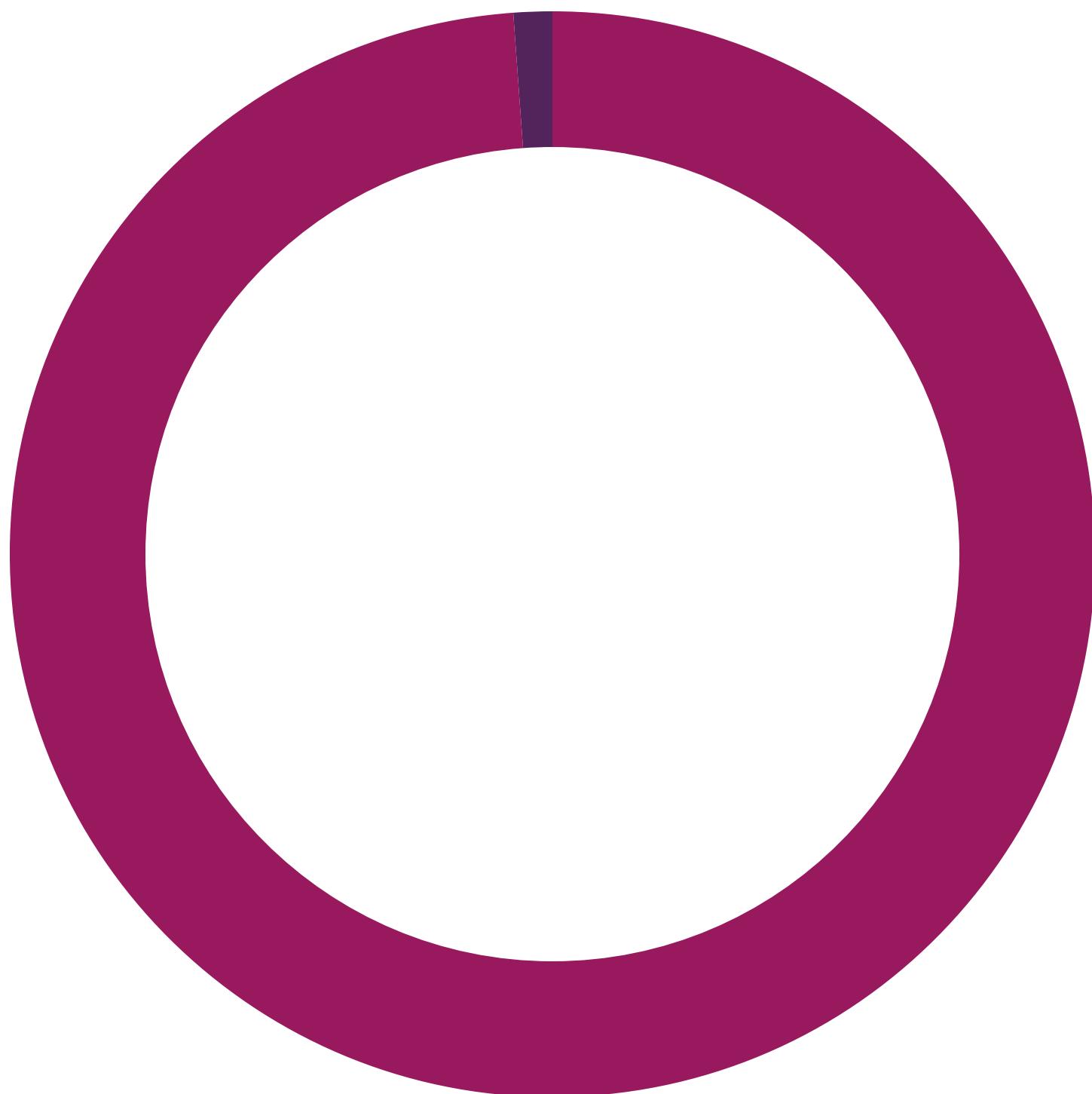
Brennende(?) Autos

Battery Temperature



Aufladeverhalten

Charging Mode



Aufladeverhalten

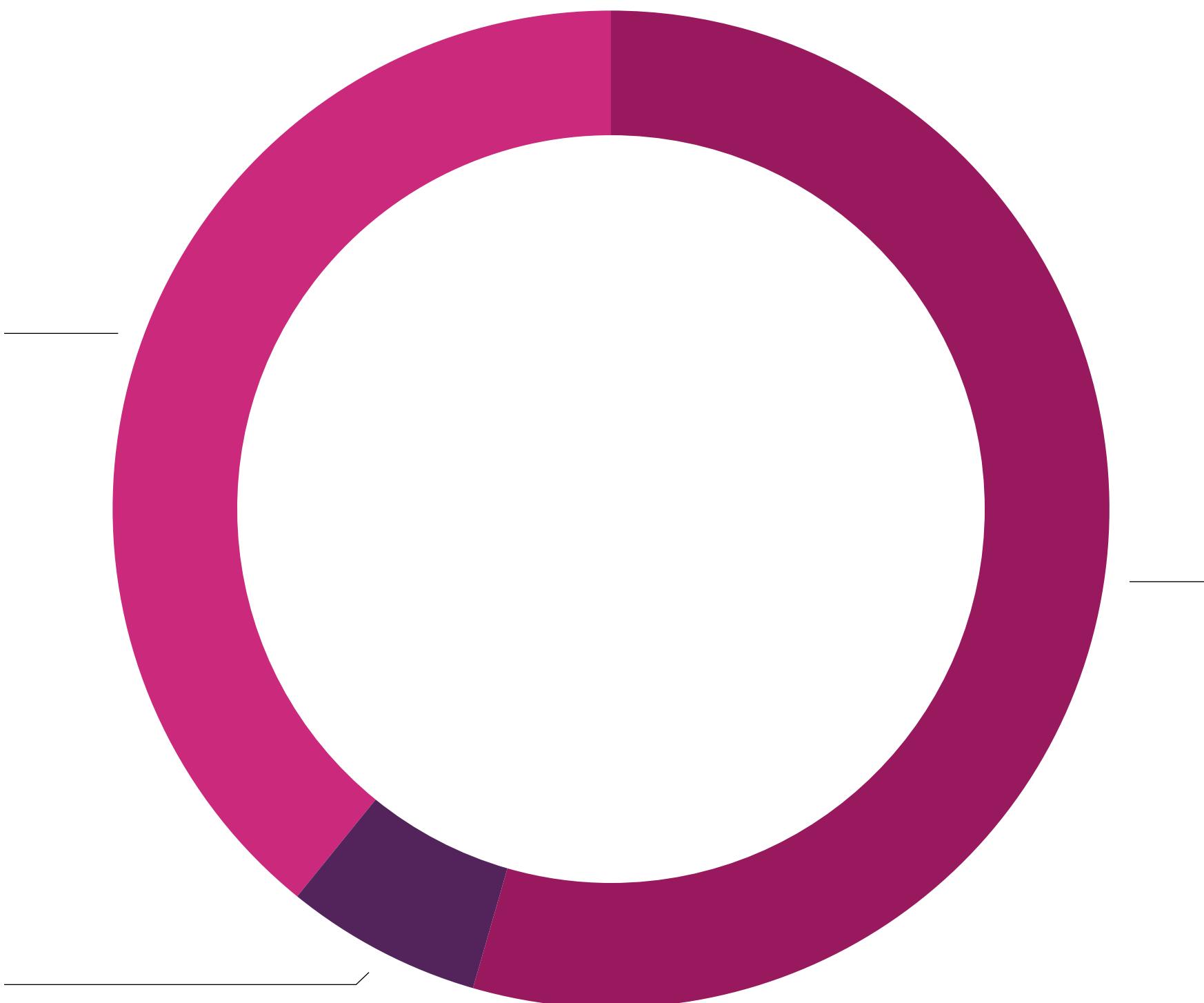
Charging Type



https://upload.wikimedia.org/wikipedia/commons/0/09/Logo_ACDC_pwrup.svg

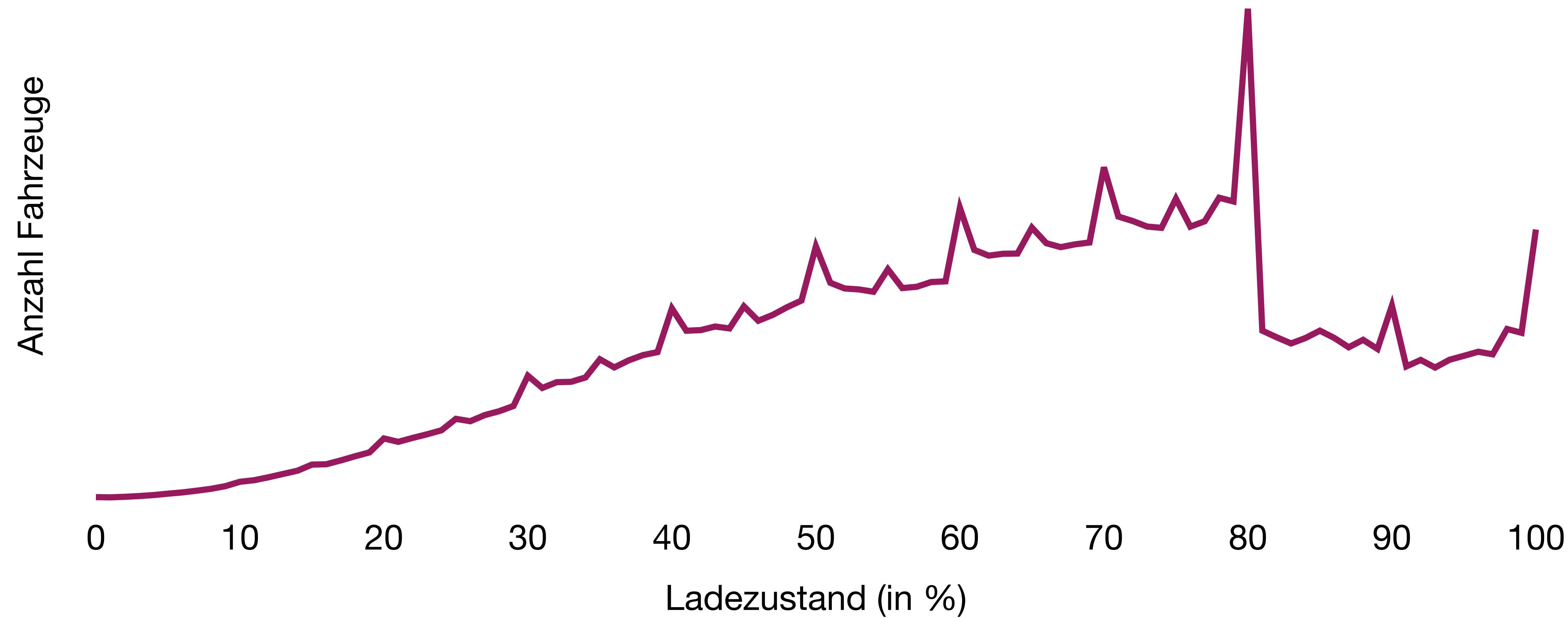
Aufladeverhalten

Charging Type



Aufladeverhalten

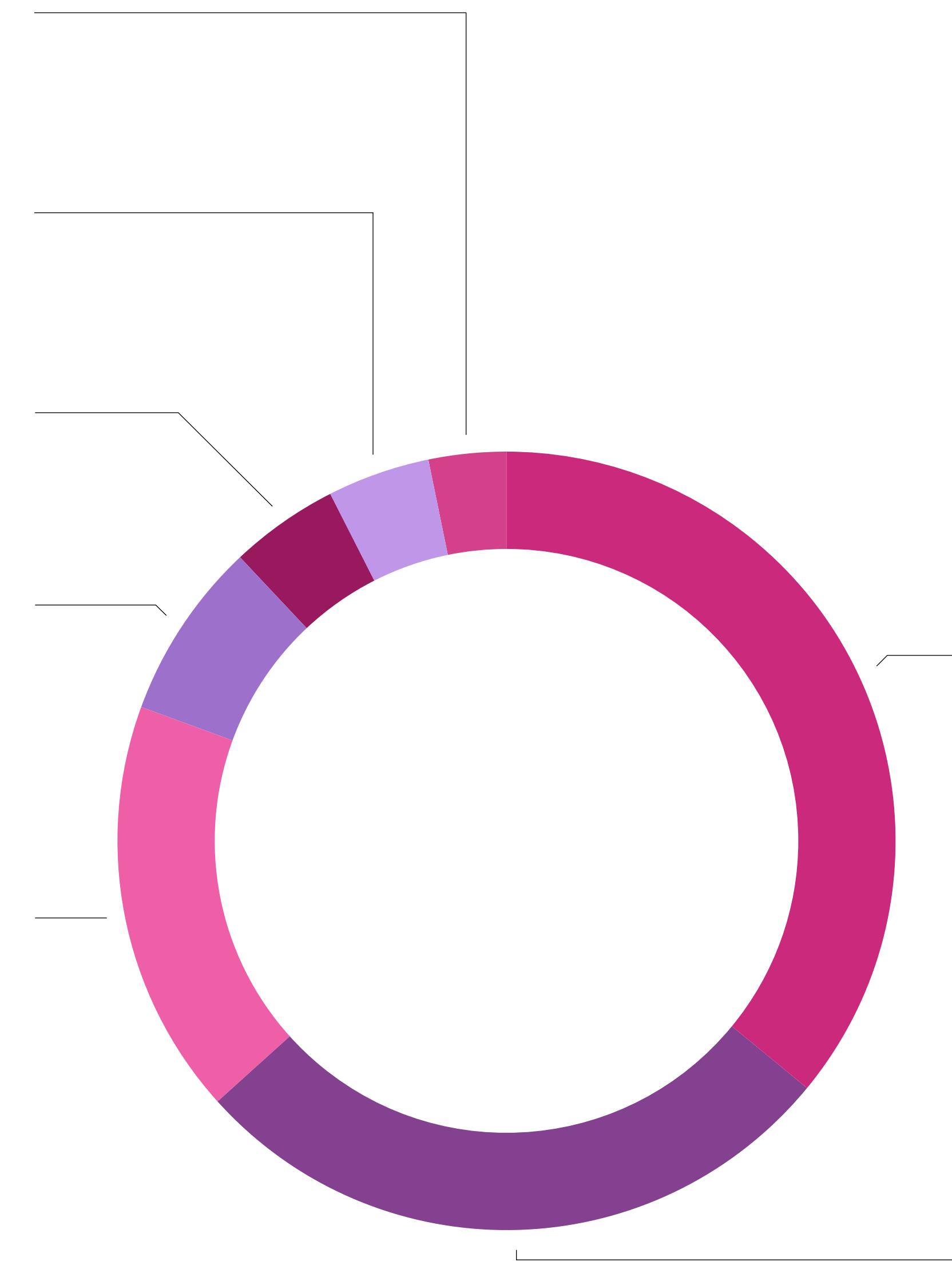
State of charge



3. User Data

User Data

Top Maildomains



Das Dilemma

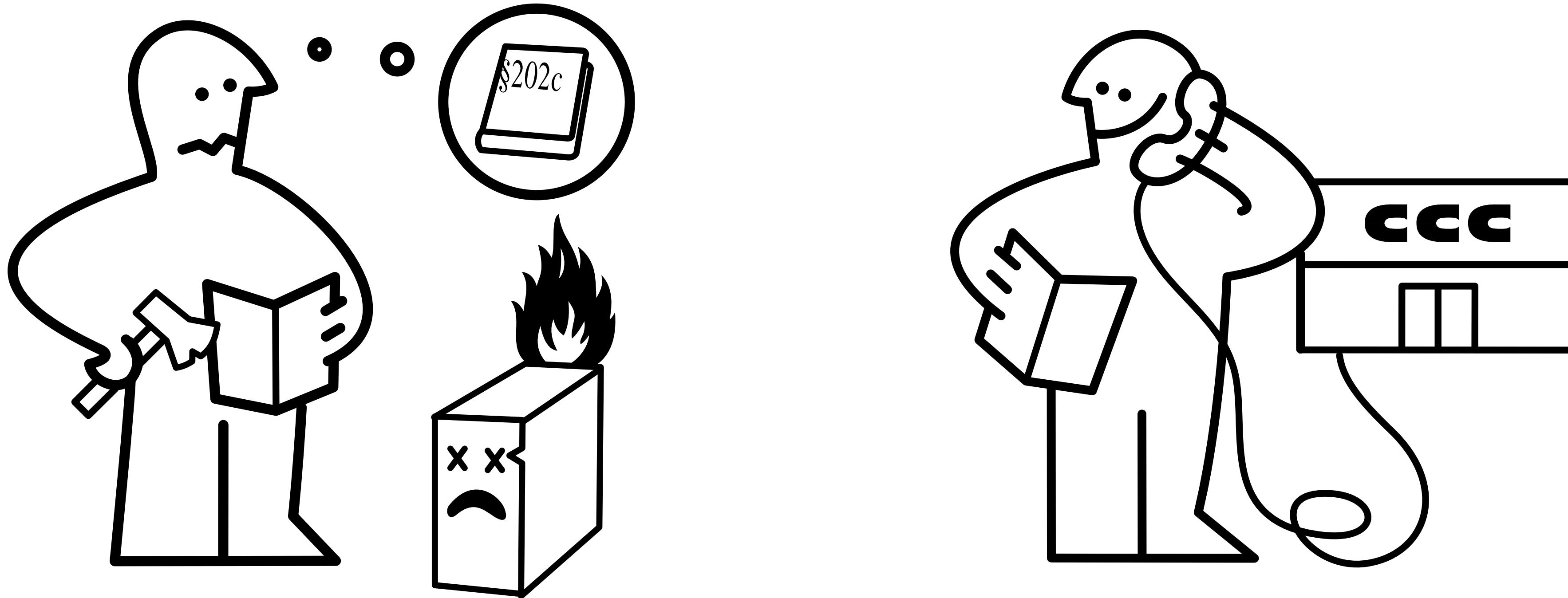
Hackerparagraph



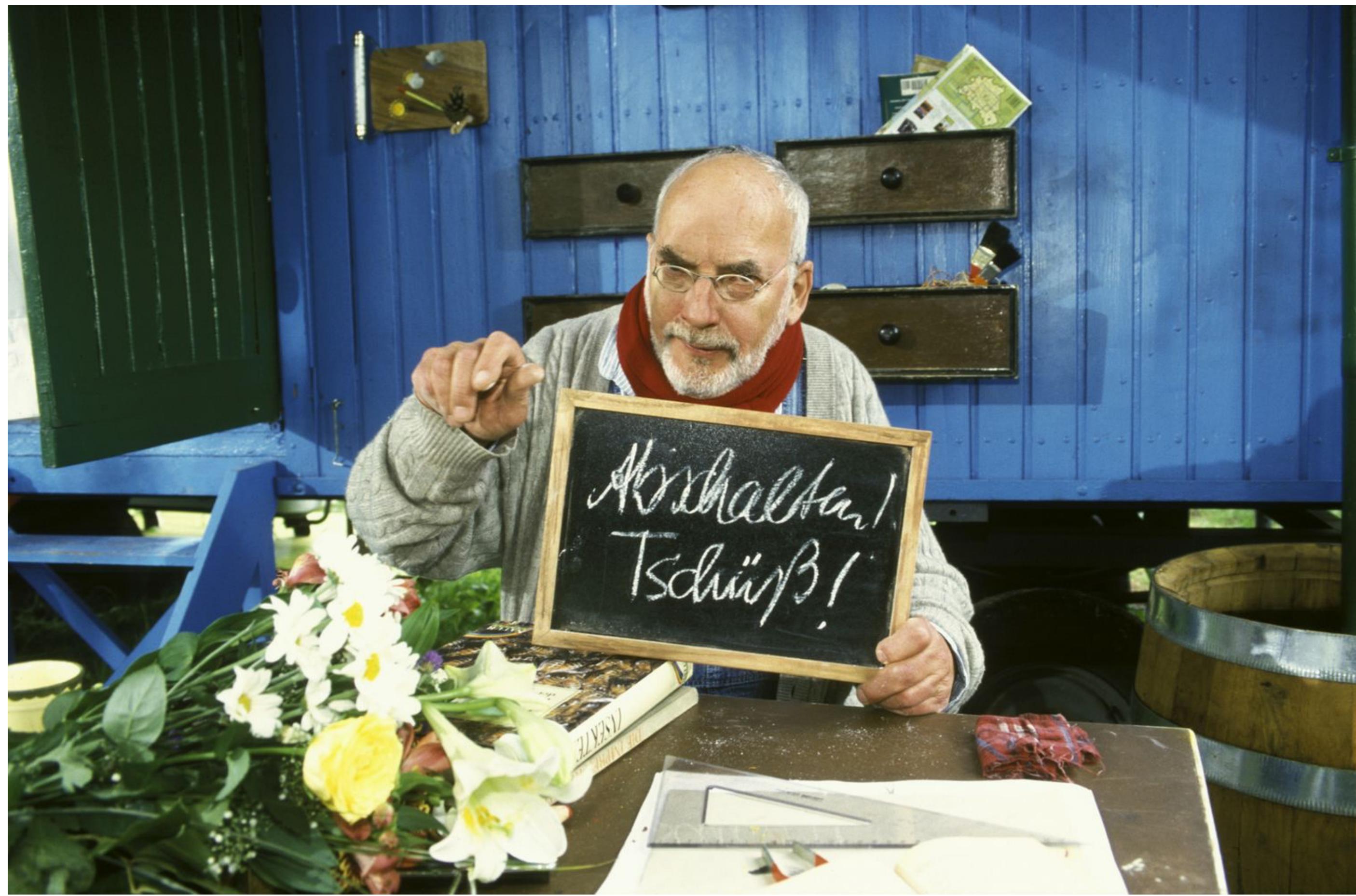
JAKE-CLARK.TUMBLR

CCC Disclosure Department

disclosure@ccc.de



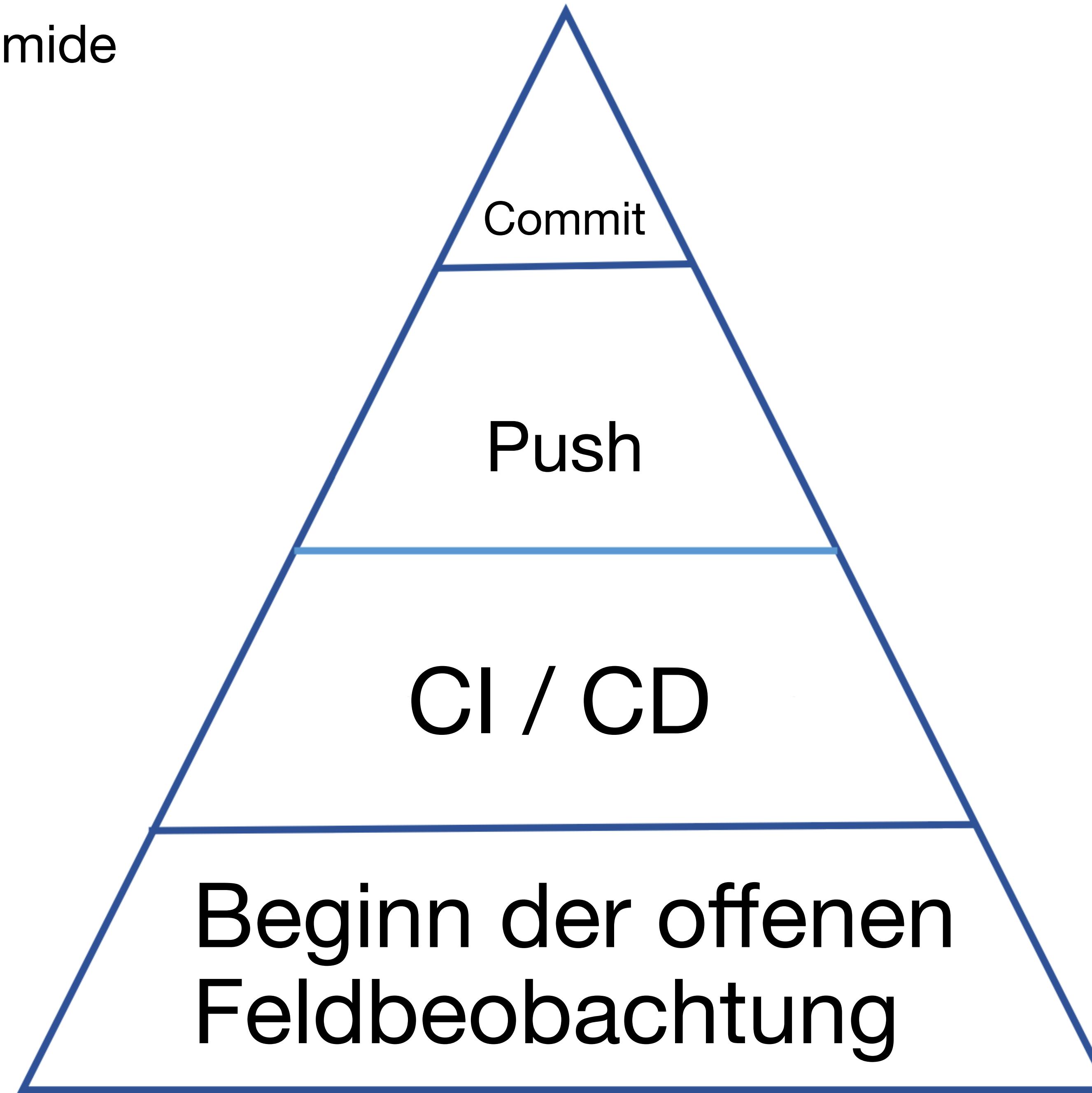
Ey, Volkswagen



https://cdn.prod.www.spiegel.de/images/bad4e508-0001-0004-0000-000000879576_w1528_r1.532871972318339_fpx45.55_fpy49.83.jpg

Disclosure

D-Day Ablaufpyramide



Ende gut, alles gut?

Nein, es wurde ~~ein~~ zwei kleine Details übersehen

Jetzt ist aber wirklich alles gut?

VW: "[...] keine sensiblen Informationen [...] betroffen."



Fragen wir den Datenjournalisten Michael Kreil!

Zusammenfassung

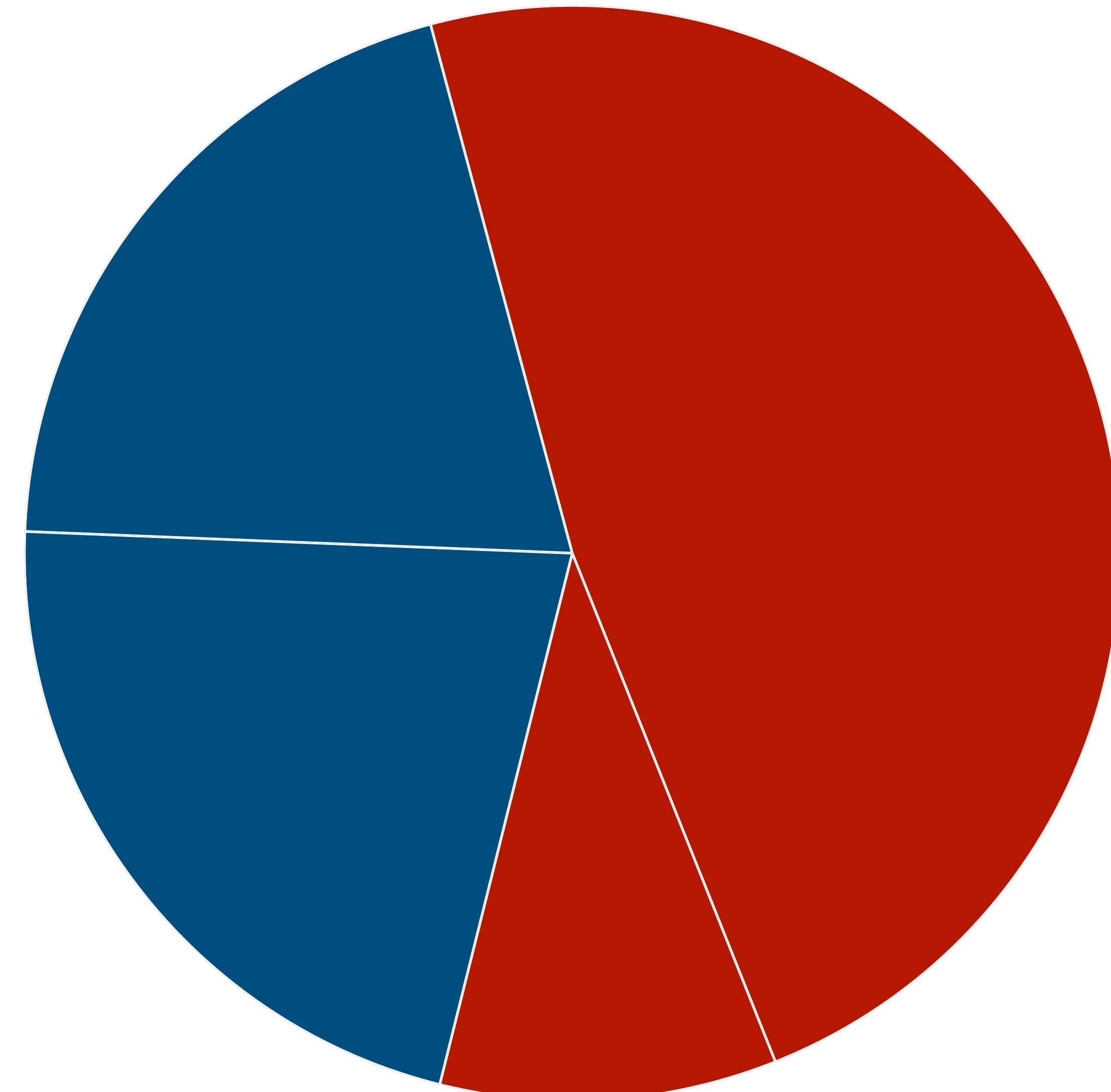
Die folgenden Daten waren unzureichend geschützt und wurden uns zugespielt:

- **enrollment data**
über 15 Mio. mal: Fahrgestellnummer, Modell, Baujahr, Land und Nutzer-ID
- **user data**
über 600'000 mal: Nutzer-ID, Name, E-Mail
und teilweise Geburtsdatum, Mobilnummer und Adresse
- **event data**
9,5 TB an Statusmeldungen, inklusive Geokoordinaten

9,5 TB JSONs

Betroffene Fahrzeuge

807'357 betroffene Fahrzeuge



338'636 Fahrzeuge

mit Geokoordinaten auf
1 Nachkommastelle, also etwa
10 km genau

468'721 Fahrzeuge

mit Geokoordinaten auf
6 Nachkommastellen, also etwa
10 cm genau

- werden von der Volkswagen AG an die für das jeweilige Land zuständigen Vertriebsgesellschaft (Importeur) für die Verbesserung von Werbung übermittelt. Im Zuge der Verarbeitung werden die personenbezogenen Daten personalisiert behandelt.
- Pseudonyme Identifikationsdaten (z.B. eine zufällig generierte pseudonyme Nutzerkennung)
 - Kfz-Nutzungsdaten (z.B. Lade-, Fahr- und Parkdaten, Lade- und Timer-Einstellungen)
 - Vertragsdaten (z.B. Fahrzeugausstattung wie die Batteriegröße)
 - IT-Nutzungsdaten (z.B. User ID, Nutzung von „VW Connect“-Diensten)
 - Standortdaten (z.B. gekürzte GPS Daten)
 - Daten zum Fahrzeug-Gesundheitszustand (z.B. Service-Intervalle, aufgetretene Warnungen, aktivierte Warnleuchten)

Im Fall im Volkswagen ID Benutzerkonto hinterlegter Fahrzeuge verarbeitet die Volkswagen AG die Fahrzeugidentifikationsnummer und reichert die oben aufgeführten Daten mit weiteren Ausstattungsdaten des jeweiligen Fahrzeuges an. Im Zuge der Verarbeitung werden personenbezogenen Daten pseudonymisiert. Die Pseudonymisierung beinhaltet die Entfernung aller direkten persönlichen Identifikationsmerkmale (z.B. Fahrzeugidentifikationsnummer). Indirekt rückführbare Identifikationsmerkmale (Pseudonyme) werden beibehalten. Darüber hinaus kürzen wir auch die GPS-Daten. Erst im Anschluss an diese Pseudonymisierung und Kürzung werden die Daten in den Analytics-Systemen der Volkswagen AG analysiert. Es erfolgt zu keinem Zeitpunkt eine Wiederherstellung des direkten Personenbezugs. Die aus der Analyse resultierenden Ergebnisse (insbesondere Metriken und Kennzahlen) sind vollständig anonym.

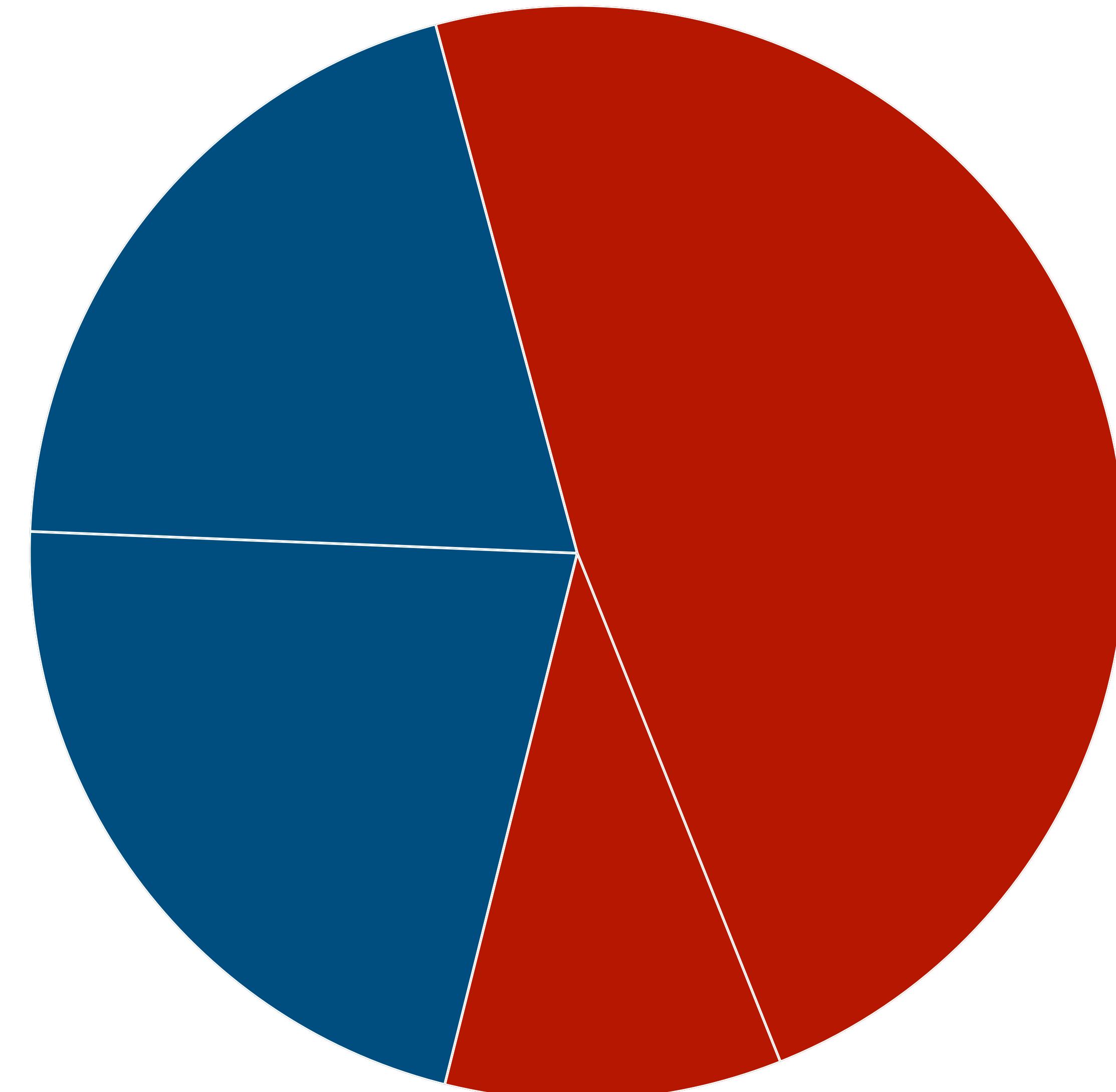
„Parkposition“ sowie „Abfahrtszeiten“ erhoben werden, verarbeitet und vor der Auswertung für die Funktion „Ladestationen-Datenservice“ anonymisiert.

Wird das Fahrzeug im Offline-Modus genutzt, werden keine Daten erfasst und an das Backend ausgeleitet. Der Offline-Modus kann im Fahrzeug eingestellt werden.

Personenbezogene Daten: Fahrzeug-Identifizierungsnummer (VIN); Parkposition; Zeitstempel; tatsächliche Ladesäulenleistung; Stromtyp (AC oder DC); Steckerstatus des Ladesteckers; verwendeter Steckertyp; eingestellte Ladegrenze; Timer Charging; Batterieladezustand (SOC); Informationen zum Abschnitt des Ladeprozesses; Grund des Ladeendes

Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO für die Anonymisierung der Daten: Das berechtigte

807'357 betroffene Fahrzeuge



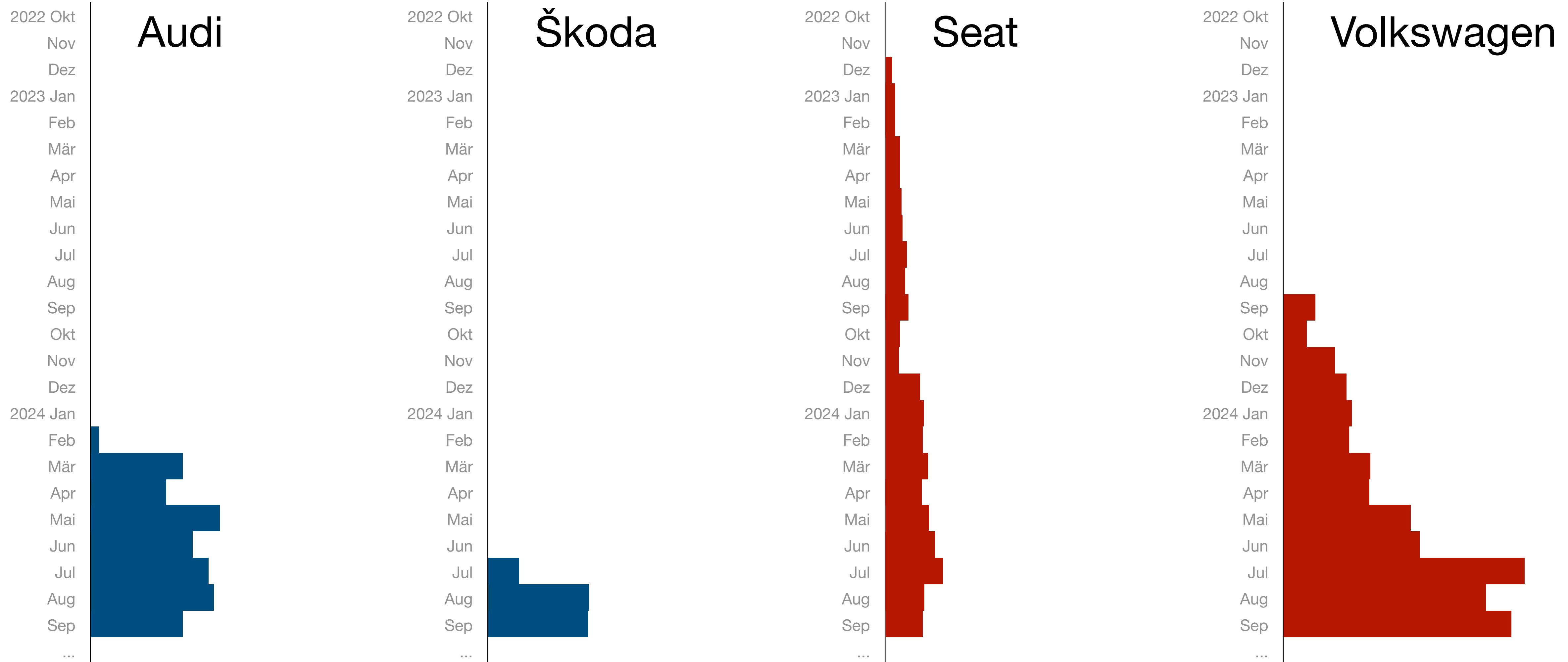
338'636 Fahrzeuge

mit Geokoordinaten auf
1 Nachkommastelle, also etwa
10 km genau

468'721 Fahrzeuge

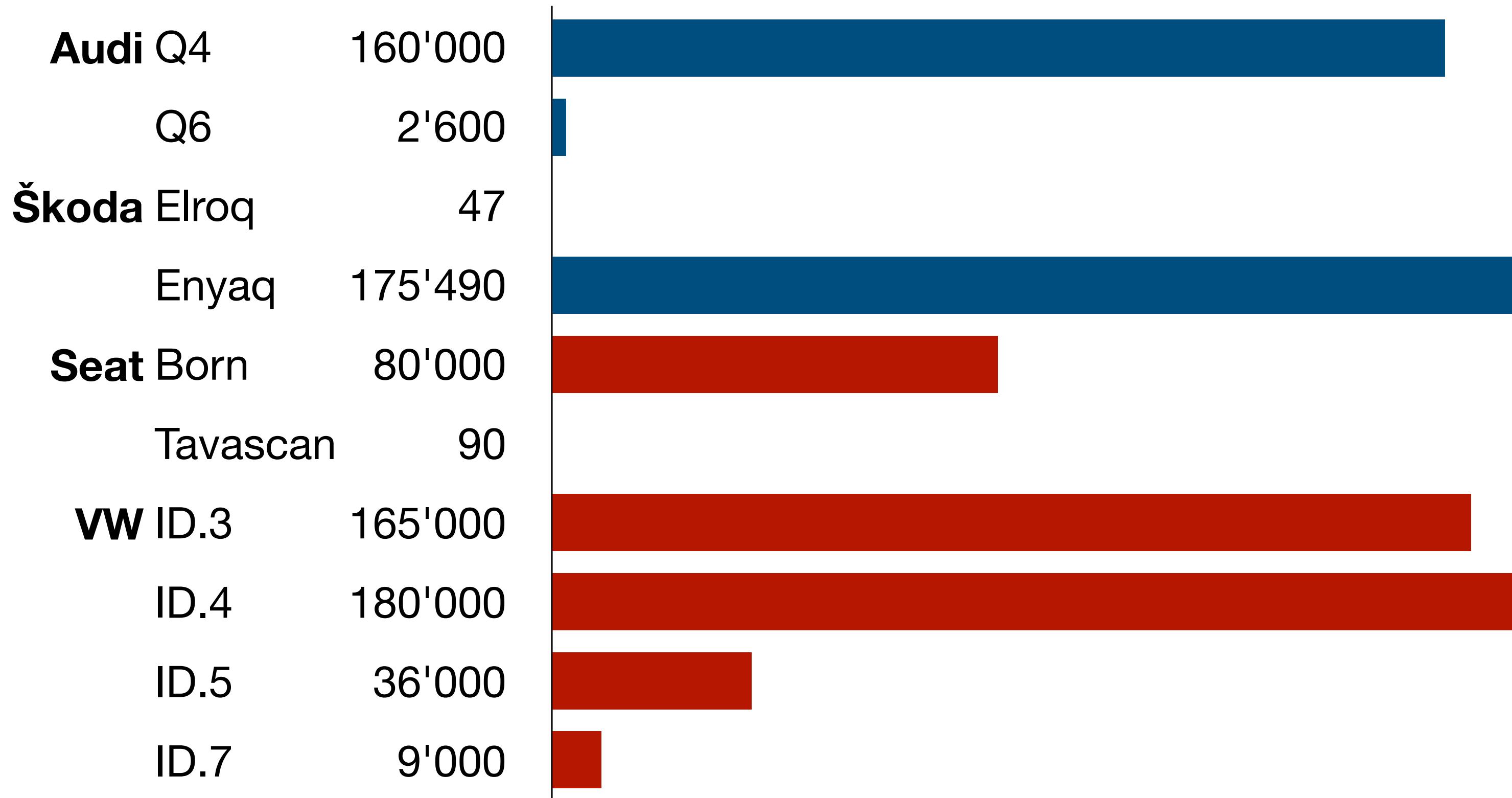
mit Geokoordinaten auf
6 Nachkommastellen, also etwa
10 cm genau

893'392'605 Geokoordinaten nach Zeit



Fahrzeuge nach Modell

(teilweise hochgerechnet)

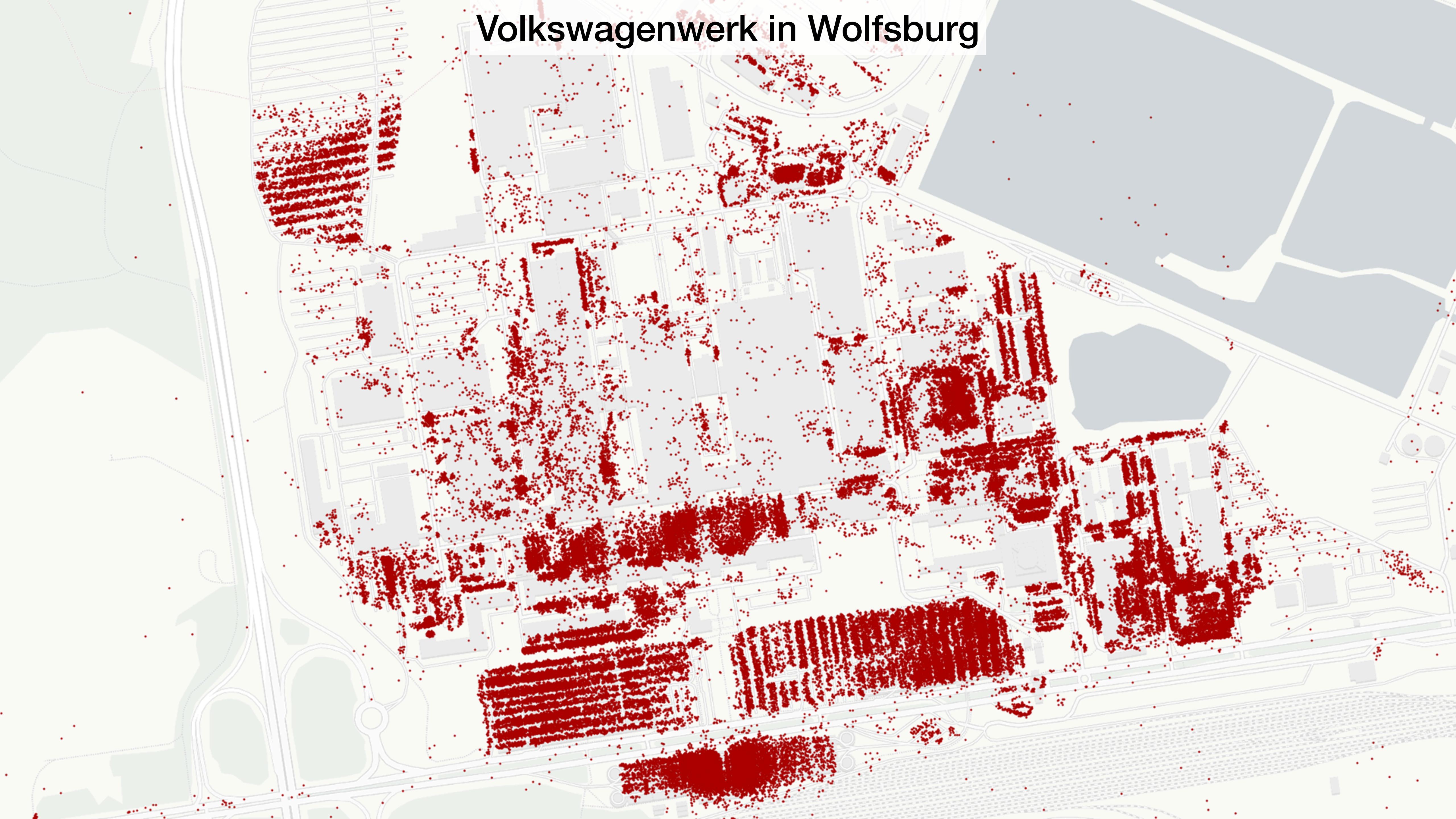


Geokoordinaten

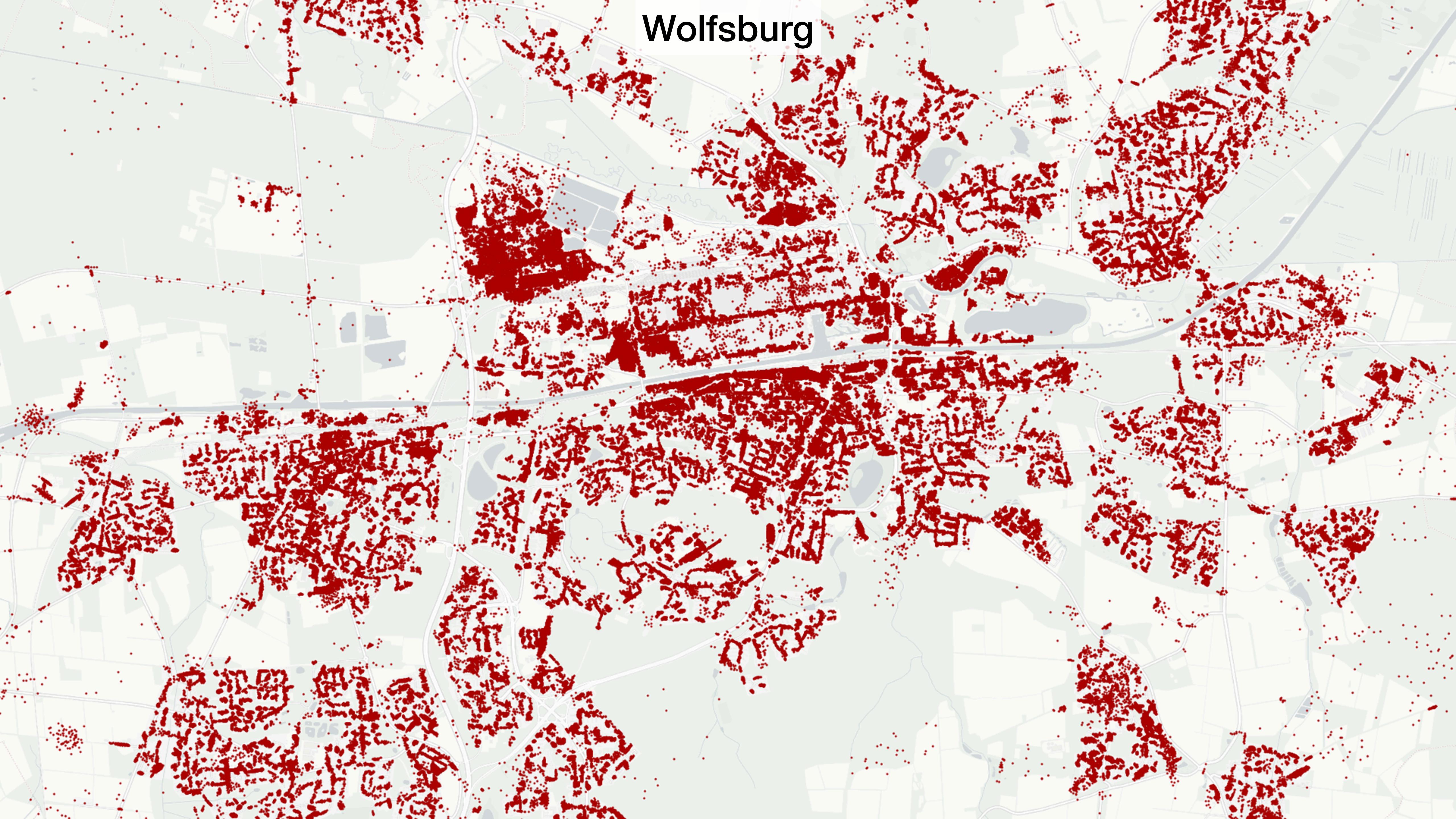
Disclaimer: Kartenausschnitte

- Alle Daten sind sauber anonymisiert
- Clustering mit Gaussian Mixture Model (GMM)
- Cluster enthalten mindestens 5 verschiedene Fahrzeuge
- Dargestellt werden nur normalverteilte Zufallspunkte dieser Cluster
- Identifikation einzelner Fahrzeuge ausgeschlossen

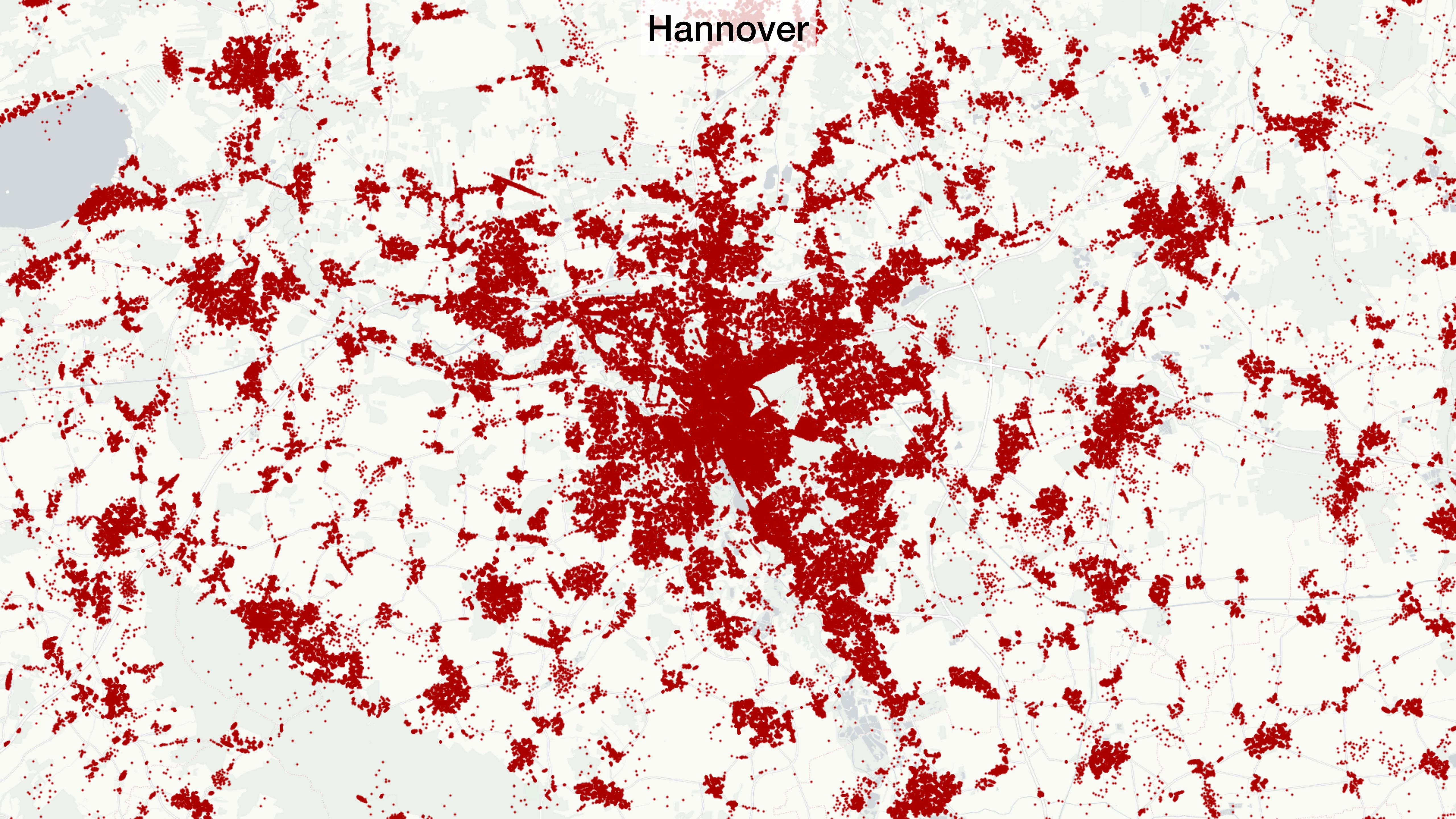
Volkswagenwerk in Wolfsburg

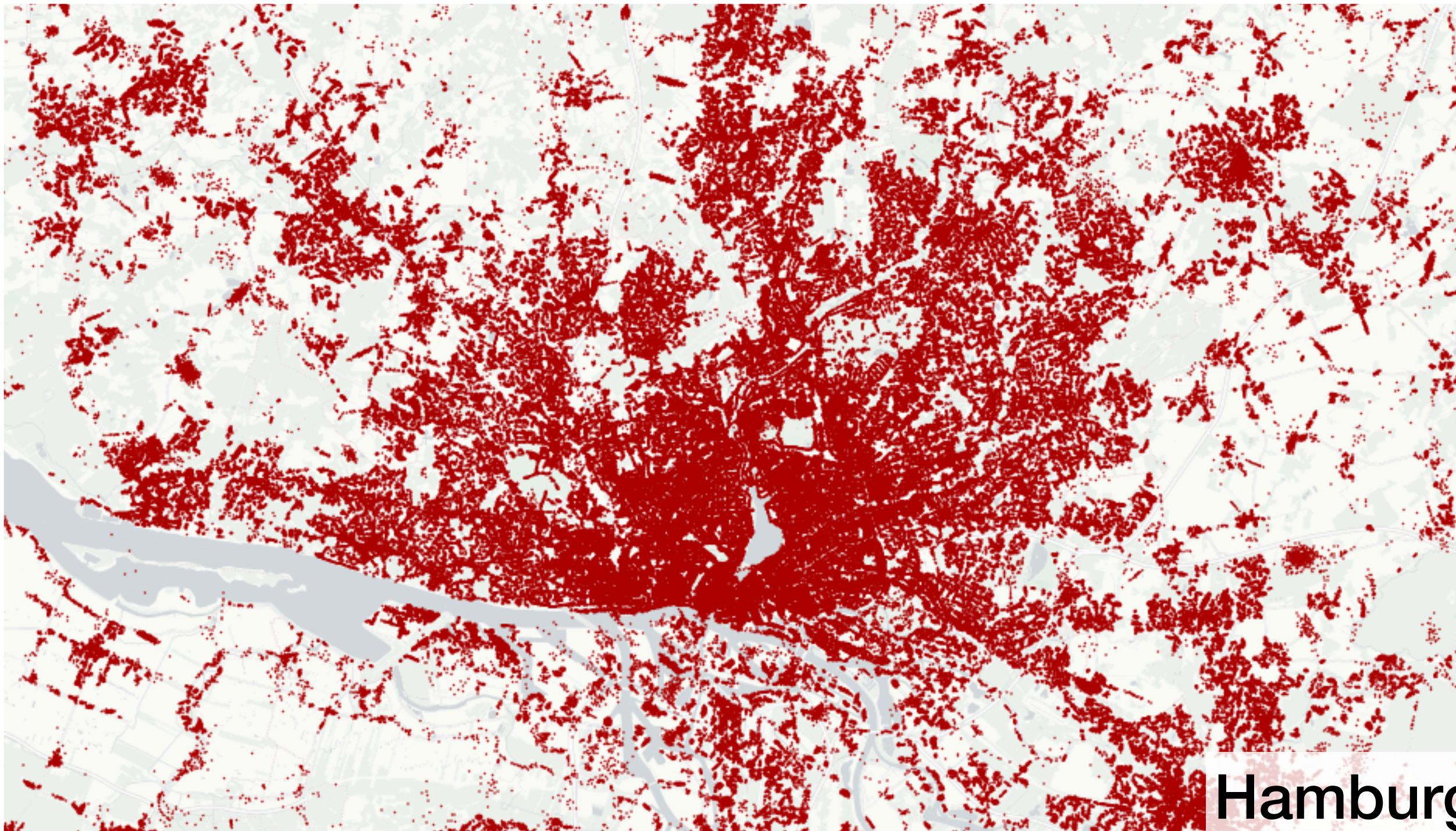


Wolfsburg

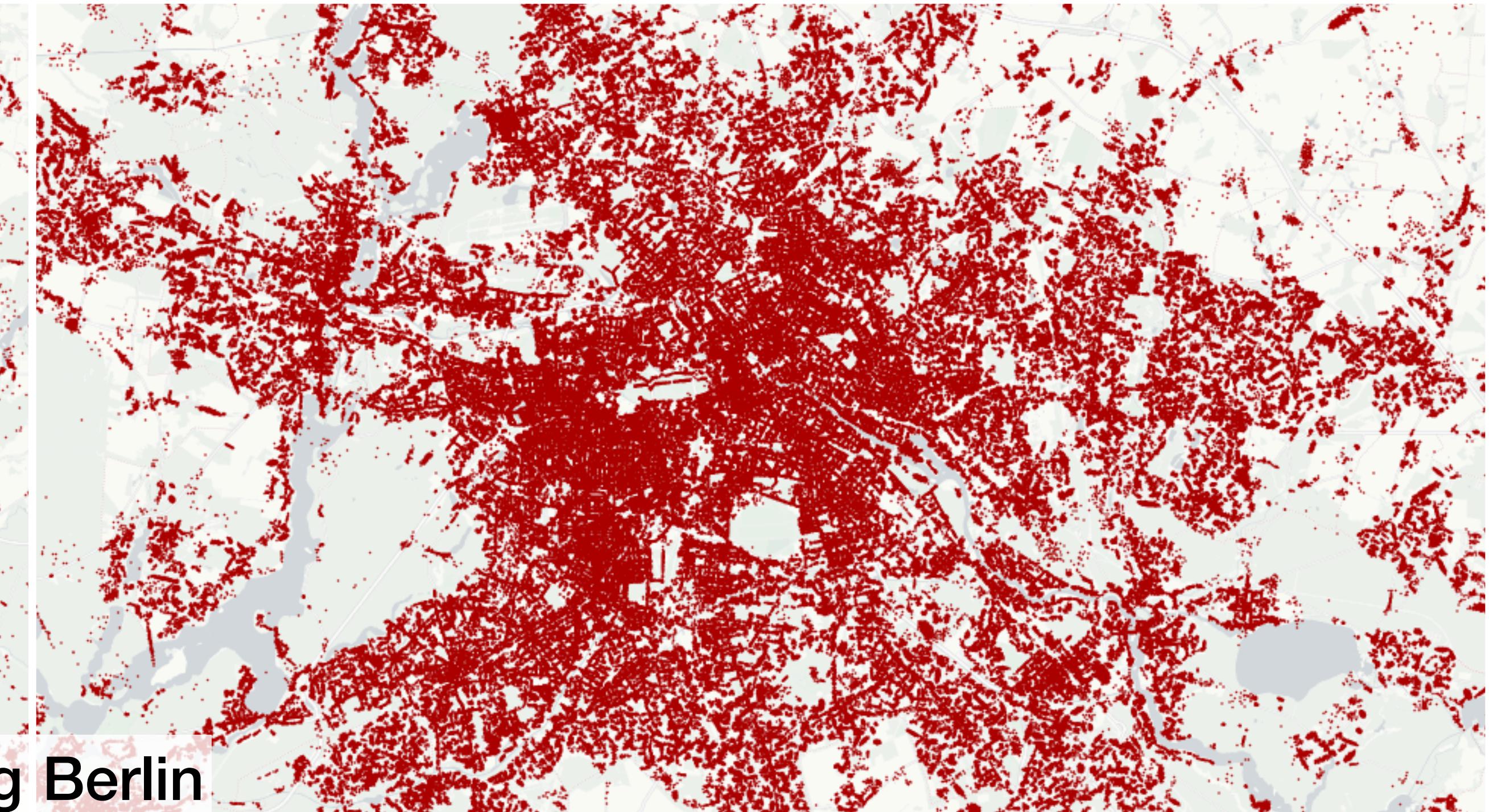


Hannover

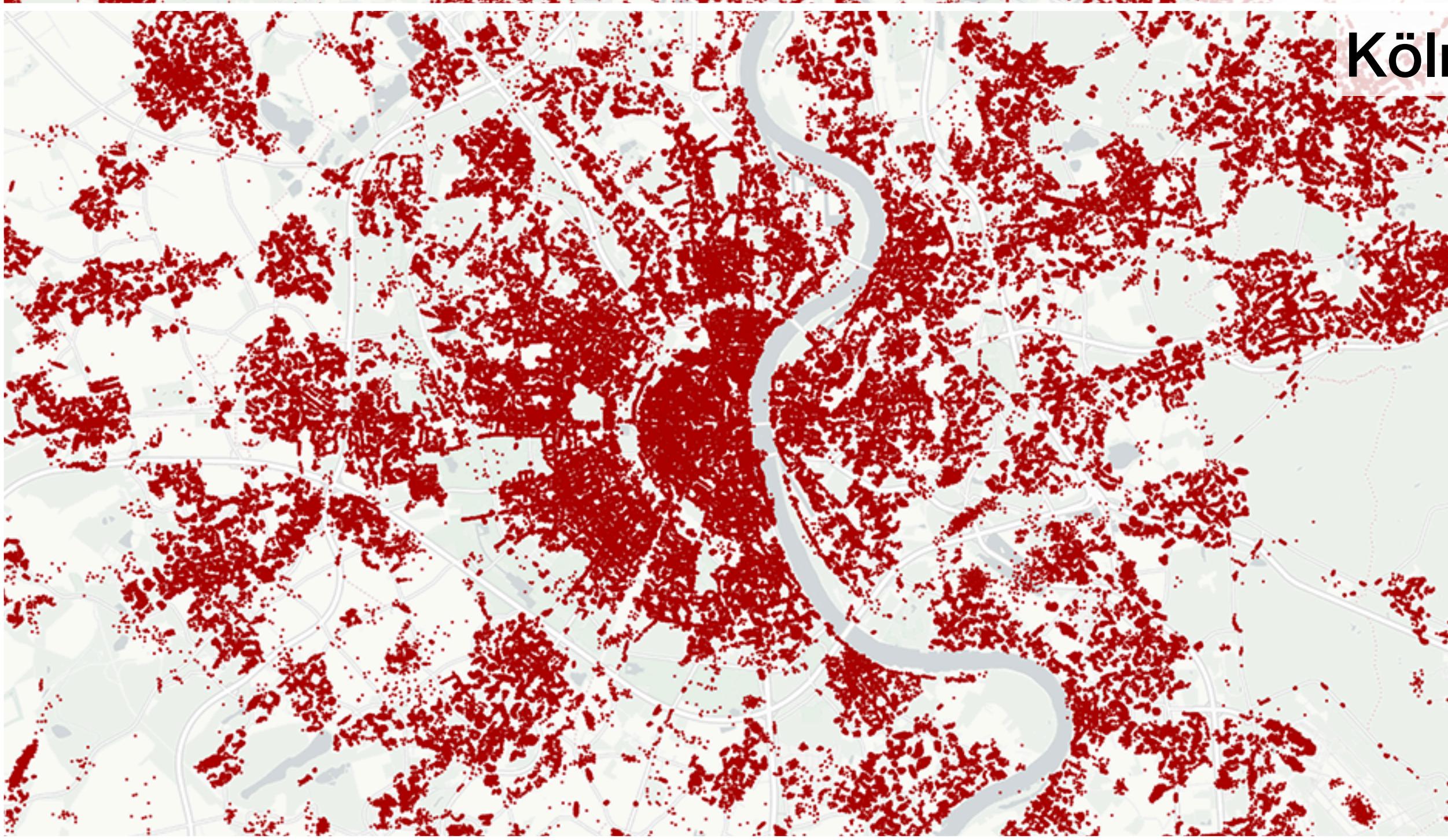




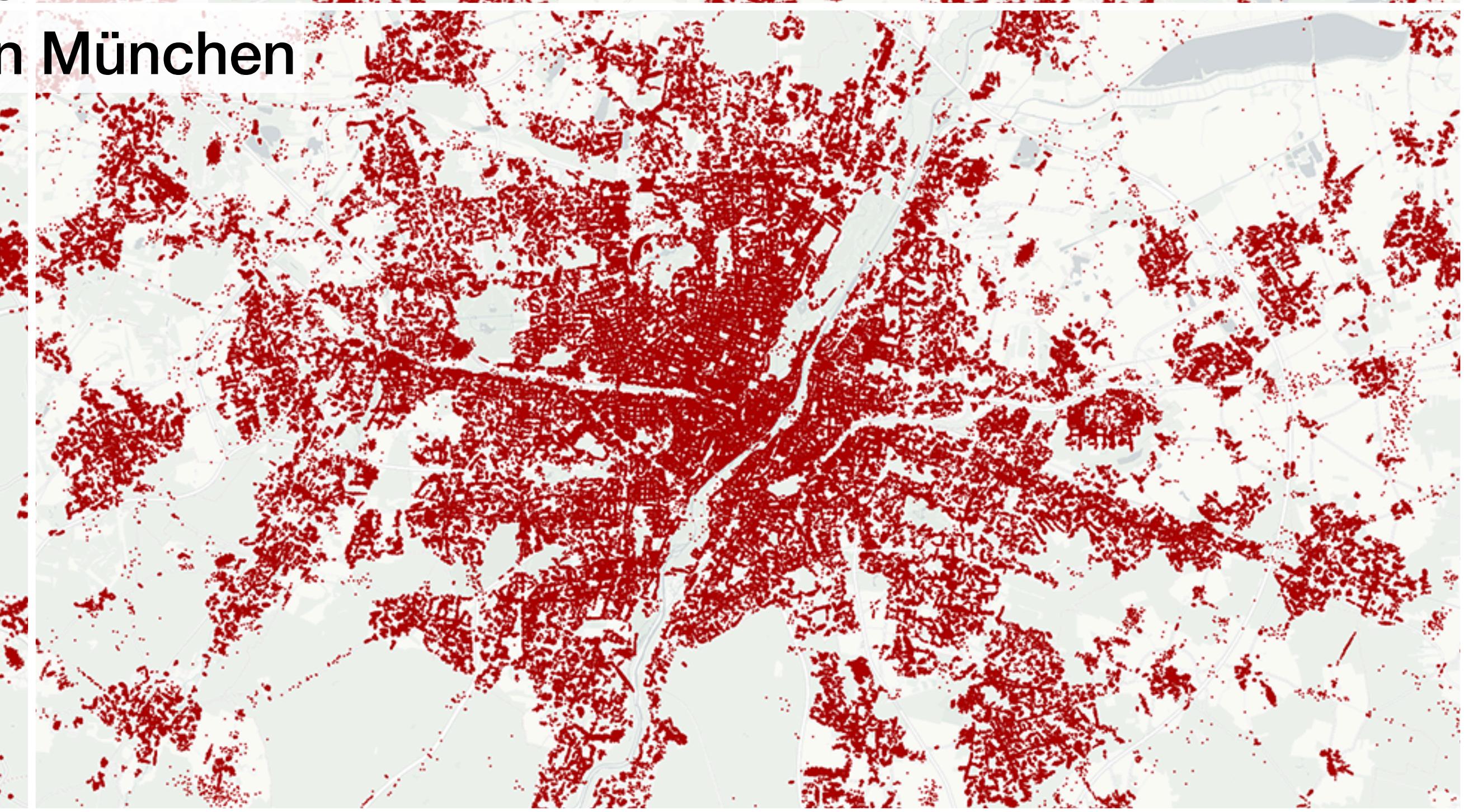
Hamburg



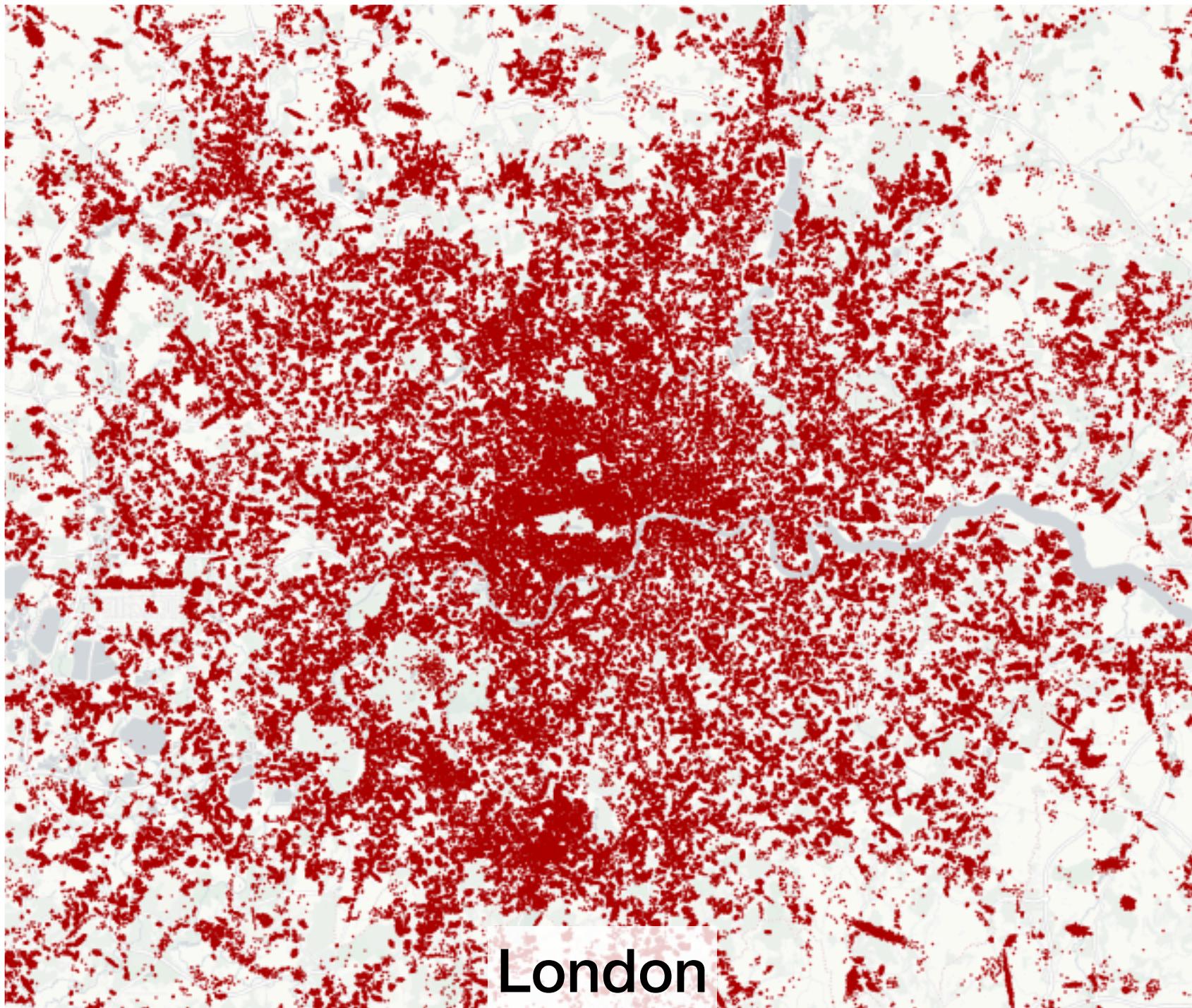
Berlin



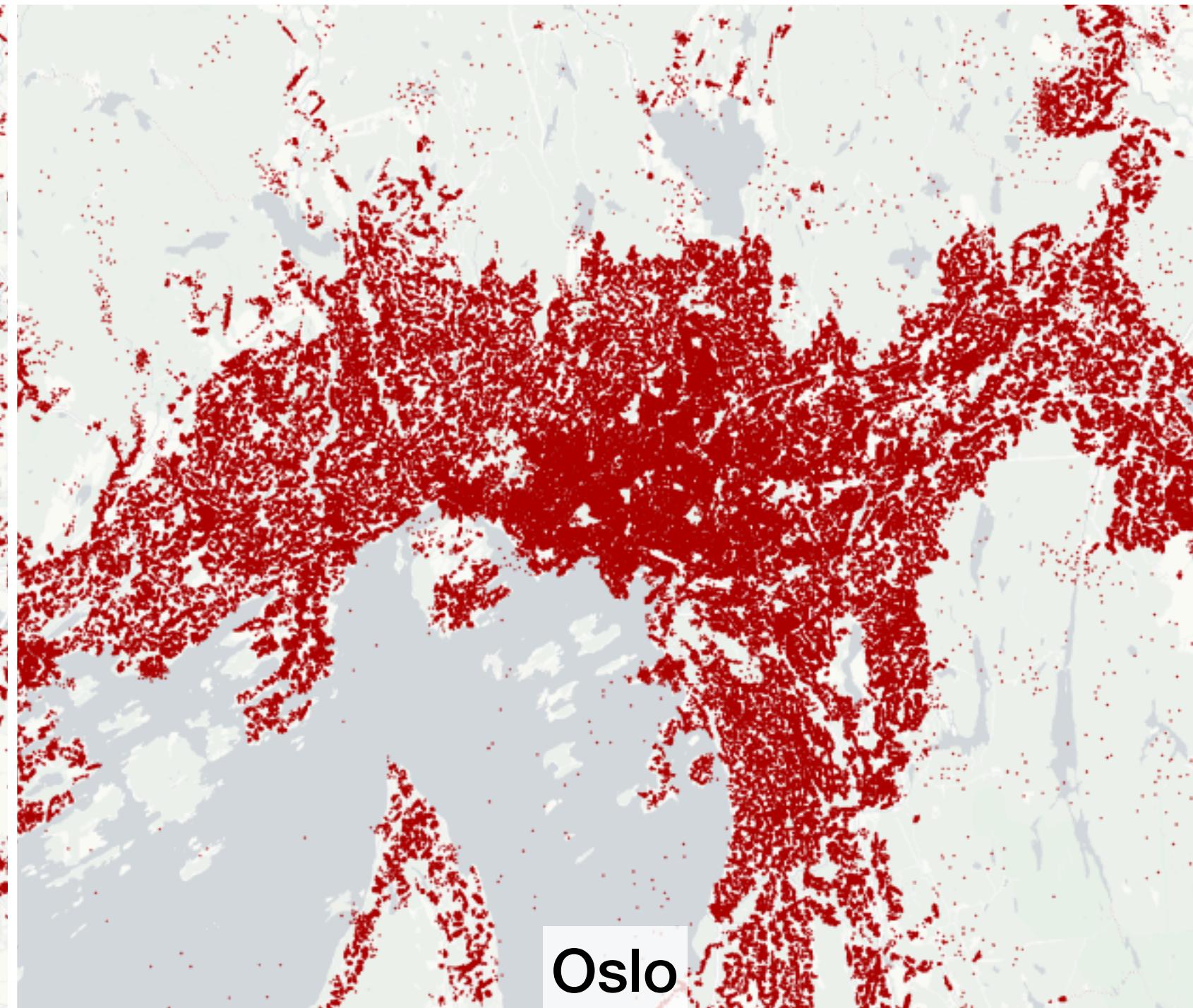
Köln



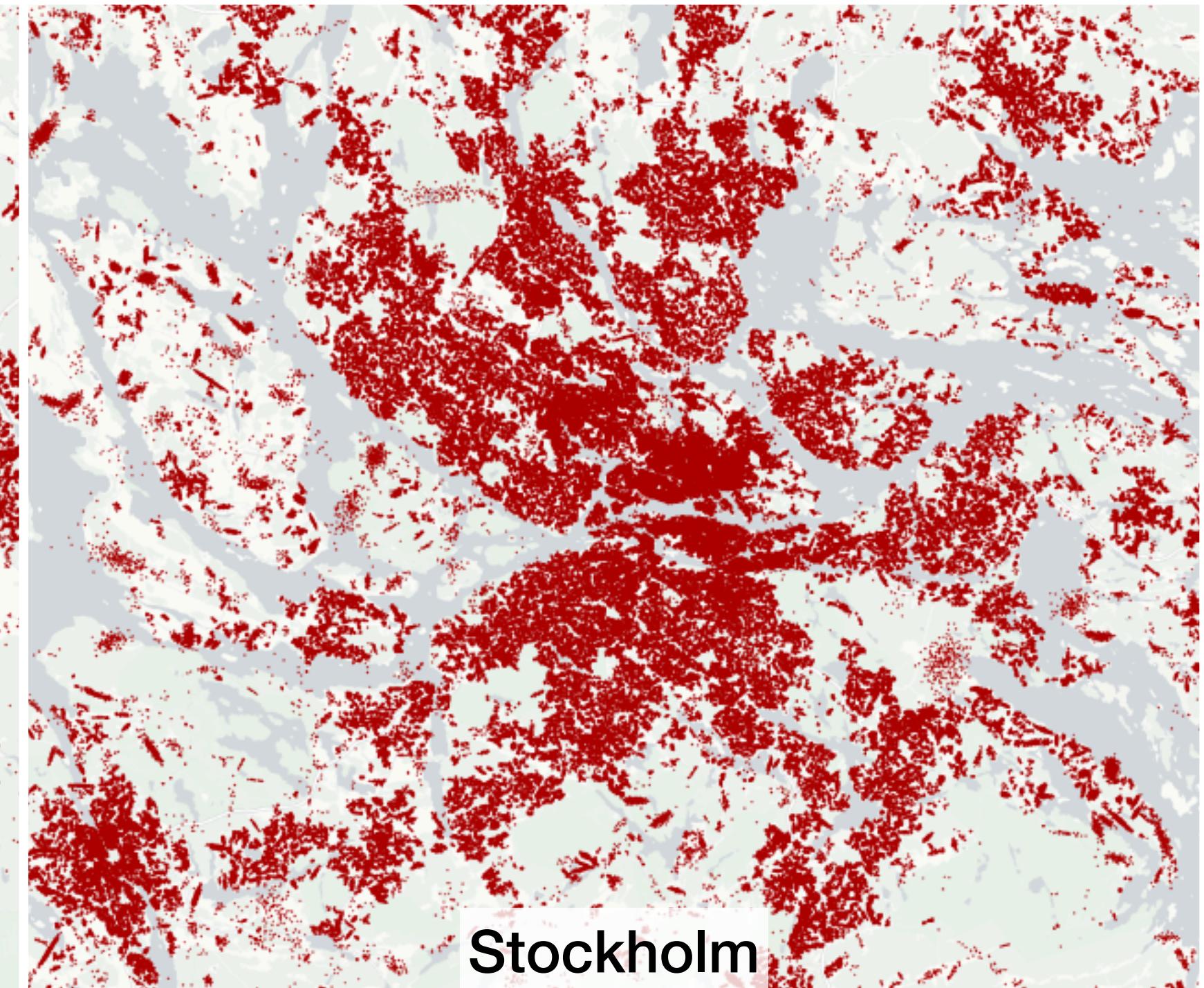
München



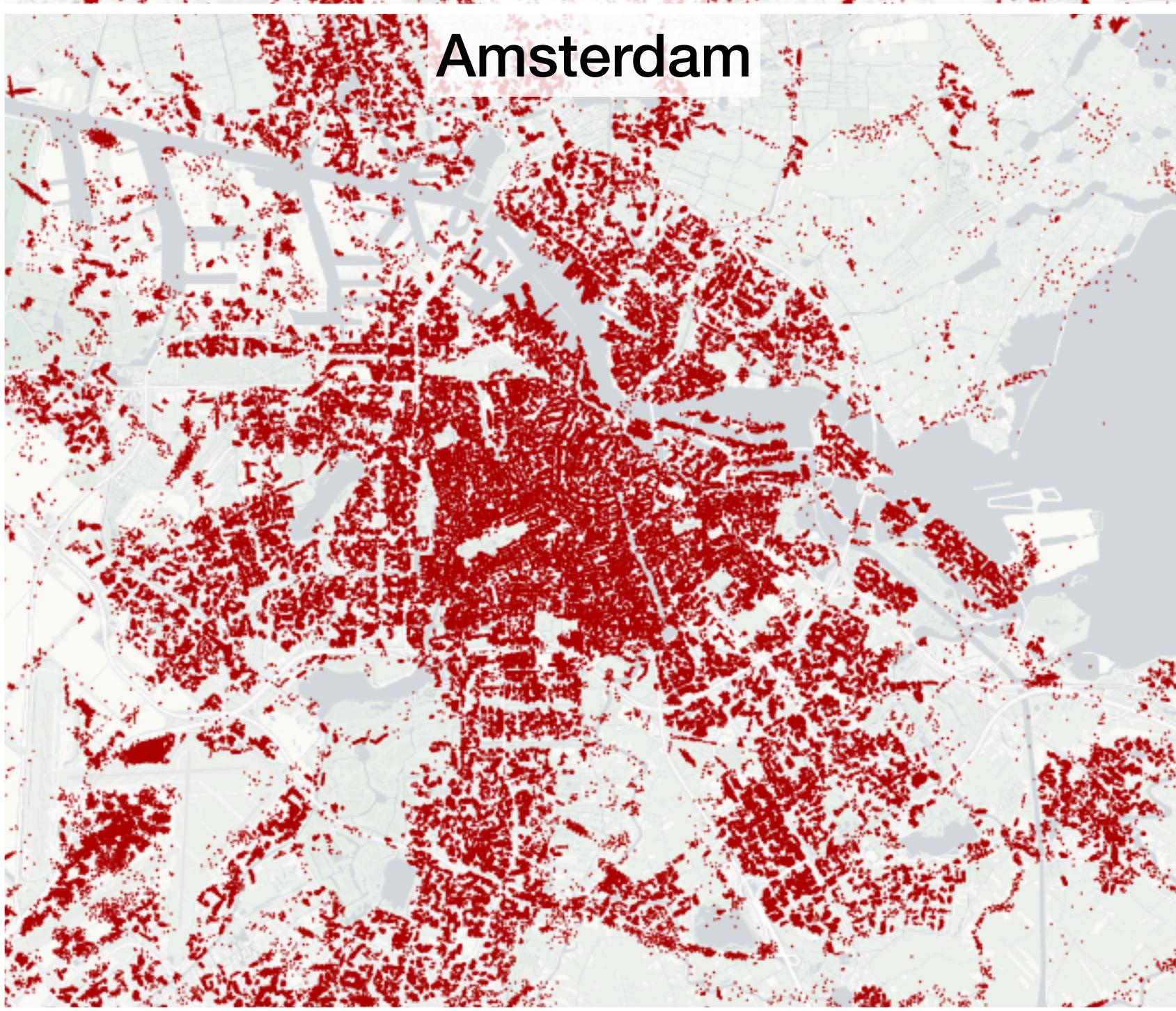
London



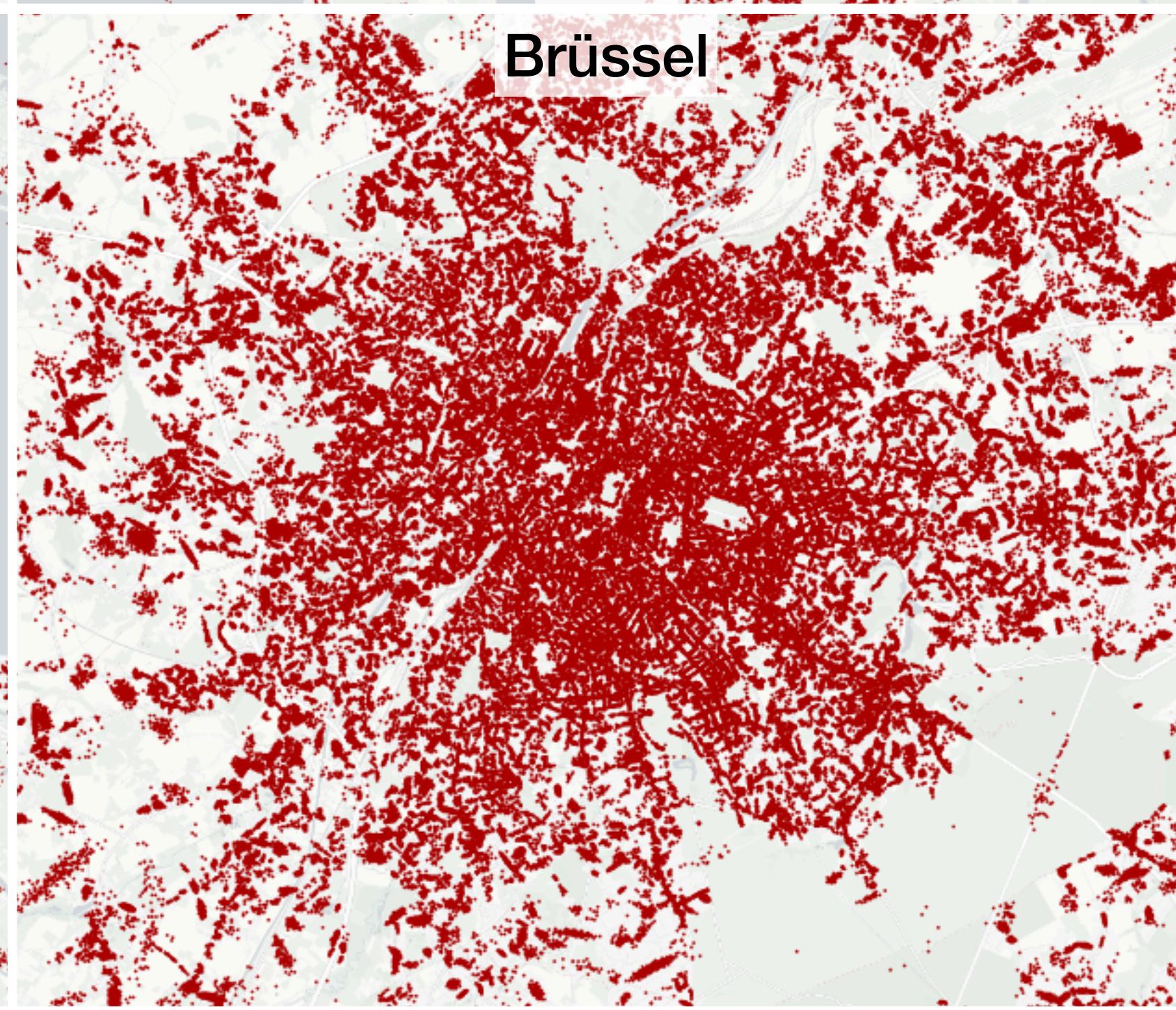
Oslo



Stockholm
Kopenhagen

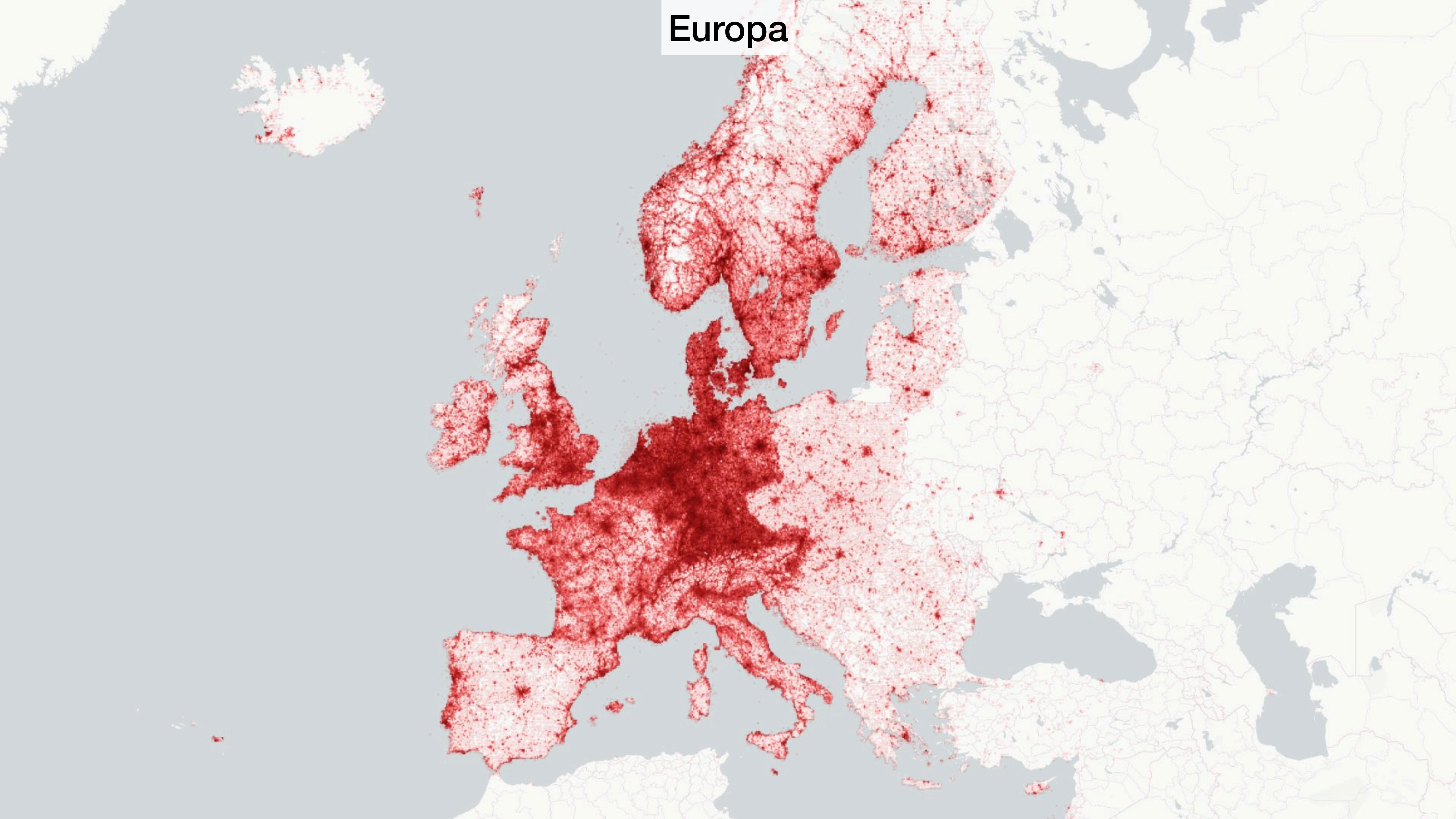


Amsterdam



Brüssel

Europa



Was steckt in den Daten?



VersaTiles

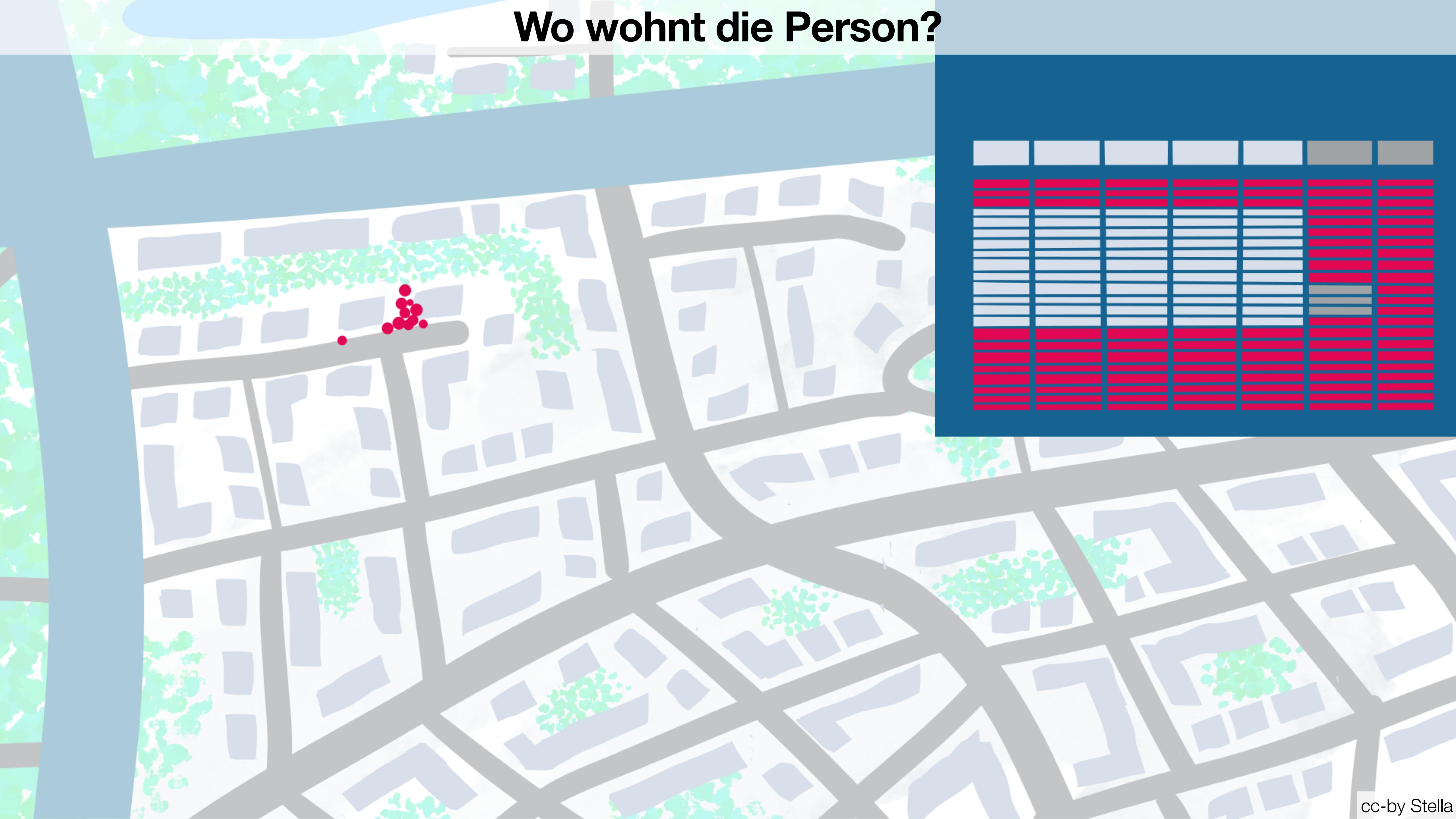
A COMPLETE FLOSS MAP STACK

versatiles.org

Natürlich zeigen wir euch
nicht die Originaldaten.

**Stella kann euch zeigen,
was sie gesehen hat.**

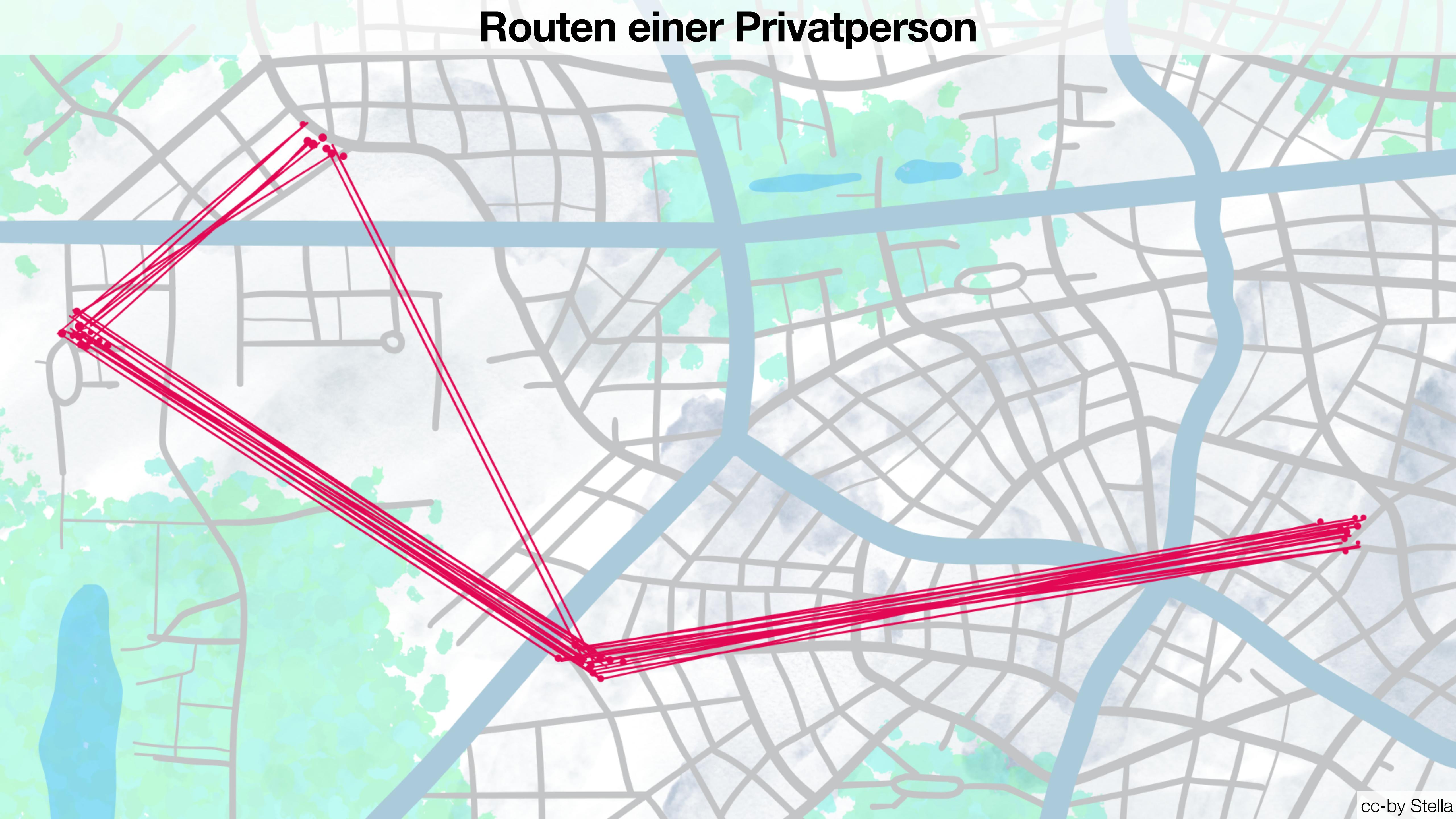
Wo wohnt die Person?



Wann und wo geht die Person arbeiten?



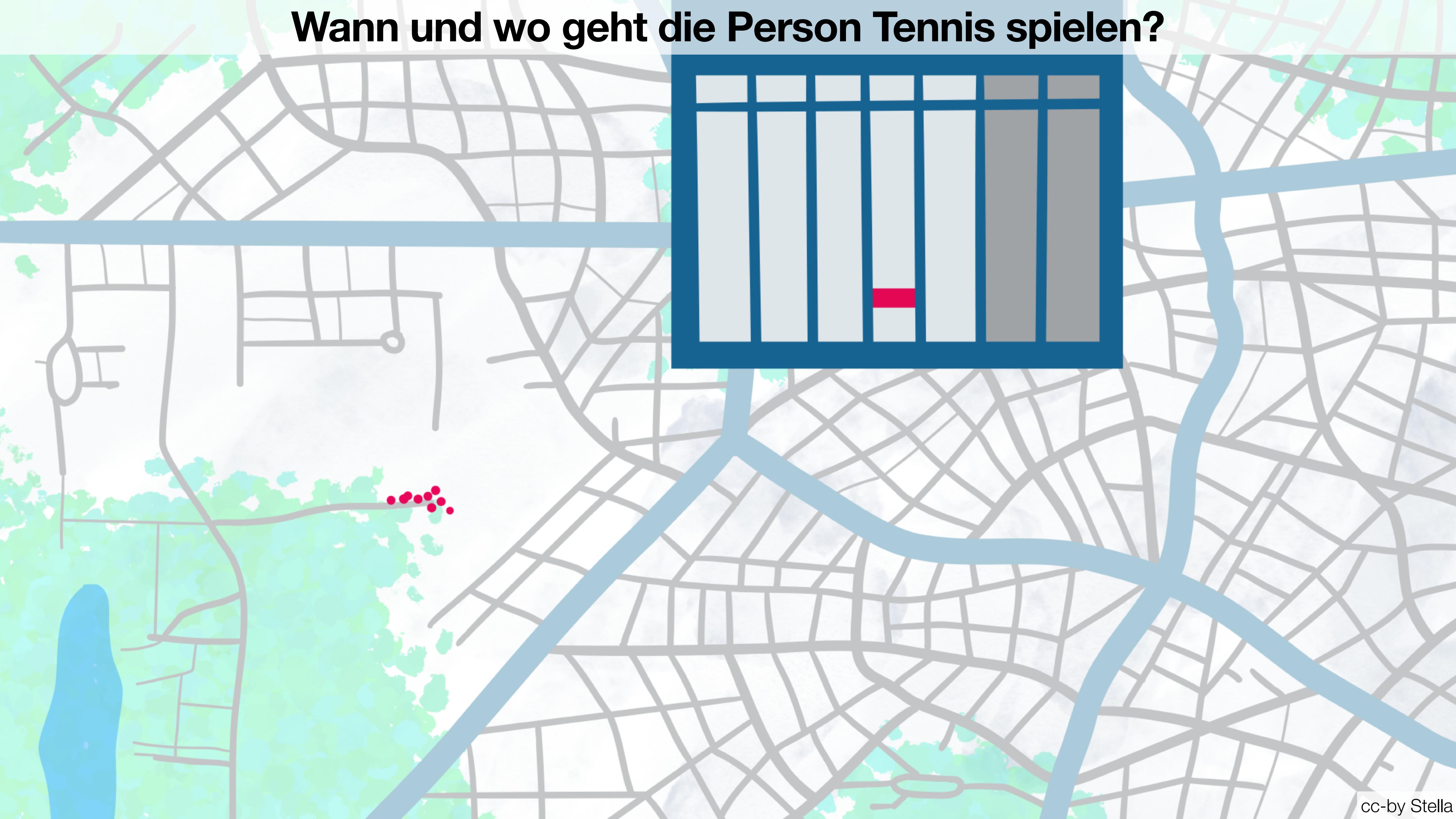
Routen einer Privatperson



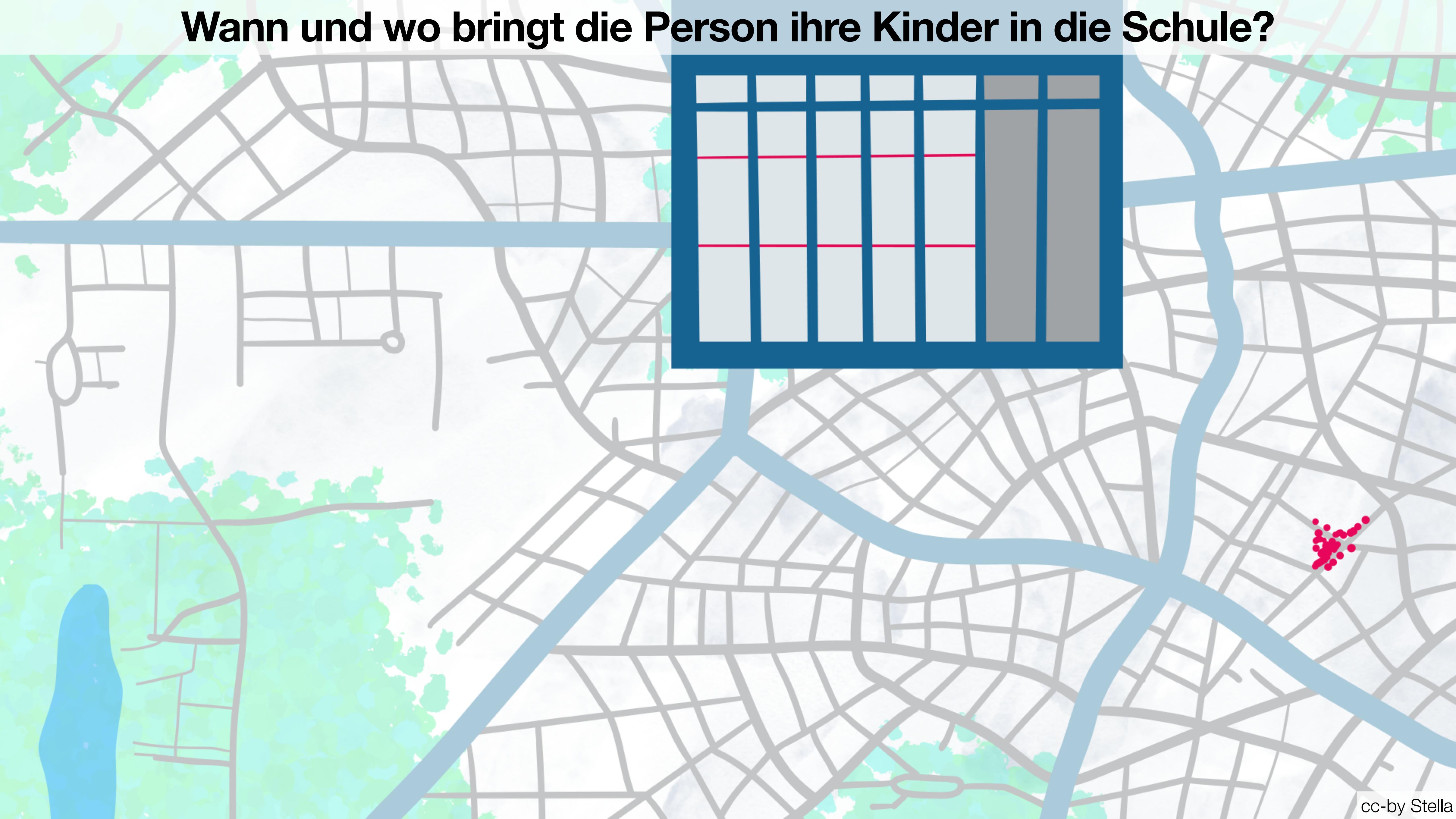
Wann und wo geht die Person einkaufen?



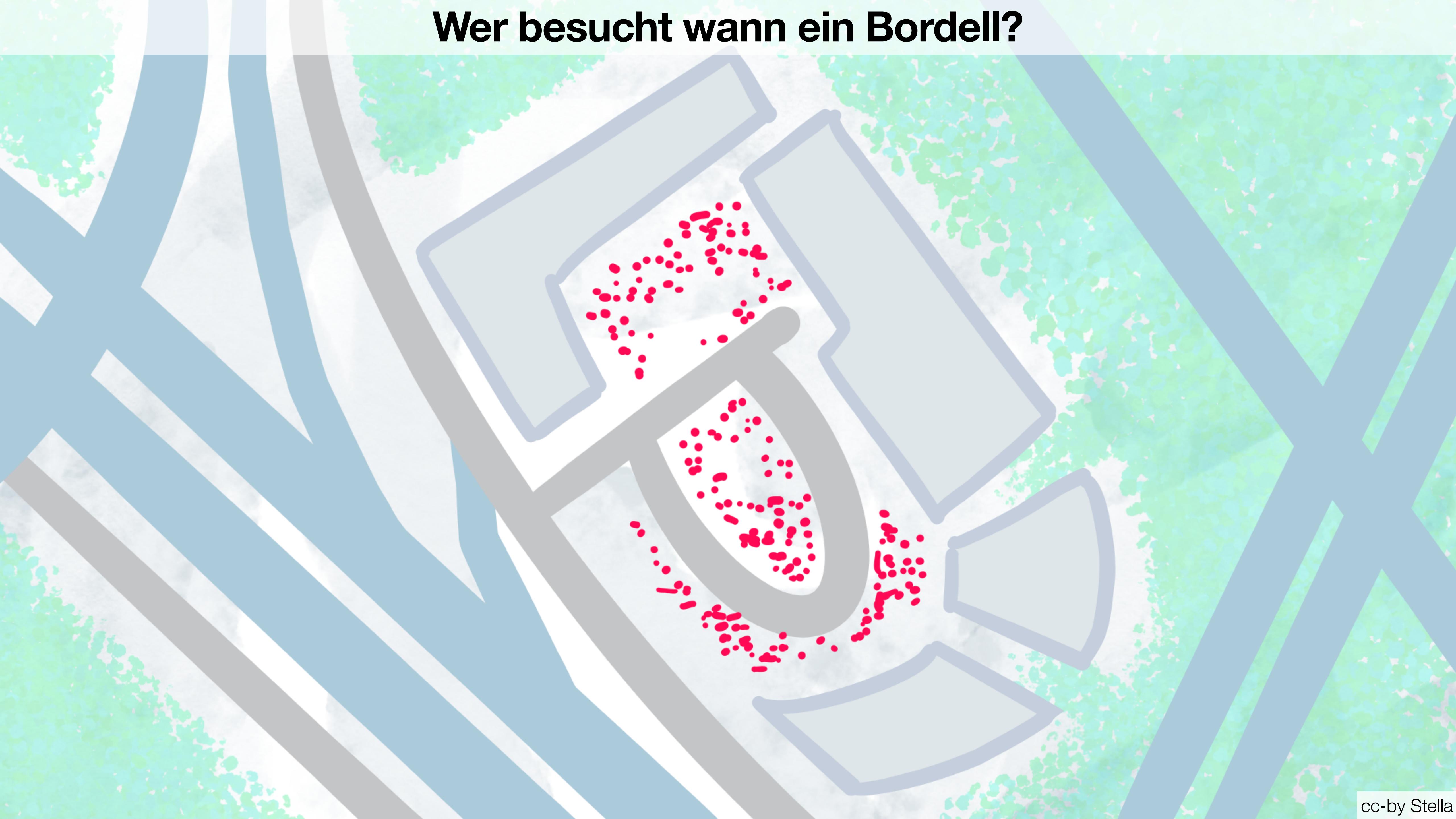
Wann und wo geht die Person Tennis spielen?



Wann und wo bringt die Person ihre Kinder in die Schule?



Wer besucht wann ein Bordell?



Wer arbeitet im Bankenviertel in Frankfurt?



Wer besucht wann eine Redaktion?



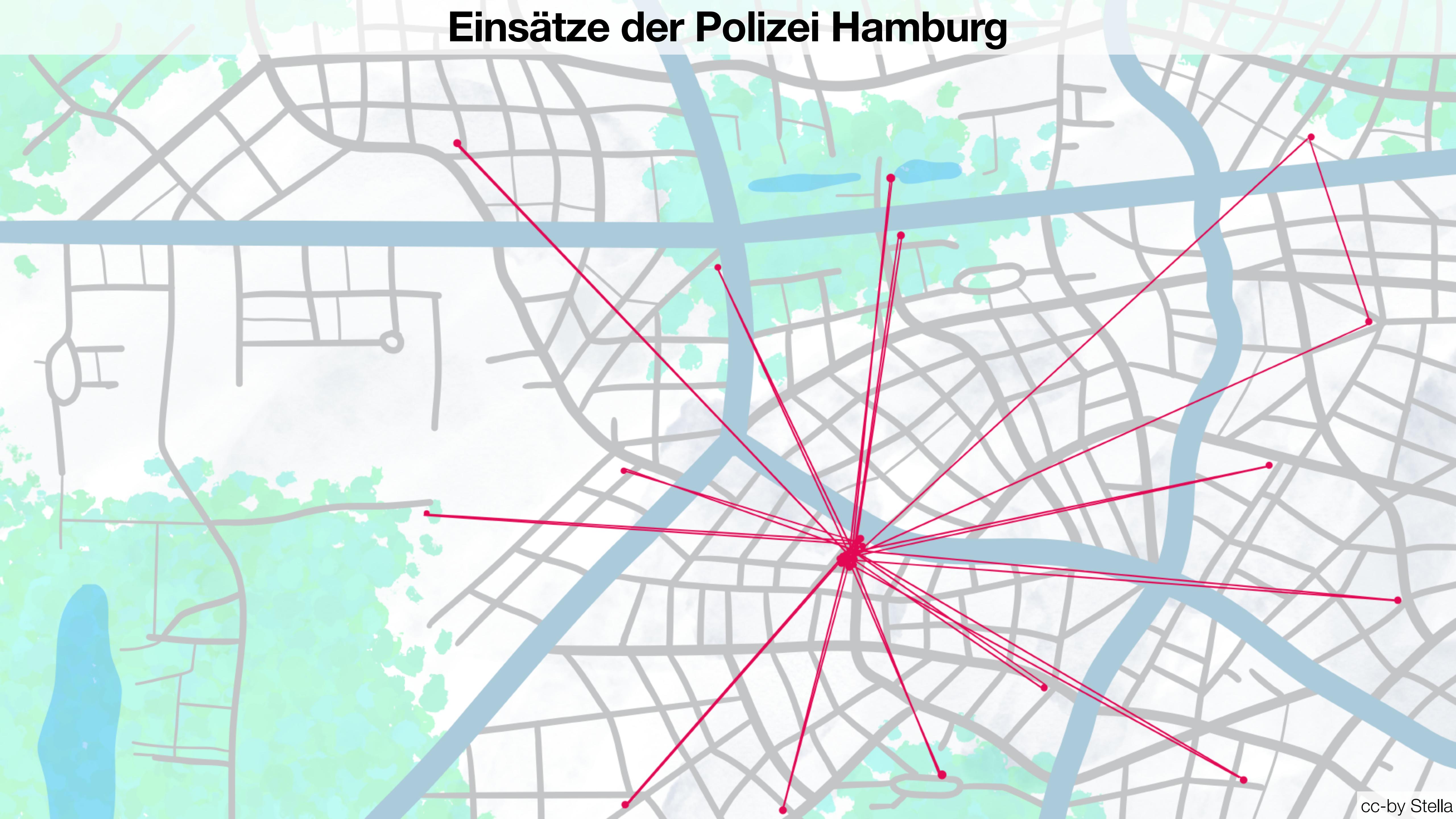
Wer besucht wann eine Botschaft?



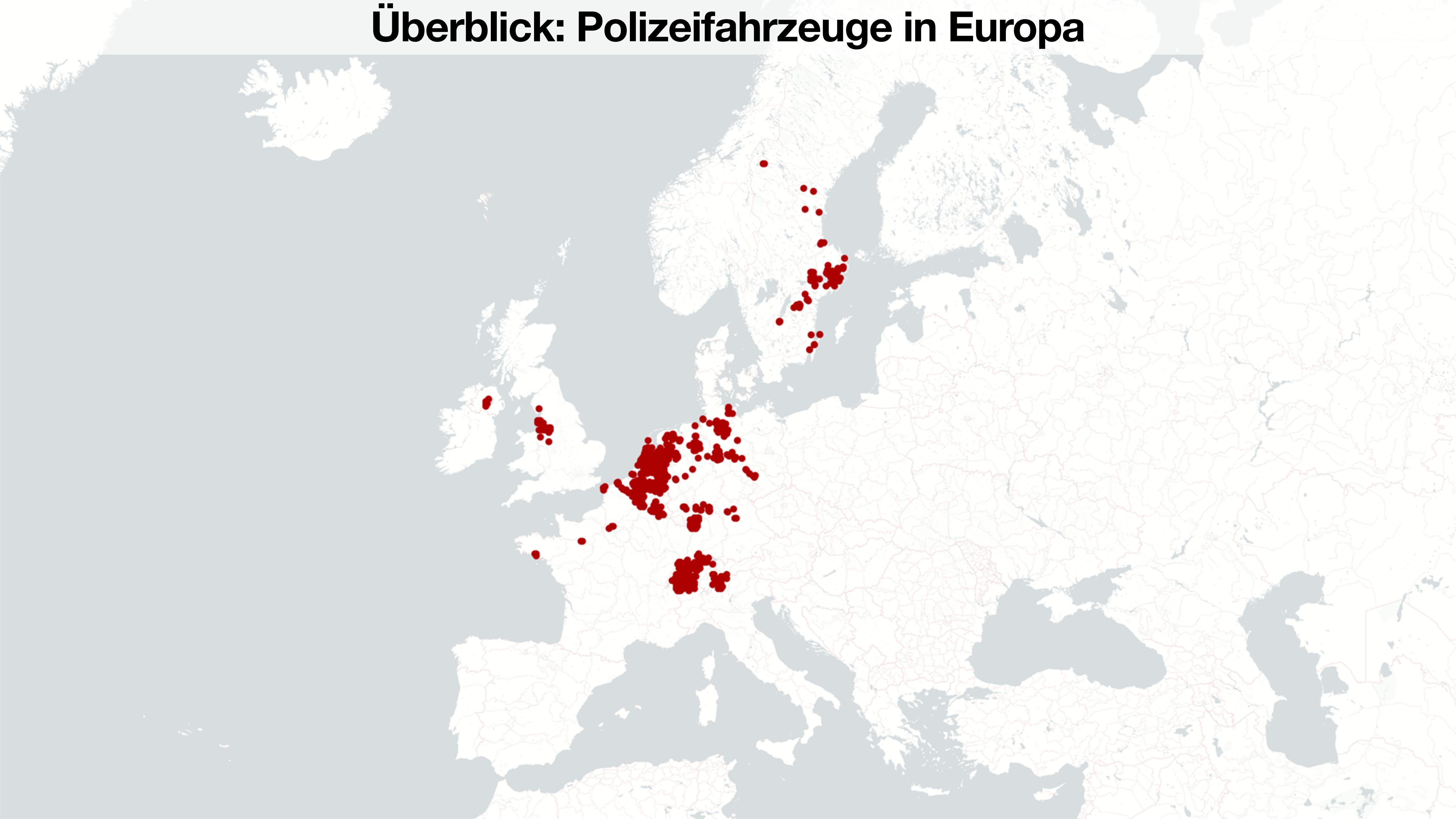
Wer arbeitet beim Bundespräsidenten?



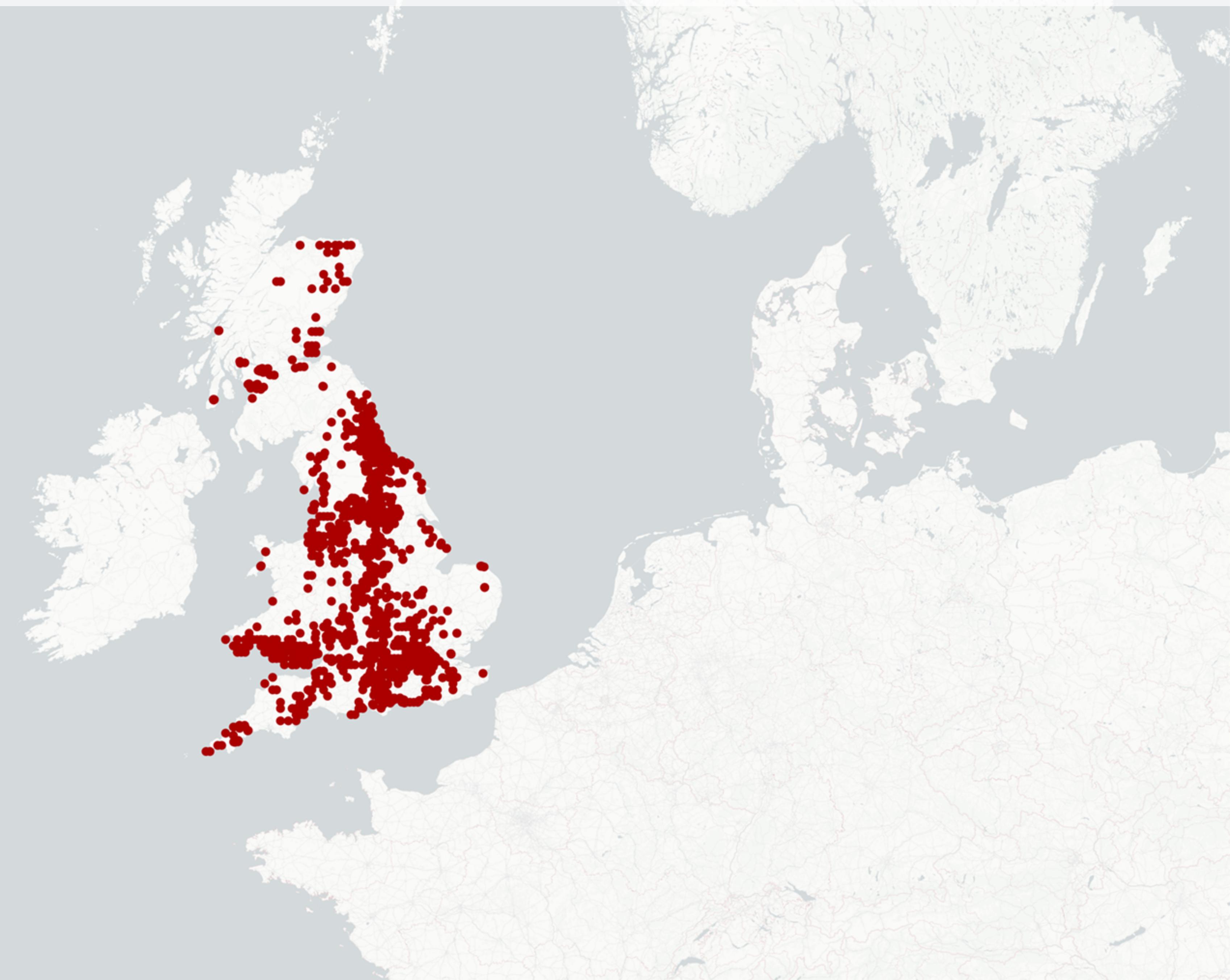
Einsätze der Polizei Hamburg



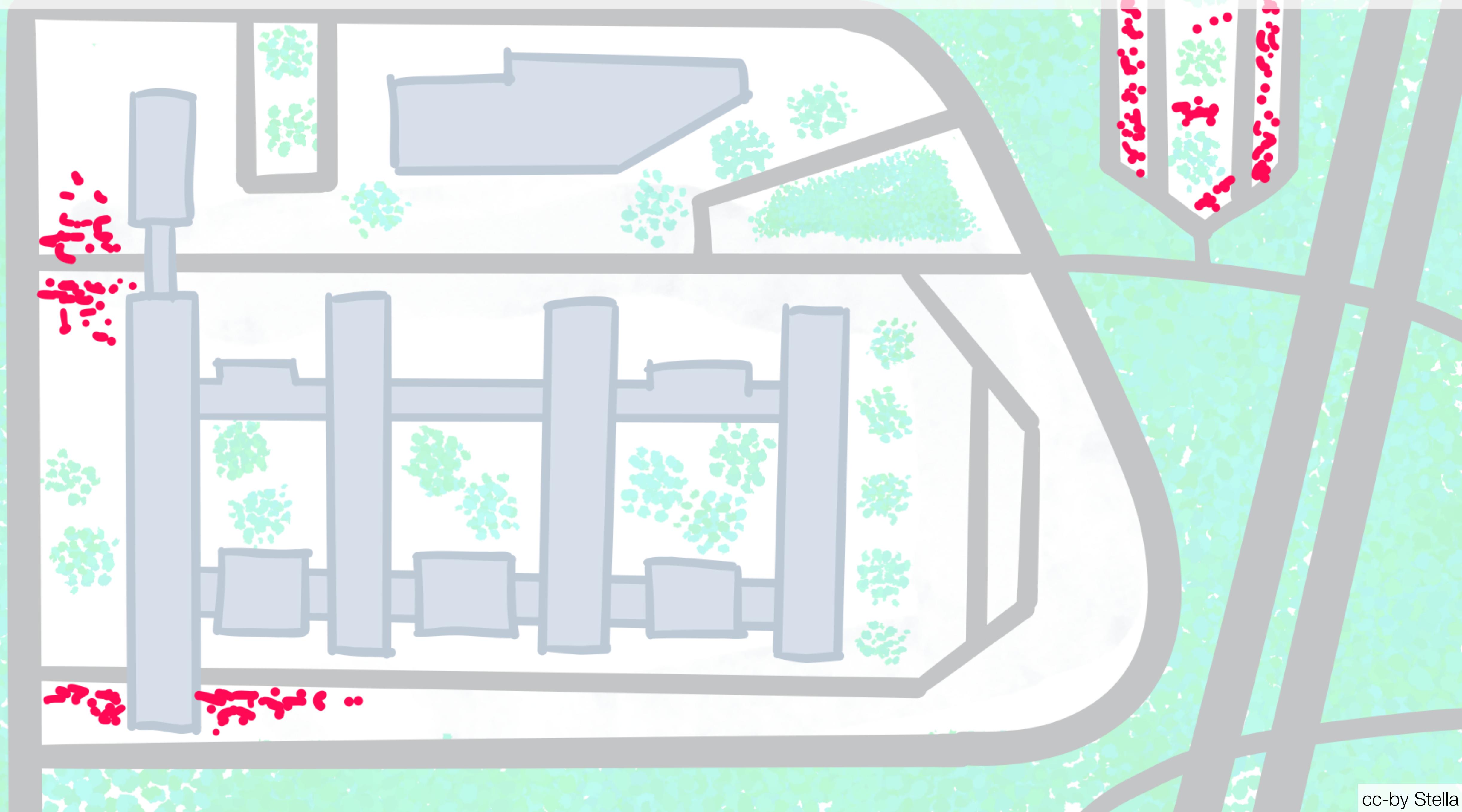
Überblick: Polizeifahrzeuge in Europa



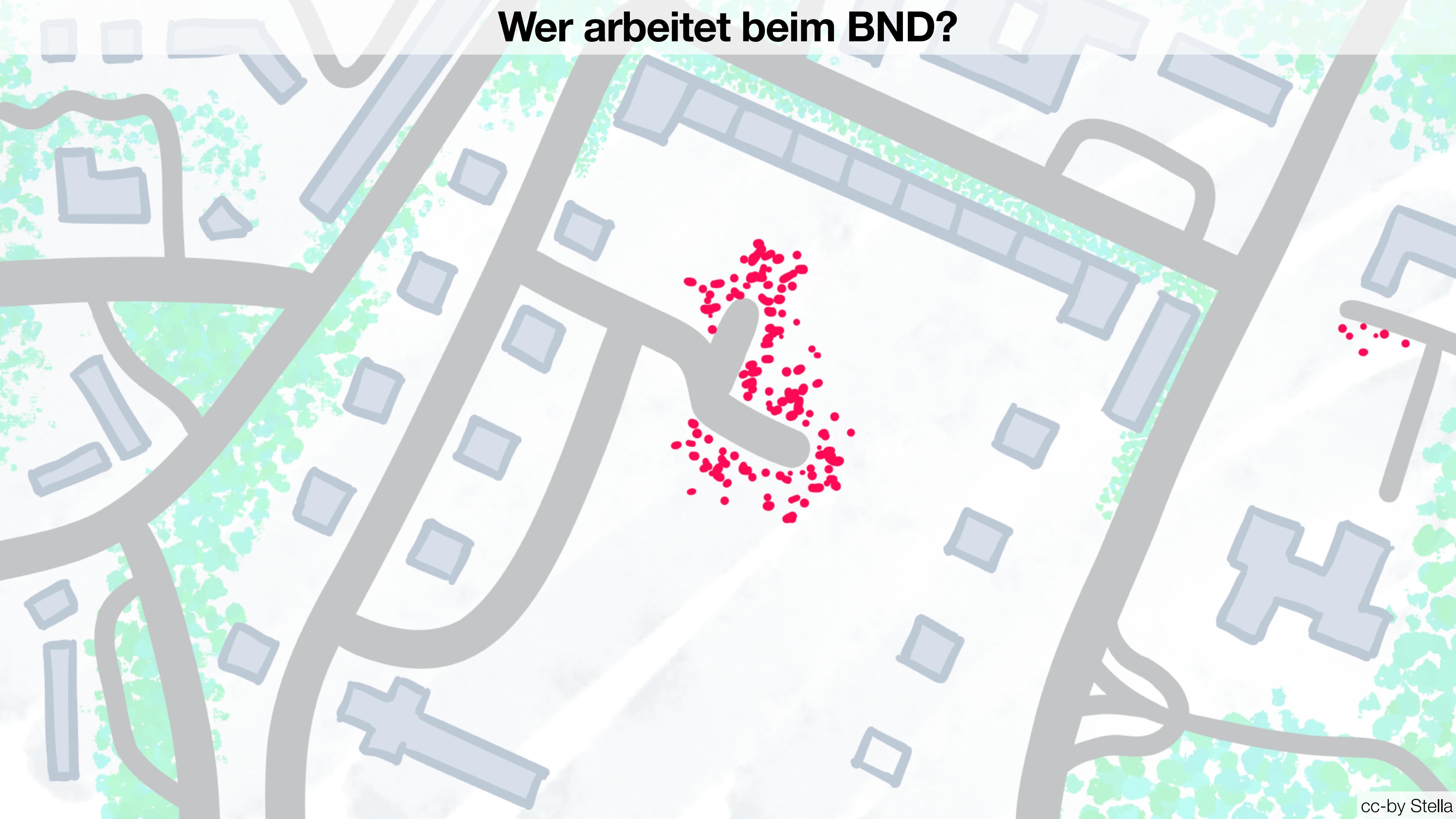
Überblick: Fahrzeuge, die mit einer „gov.uk“ Mailadresse angemeldet sind



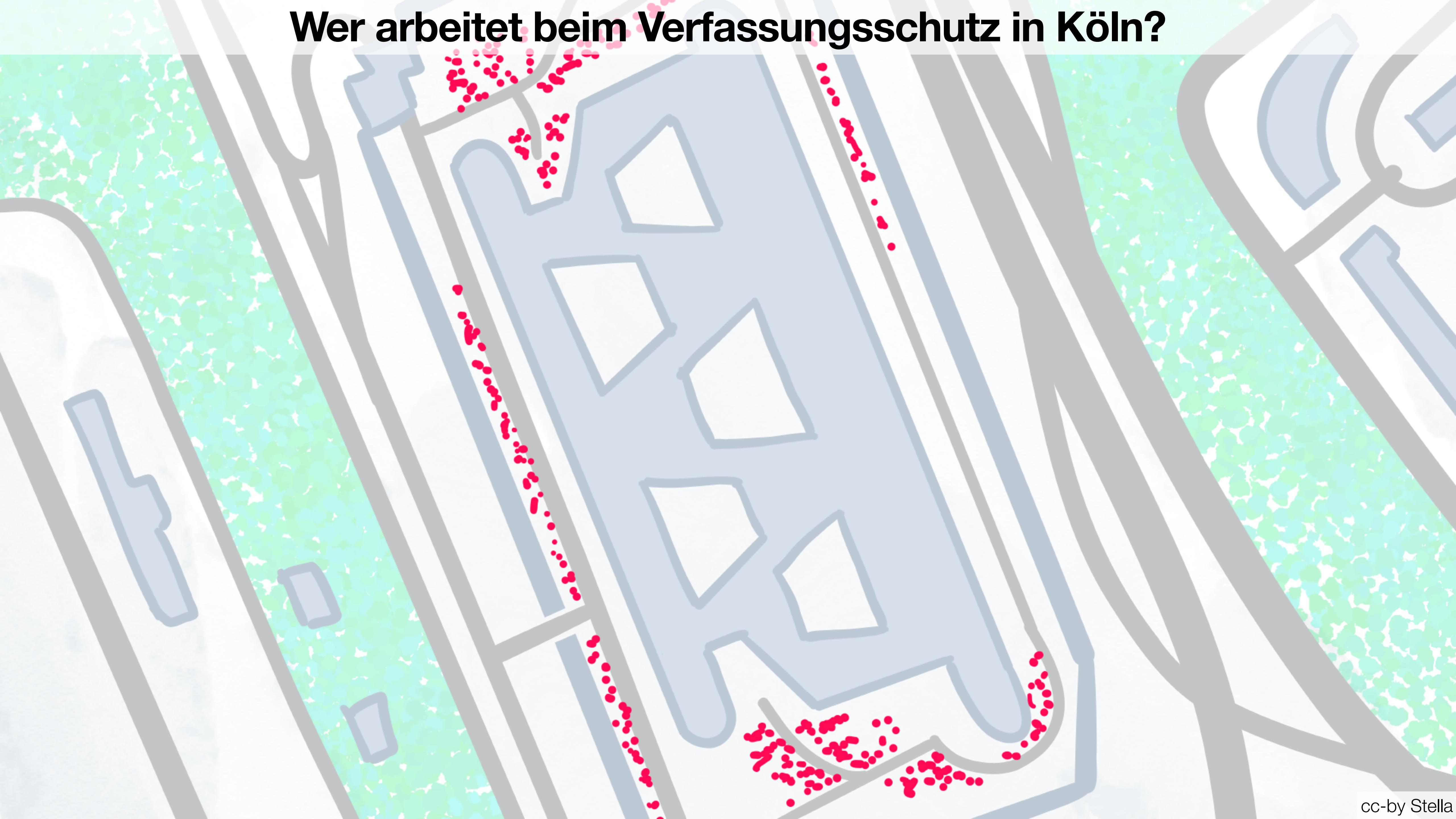
Wer arbeitet beim militärischen Abschirmdienst?



Wer arbeitet beim BND?



Wer arbeitet beim Verfassungsschutz in Köln?



**Wir haben
Volkswagen informiert.**

**Wir haben die
Sicherheitsbehörden informiert.**

**Wir haben alle
uns vorliegenden
Daten gelöscht.**

Wenn Sie nicht mehr wissen, wo Ihr Auto steht.  Ihr Volkswagen weiß es.



Mögliche juristische Konsequenzen für VW?

- VW hat vermutlich gegen eigene AGBs verstoßen.
- Art. 9 DSGVO: „Die Verarbeitung personenbezogener Daten, aus denen die ... **politische Meinungen, religiöse oder weltanschauliche Überzeugungen** oder die **Gewerkschaftszugehörigkeit** hervorgehen, sowie die Verarbeitung von ... **Gesundheitsdaten** oder Daten zum **Sexualleben** oder der **sexuellen Orientierung** einer natürlichen Person ist untersagt.“
- Art. 32 DSGVO: Sicherheit der Verarbeitung „Verschlüsselung personenbezogener Daten“
- Vermutlich wird die ganze EU das Verfahren beobachten.

Volkswagen hat geschlampt

Vergessen, */actuator/heapdump* zu deaktivieren.

Vergessen, Geokoordinaten zu kürzen.

Vergessen, eines der kompromittierten Passwörter zu deaktivieren.

Privacy by Design!

Zum Beispiel alle privaten Daten verschlüsseln!

**Für „Kontrolle“
Vertrauen ist g
gibt es bis zu 2 Jahre
Kontrolle ist besser!
Freiheitsstrafe!**

Der Hackerparagraph bedroht IT-Sicherheit und Presse.

**Niemand* kann etwas gegen
besseren Datenschutz haben.**

- * Auch nicht Sicherheitsbehörden!
- * Auch nicht VW-Vorstände!