

privacy

*Pseudonymisierung
in Theorie & Praxis*

viacryp



*Minimalisiert Risiken bei
Verwendung personenbezogener Daten*

viacryp



Pseudonymisieren

Warum eigentlich und was bieten wir?

ADAM KNOOP

Adam.knoop@viacryp.de

REFERENT: DIPLOM-INFORMATIKER ADAM KNOOP, GESCHÄFTSFÜHRER, VIACRYP

Film: online-banking commercial

Pseudonymisierung

Vom Begriff in der Theorie zur praktischen Anwendung

- Pseudonymisierung - Vorstellung Viacryp
- Beispiele mangelhaften Datenschutzes
- Rechtlicher Rahmen (DSGVO/GDPR)
- Arbeitsweise Viacryp
- Anschauliche Beispiele aus der täglichen Praxis
 - Fallbeispiel: Mobilitätskonzept der Stadt Amsterdam

Über Viacryp

- Viacryp BV ist ein junges und innovatives niederländisches Unternehmen, seit dem 1. Juli 2013 Trusted Third Party (TTP) im Bereich der Pseudonymisierung von persönlichen Daten.
- Wir pseudonymisieren kontrolliert personenbezogene Daten durch Verbesserungstechnologien (Privacy Enhancing Technologies-PET).
- Unsere extern validierten Verfahren bieten die Sicherheit, dass einzelne Kundendaten nicht mehr von den verarbeiteten Daten abgeleitet werden können.
- Wir bieten Hilfestellung beim Schutz der Privatsphäre und gleichzeitiger Ermöglichung umfassender und erfolgreicher Datenanalysen.

Kontrollrahmen & Herkunft Viacryp

- Trusted Third Party (TTP) mit öffentlichen Standardnormen
- Jährliches Prozessaudit von DNV GL
 - Umfang: Verfahren und Bedingungen
- Jährliche technische Prüfung von Madison Gurkha
 - Umfang: Qualität der Software und Verschlüsselung
- Gutachten renommierter Rechtsanwaltskanzlei
 - Pseudonymisierungslösung konform rechtlicher Anforderungen
 - Besonderer Schutz durch technische & organisatorische Maßnahmen
- Abgeleitet von Hot ITem
 - Performance-Steigerung und Master Data Management
 - ISO/IEC 27001 und ISAE 3402 type II zertifiziert

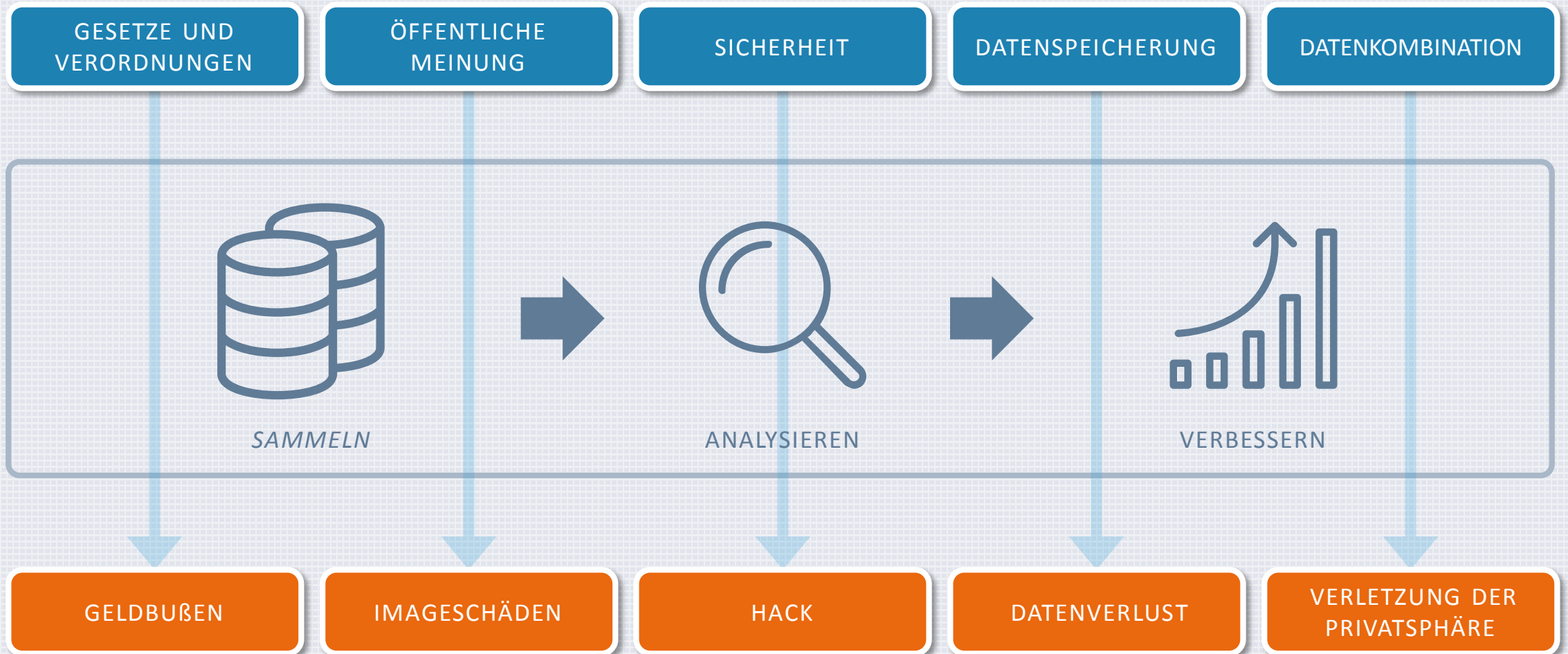


viacryp



Beispiele mangelhaften Datenschutzes

Problematische Verwendung personenbezogener Daten





Zunehmende Cyberattacken und Hackerangriffe

E-MAIL-PASSWÖRTER

RIESEN-DATENDIEBSTAHL

Kriminelle klauen 18 Mio. E-Mail-Passwörter

Es ist der bislang größte Datendiebstahl in Deutschland! Kriminelle haben die Passwörter von 18 Millionen E-Mail-Konten geklaut.

E-MAIL-ADRESSEN



16 MIO. GEHACKT

Wie gefährlich ist der Mega-Datenklau?

Das BSI schlägt Alarm: 16 Millionen Datensätze sind gestohlen wurden, Mailkonten und Passwörter tauchten im Internet auf.

VODAFONE-HACK



FALL VODAFONE

Daten-Klau: So werden Sie nicht zum Opfer

Kriminelle haben die Daten von 2 Mio. Kunden von Vodafone Deutschland gestohlen. Der größte Fall in Deutschland?

Zunehmende Cyberattacken und Hackerangriffe



Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

Yahoo Confirms At Least 500 Million Accounts Were Hacked

by Reuters SEPTEMBER 22, 2016, 2:48 PM EDT



LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords

Das schwächste Glied in der Kette ist meistens der Mensch



Je weniger Orte der Datenspeicherung, desto weniger Menschen die damit arbeiten, desto geringer das Risiko

viacryp



*Pseudonymisierung
&
Rechtliche Aspekte*

Definition des Begriffs Pseudonymisierung

- Nicht zu verwechseln mit dem Begriff Anonymisierung.
- Bei der Pseudonymisierung wird der Name oder ein anderes Identifikationsmerkmal durch ein Pseudonym (zumeist eine mehrstellige Buchstaben- oder Zahlenkombination, auch Code genannt) ersetzt, um die Identitätsfeststellung des Betroffenen auszuschließen oder wesentlich zu erschweren.
- Im Gegensatz zur Anonymisierung bleiben bei der Pseudonymisierung Bezüge verschiedener Datensätze, die auf dieselbe Art pseudonymisiert wurden, erhalten.
- Die Anonymisierung ist das Verändern personenbezogener Daten derart, dass diese Daten nicht mehr einer Person zugeordnet werden können ... aber auch keine aussagefähigen Analysen möglich sind.

Anonymisieren versus Pseudonymisieren

ANONYMISIEREN

*Das **Löschen** von
direkt zu identifizierenden Personendaten*

*“10 Produkte sind
verkauft”*

PSEUDONYMISIEREN

*Das **Ersetzen** von
direkt identifizierbaren Personendaten
durch einen Pseudo-Code*

*“Diese 6 Produkte wurden
von derselben Person
gekauft und die übrigen
von einer anderen Person”*

*Man kann mehr als 90% der Analysefragen ohne
identifizierende Personendaten beantworten.*

Rechtlicher Rahmen *(u.a. GDPR, Datenschutz-Grundverordnung)*

- Grundlage für die Bearbeitung
 - Explizites Opt-in oder ein berechtigtes Interesse
- Daten-Minimierung
 - Nur das Nötigste sammeln
- Grundsatz der Zweckbindung
 - Verarbeitung sollte 'Zweck gebunden' sein
- Verhältnismäßigkeit und Subsidiarität
- Datenschutz durch Design (privacy by design)
 - Geeignete Maßnahmen zur Gefahrenabwehr
 - Nicht länger speichern als notwendig
 - Nachweis aller notwendigen Maßnahmen
- Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme



Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit



AUTORITEIT
PERSOONSgegevens

Die Grundsätze der europäischen Datenschutzverordnung

Nachweis des Datenschutzes der Verantwortlichen

- Die technischen und organisatorischen Maßnahmen müssen den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) entsprechen.
- Die verantwortlichen Parteien verpflichten sich auch dazu, beim Pseudonymisieren von Daten im Verhältnis zum Kostenaufwand die vorhandene Technik maximal zu verwenden.
- Mögliche Maßnahmen:
 - Datenminimalisierung
 - minimalisierte Speicherung von Daten
 - schnellstmögliche Pseudonymisierung
 - Verschlüsselung von Daten
 - Aufnahme von notwendigen Garantien zum Personenschutz

Pseudonymisierung erwähnt in 6 Teilen DSGVO

1. Als Bestandteil von “Datenschutz durch Technikgestaltung”
 - Artikel 25(1)
2. Als Bestandteil der allgemeinen Datenschutzpflichten
 - Auch in Bezug auf Informationspflichten bei einem Datenleck
 - Artikel 32, 33, 34
3. Aufnahme in die veröffentlichten Verhaltensregeln (code of conduct)
 - Artikel 40



Pseudonymisierung erwähnt in 6 Teilen der DSGVO

4. Bestandteil der Prüfung auf Zulässigkeit für sekundäre Benutzung der Ursprungsdaten
 - Artikel 6(4e)
5. Recht auf Einsicht, Berichtigung, Löschung und Daten-Portabilität nicht zutreffend auf pseudonymisierte Daten, sofern Nicht-Herleitbarkeit bewiesen werden kann
 - Artikel 15, 16, 17
6. Anwendbarkeit in Bezug auf die Verarbeitung von Daten für öffentliche Archive, wissenschaftlicher oder historischer Forschungszwecke sowie statistischer Zwecke
 - Artikel 89

viacryp



Arbeitsweise Viacryp



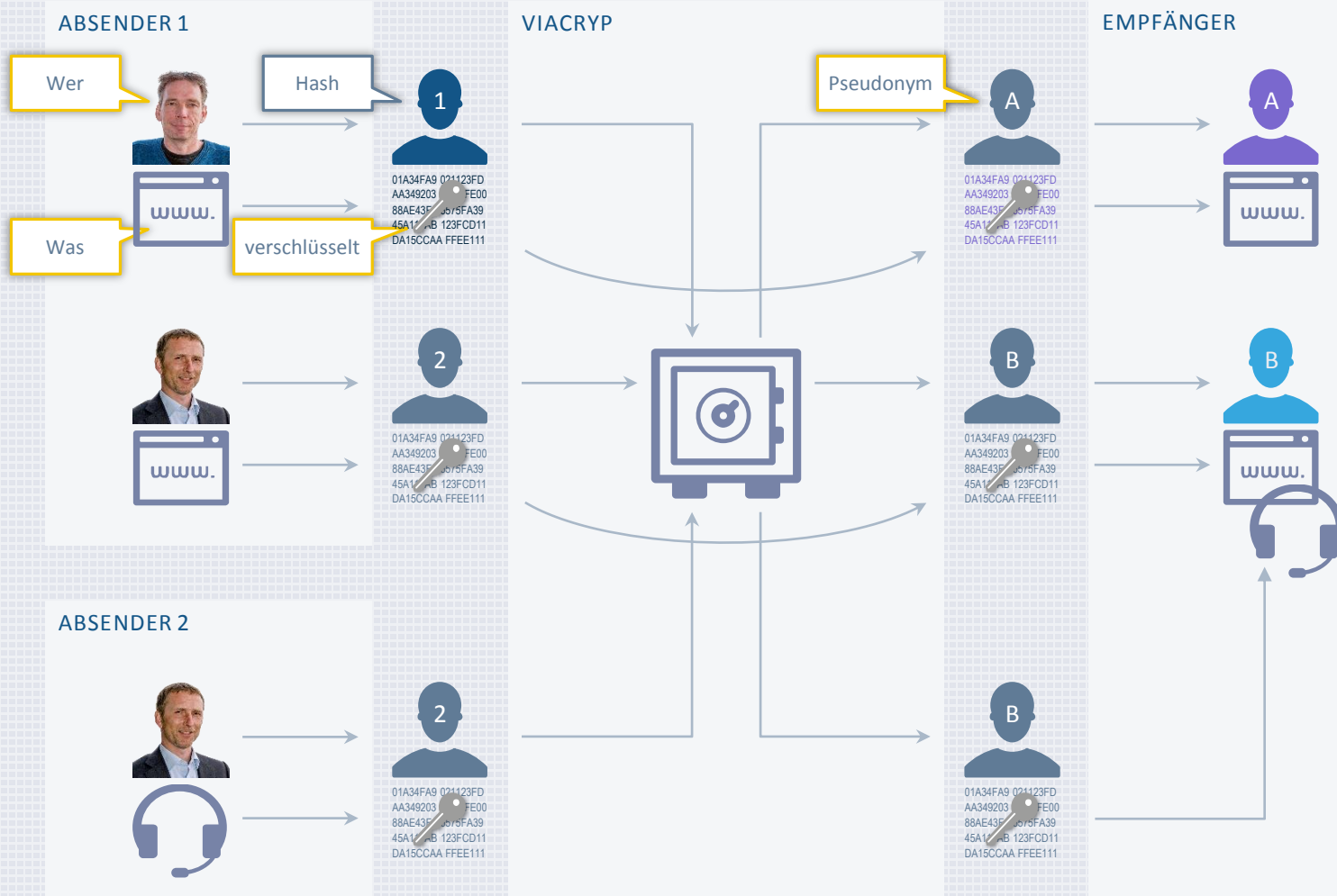
Pseudonymisierungsrichtlinie

- Fachkundige Anwendung der Pseudonymisierung, wobei die erste Verschlüsselung beim Anbieter der Daten erfolgt.
- Es gibt technische und organisatorische Maßnahmen zur Verhinderung der Rückverfolgbarkeit der Verschlüsselung ("Replay-Attack").
- Die verarbeiteten Daten sind nicht indirekt zu ermitteln.
- In einem unabhängigen Gutachten (Audit) wird zu Beginn und am Ende einer jeden Verarbeitung und in regelmäßigen Abständen festgestellt, ob oben genannte Bedingungen erfüllt werden.
- Die Pseudonymisierungslösung wird deutlich in öffentlich zugänglichen Richtlinien beschrieben.



AUTORITEIT
PERSOONSGEGEVENS

Pseudonymisierungsdienst



ERSTE VERSCHLÜSSELUNG
AM BRUNNEN

KEINE LESBAREN DATEN, SONDERN NUR
BEZIEHUNG HASH-PSEUDONYM IM TRESOR

EINZIGARTIGE PSEUDONYME
FÜR DIESEN ANALYSE ZWECK

Sonstige Dienstleistungen

- White-Listing Dienst
 - Filter-Service für den Datenaustausch zwischen Parteien.
 - Use-Cases: Betrugsaufdeckung, basierend auf der Verarbeitung von Opt-ins (Verhältnismäßigkeitsansatz).

- Aggregationsdienst
 - Periodische Verarbeitung, Verbindung und Aggregation von Brunnen.
 - Ausgabe enthält keine Pseudonyme, nur Zählungen.
 - Keine Informationen mehr über ursprüngliche Angaben. Hohes Maß an Anonymität.
 - Use-Cases: Trendanalyse über längere Zeiträume auf Grundlage kombinierter Brunnen.

White-List Dienst (Opt-in Dienst)

WHITELISTER

In regelmäßigen Abständen alle Whitelisted Id's



VIACRYP

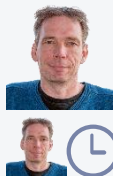
Vollständige Aktualisierung des Tresors



EMPFÄNGER

ABSENDER

In regelmäßigen Abständen alle Daten



```
01A34FA9 024123FD
AA349203 FE00
88AE43F1 6575FA39
45A111AB 123FCD11
DA15CCAA FFE111
```



NICHTS TUN

```
01A34FA9 024123FD
AA349203
CD66FE
88AE43F1 6575FA39
45A111AB
123FCD11
DA15CCAA FFE111
```



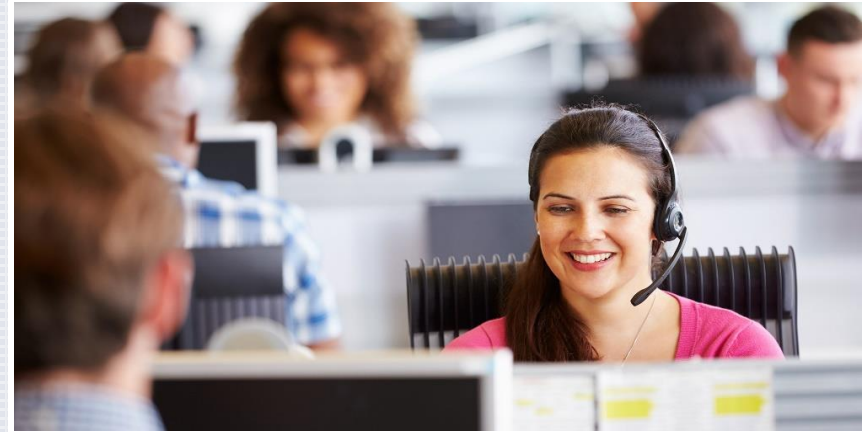
NB: Daten sind nie anonym!



Anwendungsbeispiele



Öffentliche Mobilitätsanalyse



Wirksamkeit Call-center/Webseite



Studie über Käuferverhalten, Crumbbase

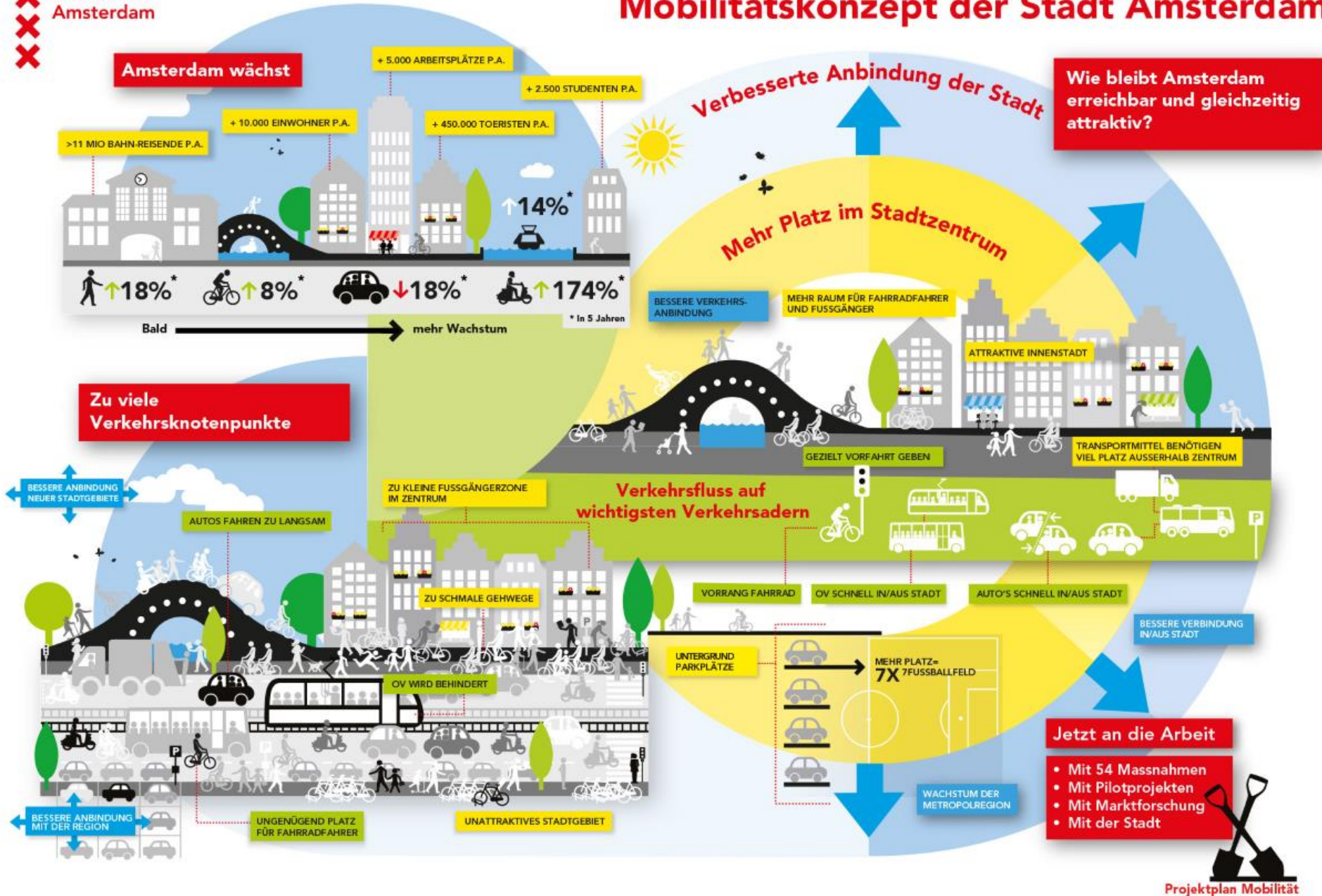


Proportionale Betrugsprävention

viacryp



Fallbeispiel



Herausforderungen der Stadt Amsterdam

- Amsterdam wächst
- Wie bleibt Amsterdam erreichbar und gleichzeitig attraktiv?
- Zu viele Verkehrsknotenpunkte
- Zu viel Verkehr im Stadtzentrum
- Kombination verschiedener Verkehrsmittel ist problematisch

Herausforderungen der Stadt Amsterdam

- Klagende Bürger
 - Unhaltbare Verkehrslage
 - Wunsch nach einer dauerhaften Lösung
 - Waren aber gegen Datenspeicherung

- Kommission für Personen- und Datenschutz
 - Hat die Untersuchung wegen mangelnder Datensicherheit nicht erlaubt



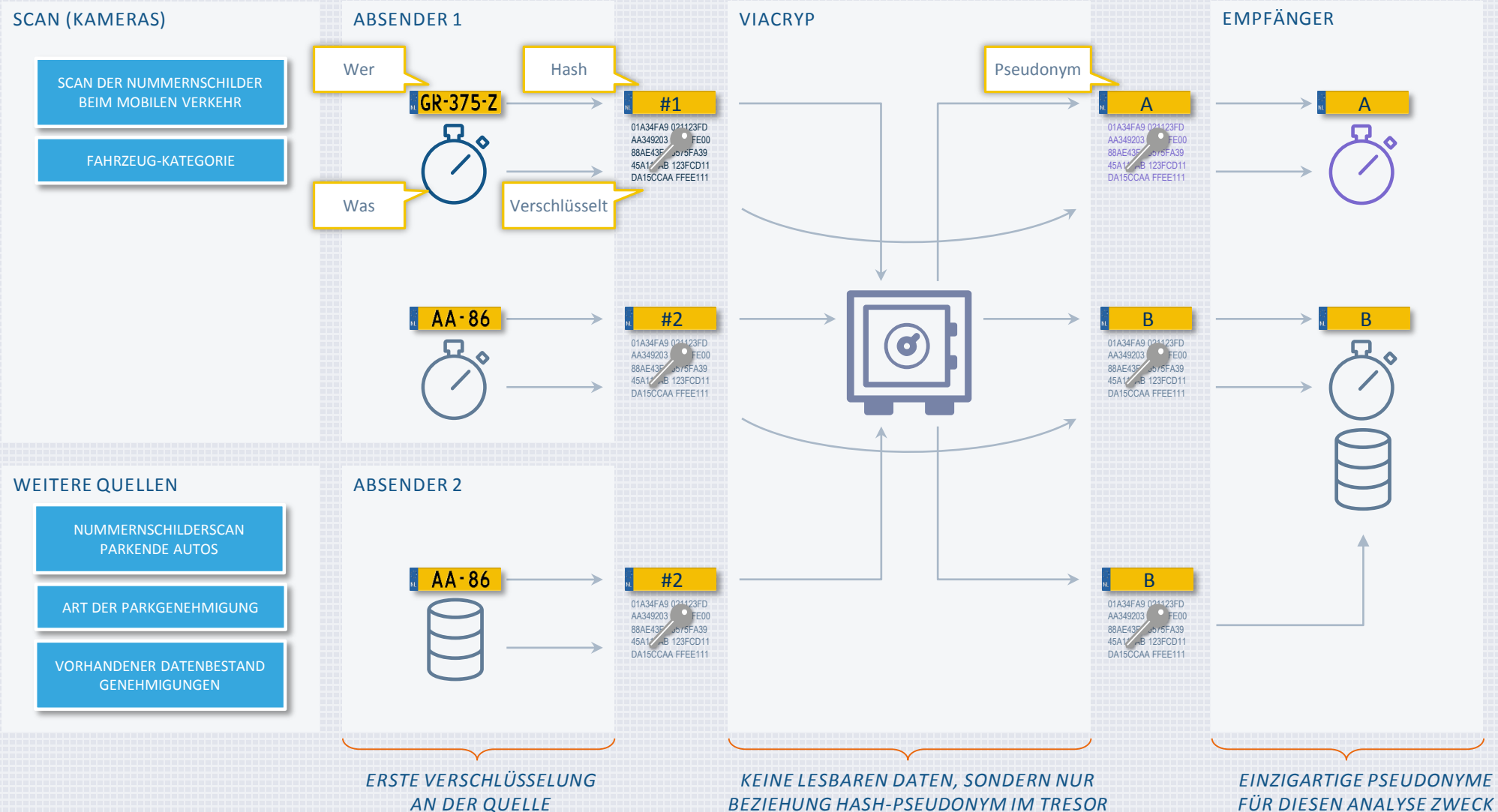


Wie sind wir mit Privacy umgegangen?

- Klagende Bürger
 - Informationsveranstaltungen
- Kommission für Personen- und Datenschutz
 - Pseudonymisierung
 - Klare Kommunikation in der Stadt

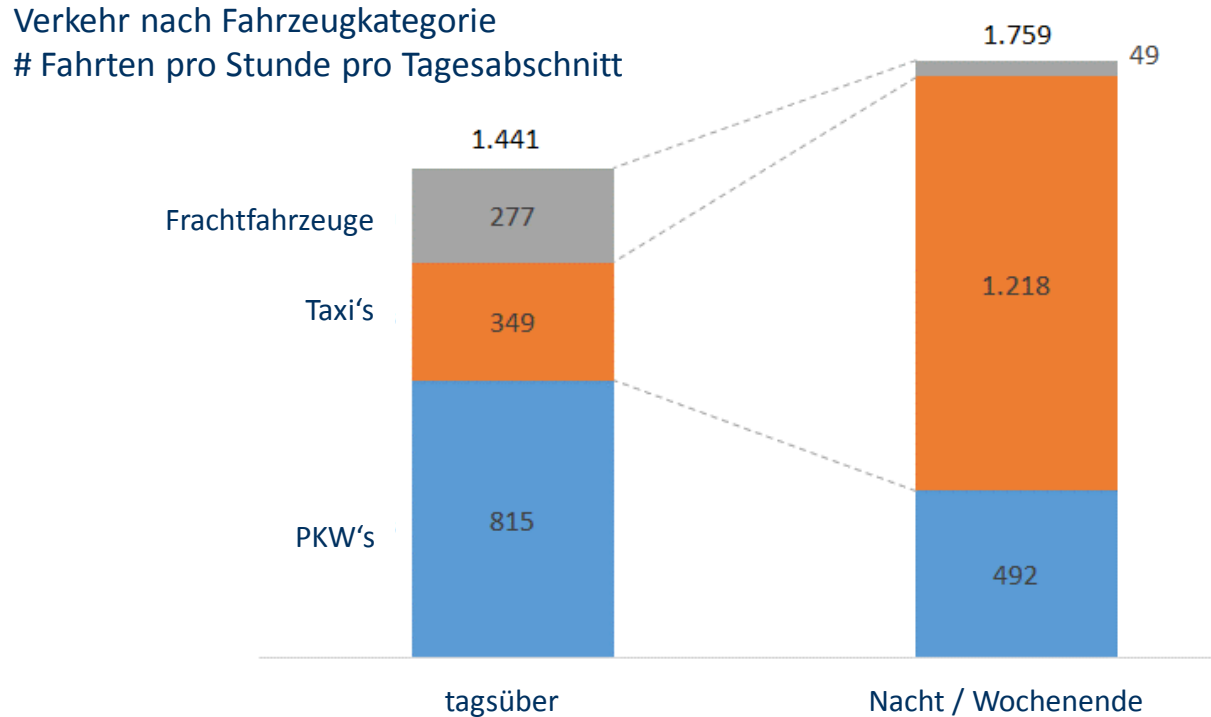


Lösung durch Pseudonymisierung der Verkehrsuntersuchung



Ergebnisse der Fallstudie

Tagsüber besteht mehr als die Hälfte des Verkehrs aus privaten PKWs, nachts dominieren Taxis



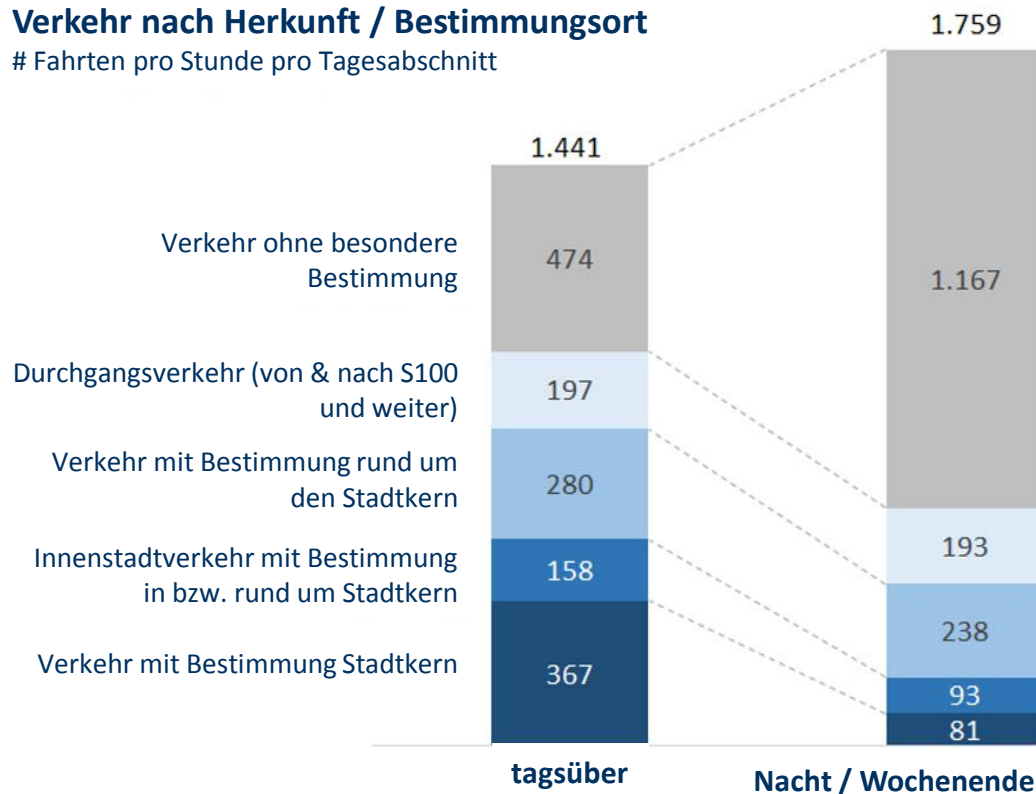
* Bei Aufenthalt im Stadtzentrum werden An- und Abfahrten separat gezählt

Ergebnisse Fallstudie

Nur ein kleiner Teil des städtischen Kernverkehrs ist dort wohnhaft oder Bestimmungsverkehr

Verkehr nach Herkunft / Bestimmungsort

Fahrten pro Stunde pro Tagesabschnitt



Mehrwert des Verkehrs ist diskutabel

Gute Alternativen: Verkehrsführung außerhalb des Stadtkerns

Direkte An- und Abfahrten (Anbindung) zum Hauptnetz vorhanden, manchmal etwas längere Wege

Kürzester Weg deutlich durch den Stadtkern.

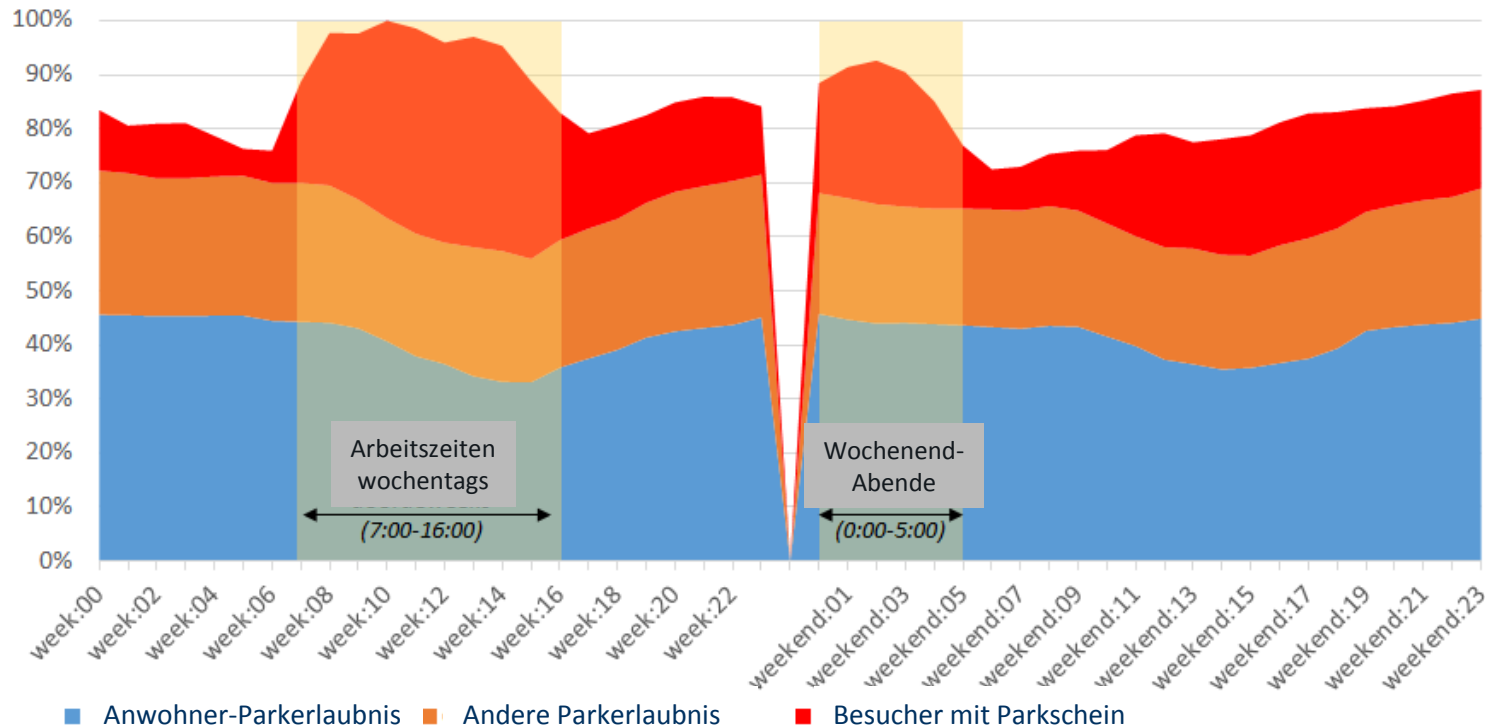
Primäres Ziel ist, das Wege-Netz des Stadtkerns zu entriegeln

Fallstudie bezieht sich auch auf das Parkverhalten

Parkaufkommen von Nicht-Anwohnern sorgt für erhöhtes Verkehrsaufkommen während des Berufsverkehrs und Wochenendabenden

Zusammenstellung geparkter Autos Groenburgwal während der Untersuchs Periode

% Auslastung von Parkplätzen (inkl. nicht öffentlicher Parkplätze, wie z.B. Ladezonen und Parken auf Kennzeichen)



Erfolgsmeldungen in der Presse

Auto wordt ongenode gast in de binnenstad

11-11-15 08:39 uur - Bron: Het Parool



Kop Vijzelstraat afgesloten voor verkeer

Een opstopping op de Gelderse Kade. Onderzoek wijst uit dat veel auto's zinloos door de binnenstad rijden © Floris Lok

Wethouder Pieter Litjens (Verkeer) komt met vergaande maatregelen om doorgaand verkeer uit de binnenstad te weren. Onder meer de kop van de Vijzelstraat wordt vanaf eind 2016 helemaal afgesloten.

De maatregelen zijn het gevolg van een uitgebreid kentekenonderzoek dat in juni is uitgevoerd. Hieruit kwam naar voren dat tweederde van de auto's niets te zoeken heeft in het stadshart. Slechts een kwart van het autoverkeer blijkt de binnenstad zelf als bestemming te hebben.

Het college neemt hiermee een reusachtige stap: de afgelopen jaren is uitentreeuren overleg gevoerd over bijvoorbeeld het afsluiten van slechts één zijde van de Vijzelstraat. Litjens voelt zich door de uitkomsten van het kentekenonderzoek gesterkt om door te pakken en doorgaand verkeer steviger aan te pakken.

Leidsestraat en Nieuwezijds

Naast het afsluiten van de Vijzelstraat wil Litjens ook een 'knip' maken in de Leidsestraat waardoor het onmogelijk wordt deze straat te passeren in oostelijke of westelijke richting. Verder wil hij onnodig verkeer weren van de Nieuwezijds Voorburgwal.

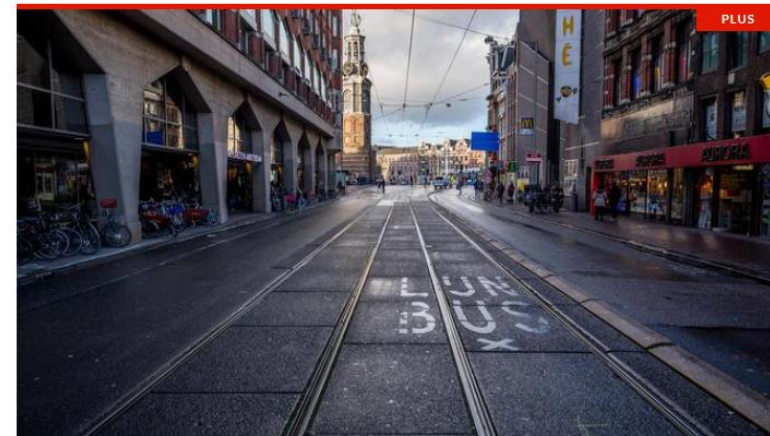
Het Parool

Vrij, Overveerd

DIGITALE KRANT SERVICE

HOME AMSTERDAM STADSGIDS

Even wennen: het verkeer rond de Munt staat niet meer te stinken



Een lege Vijzelstraat © Rink Hof



De fietsster heeft geen idee. Om te beginnen niet dat het voormalige fietspad waar ze over rijdt, tegenwoordig een stoep is. En al helemaal niet dat die keurige man die haar vertelt dat ze hier dus niet mag fietsen, de bedenker van dit alles is: Pieter Litjens,

Zusammenfassung

- Das europäische Datenschutzgesetz verpflichtet, wenn technisch möglich, zur Pseudonymisierung.
- Aktuelle Fälle in der Industrie und beim Staat zeigen, wie hilfreich Pseudonymisieren zur Wahrung von Privacy ist.
- Die Fallstudie der Stadt Amsterdam hat gezeigt, dass Pseudonymisierung sinnvoll ist und Personendaten geschützt werden.
- Viacryp bietet technischen und organisatorischen Maßnahmen zur Pseudonymisierung von Daten als unabhängige Dritte Partei.

Was möchte ich Ihnen mitgeben

- Gesetzgebung zwingt zur Transparenz
 - Fokus sollte beim Kunden bzw. Bürger liegen.
 - Transparente Behörden und Betriebe haben bessere Chancen in der Zukunft. (Vertrauen & Image)!
 - Datenschutz aktiv betreiben!
- Der Wert der Pseudonymisierung (und anderer PETs):
 - Leistungsstarkes Mittel im Gesamtpaket von Sicherheitsmaßnahmen.
 - Je mehr Orte der Datenspeicherung und je mehr Personen involviert, desto größer das Risiko (darum: Vermeiden).
 - Pseudonymisierung ist breit anwendbar.
- **Es muss besser und es kann besser!**

Filmpje viacryp DE zonder ondertitels

viacryp



Fragen?

KONTAKT / INFORMATION

www.Viacryp.de

info@viacryp.com

+31(0)20-5810205

viacryp

