

# Privacy Self-Protection for Connected Cars

Harald Zwingelberg

ULD

at the meeting of the International Working  
Group on Data Protection in  
Telecommunications

Berlin, 22 November 2017

Partly based on research results of the projects:



Unabhängiges Landeszentrum für  
Datenschutz Schleswig-Holstein

## *Overview*

- challenges of connected cars identified
- methodology used
- requirements derived

***Data protection is about ~~data~~***



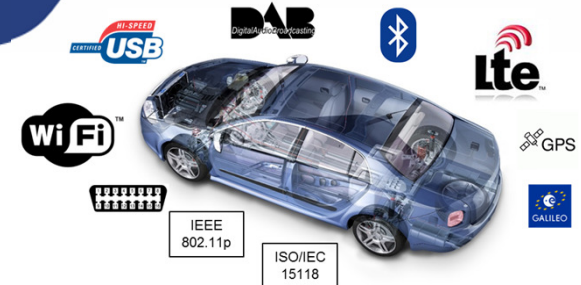
Foto: Ashtyn Renee

***people  
and their  
fundamental  
rights***

To be checked while  
developing technologies  
for connected cars

- impact on persons
- impact on society

# Motivation for the project work



- Connected cars allow a series of new **possible applications**, e.g.:
  - assistance systems (from finding parking spots to self driving car)
  - infotainment (optimizing routes, finding POI)
  - value added services (booking of charging stations along route)  
=> this may be a enabler for e-mobility!
  - business models (e.g. car insurances as "pay how you drive")
  - services by car manufacturers (ongoing quality assurance)

## Challenges

- **data** involved are often personal data or allow for indirect identification of persons
- profiles on movements and interests
- profiles about driving habits
- ...



By Maryland Pride (Own work) [CC BY-SA 3.0  
(<http://creativecommons.org/licenses/by-sa/3.0>) or GFDL  
(<http://www.gnu.org/copyleft/fdl.html>)], via Wikimedia Commons

Slide initially by Christoph Krauß (SeDaFa project)

# Challenges to Data Protection – collection and interpretation of data 1

## Car:

- communication centre with network connection
- ... using identifier (e.g. MAC address)
- ... collecting broad set of data  
(> 10 GB / h, e.g. sensors)
- ... leaving many data traces (e.g. location data)
- ... combined with further technology (e-Call, navigation unit, infotainment system)



<http://www.mac-address.info/BMW+AG>



DANA 1/2015



<https://pixabay.com/>

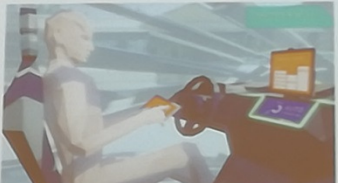



# Challenges to Data Protection – collection and interpretation of data 2

**Motivation**

- Demografischer Wandel:
- Individuelle Einschränkungen:
- Assistenzsysteme / HAF
- Bedienung:
- Sicherheit:

Mobilität erhalten  
Mobilität ermöglichen  
Mobilität unterstützen  
Mobilität erleichtern  
Mobilität sichern

Die Autos werden sich in Zukunft den Insassen anpassen. Dafür müssen wir die Insassen kennen und verstehen.

InCarIn

Source: InCarIn

02.08.2016 | Fahrerassistenz | Nachricht | Onlineartikel

Projekt InCarIn arbeitet an kamerabasierter Auto-Innenraum

- Camera observation inside the car itself used for
- observing drivers and passengers
  - Identification of persons
  - identification of items held or used
  - identification of passengers' actions



...um die Insassen im Auto beschäftigen. Wichtig ist dies etwa beim automatisierten Fahren. © Fraunhofer IAO

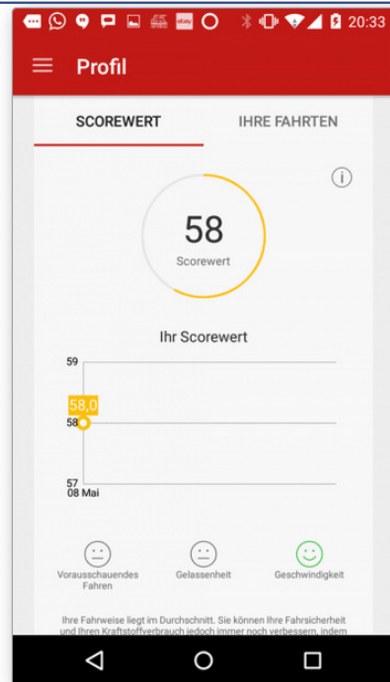
<https://www.springerprofessional.de/fahrerassistenz/interieur/projekt-incarin-arbeitet-an-kamerabasierter-personenerfassung-fu/10551520>

# Challenges to Data Protection – collection and processing of data

Um volle Datensicherheit und -schutz zu gewährleisten, sind persönliche Angaben und Vertragsinformationen von den Fahrdaten getrennt. Die Generali Mobility-App wird von dem externen Dienstleister MyDrive Solutions zur Verfügung gestellt, der Teil der internationalen Generali Gruppe ist. MyDrive Solutions kennt vom Kunden lediglich die Telematik-ID, welche keinen Rückschluss auf Personen- oder Vertragsdaten zulässt. MyDrive übermittelt an das Versicherungsunternehmen nur die Information, ob sich der Kunde mit seinen Zugangsdaten in der App angemeldet hat, den Scorewert, die Anzahl der Fahrten und die gefahrenen Kilometer sowie das Datum der letzten Aufzeichnung einer Fahrt. Das Versicherungsunternehmen kann daher kein Bewegungsprofil vom Kunden oder dem Fahrzeug erstellen.

## Fahrstil verbessern

Die App erfasst aber nicht nur die gefahrenen Kilometer, Fahrten und den Scorewert, sie gibt dem Fahrer auch nach jeder Fahrt in Form von Smilies ein individuelles Feedback zu den Punkten „Vorausschauendes Fahren“, „Gelassenheit“ und „Geschwindigkeit“. Diese Rückmeldung soll ihm dabei helfen, seinen Fahrstil zu verbessern und damit das Unfallrisiko weiter zu verringern. Um die Nutzung der App für den Kunden so einfach wie möglich zu gestalten, ist diese mit einer Autostart-Funktion ausgestattet, die selbstverständlich auch ausgeschaltet werden kann. Die Aufnahme startet sobald eine Mindestgeschwindigkeit von 30 km/h erreicht ist und wird automatisch gestoppt, wenn das Fahrzeug 10 Minuten lang nicht bewegt wird.



Quelle: Generali

PAYD – Pay as you drive

PHYD – Pay how you drive

First minor step done:  
Separating the storage  
of information on driving  
behaviour (ext. service  
provider) and customer /  
contract data (insurance  
company).

Philipp Benkler: PAYD: Generali testet Mobility-App in der Praxis – Bessere Smartphone-Software mithilfe der Crowd  
<http://www.it-finanzmagazin.de/payd-generali-testet-mobility-app-in-der-praxis-bessere-software-mithilfe-der-crowd-37262/> (26.09.2016)

# Challenges to Data Protection – authorities’ desires

Donnerstag, 13. Oktober 2016, 16.36 Uhr

**Automobilwoche**  
DER BRANCHEN- UND WIRTSCHAFTSZEITUNG

## Vernetzung: China will E-Autos überwachen

**Künftig sollen alle Elektroautos in China die Regierung über jede ihrer Bewegungen informieren. Gerade die deutschen Hersteller stürzt diese Vorgabe in ein schwieriges Dilemma.**

Von Stefan Wimmelbücker

**Peking.** China will Elektroautos permanent überwachen. Wie das "Handelsblatt" berichtet, arbeitet die Regierung an einem Plan, der vorsieht, dass die Bordcomputer den Standort des Fahrzeugs einmal pro Sekunde an die Behörden meldet. In einem 35 Seiten langen Entwurf erklärt die Behörde detailliert, welche Informationen sie in welchem Format von den Hersteller geliefert bekommen will. Dabei geht es nicht nur um allgemeine Daten über Batterien, Motor oder Standort, sondern die Chinesen verlangen auch individuelle Daten wie Gerätenummern und im Auto eingelegte SIM-Karten. Damit können die Daten bestimmten Personen zugeordnet werden, die Regierung wüsste also jederzeit, wo sich welcher Autofahrer gerade aufhält, wie schnell er fährt oder wo er sein Auto wie lange geparkt hat.



Elektroauto von Brilliance auf der Peking Motor Show. (Foto: Thomas Geiger)

Für deutsche Datenschützer ist eine lückenlose Überwachung, wie sie jetzt in China geplant ist, ein Alptraum. Die deutschen Hersteller befinden sich durch die chinesischen Pläne in einer schwierigen Situation: Aus Rücksicht auf den in Deutschland sehr wichtigen Datenschutz haben sie den Schutz der Privatsphäre ihrer Kunden zu einem ihrer Markenzeichen erklärt. Aus diesem Grund gibt es auch immer wieder Schwierigkeiten bei der Zusammenarbeit mit Internetkonzernen wie Google und Apple, bei denen das Sammeln von Daten zum Geschäftsmodell gehört.

<http://www.automobilwoche.de/article/20161013/NACHRICHTEN/161019944/1276/vernetzung-china-will-e-autos-ueberwachen>

According to the press  
China has plans that  
e-cars must share data  
every second including  
current location and  
identifiers allowing the  
identification and  
tracking of cars and  
persons.



# *Challenges to Data Protection – businesses’ desires*

17. November 2016, 07:27 Uhr Digitale Infrastruktur

## **Dobrindt will Zugriff auf Daten erleichtern**



<http://www.sueddeutsche.de/wirtschaft/digitale-infrastruktur-dobrindt-will-zugriff-auf-daten-erleichtern-1.3252303>

German minister for transport and infrastructure asking for brining individual rights and data protection in line with the value chain of the economy.

Anonymisation and pseudonymisation seen as business enabler

***Research papers  
related to tracking***

## Tracking- und identification possibilities:

- location data not anonymous

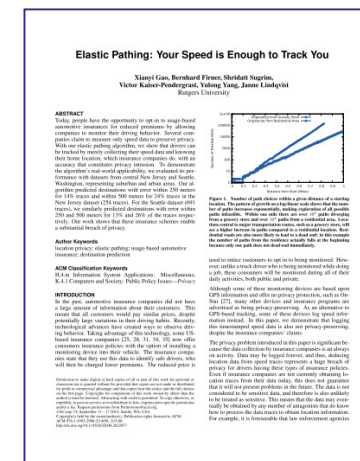
Zang, Bolot: Anonymization of Location Data Does Not Work:  
A Large-Scale Measurement Study, MobiCom 2011

- inferring trip dentitions from driving habits

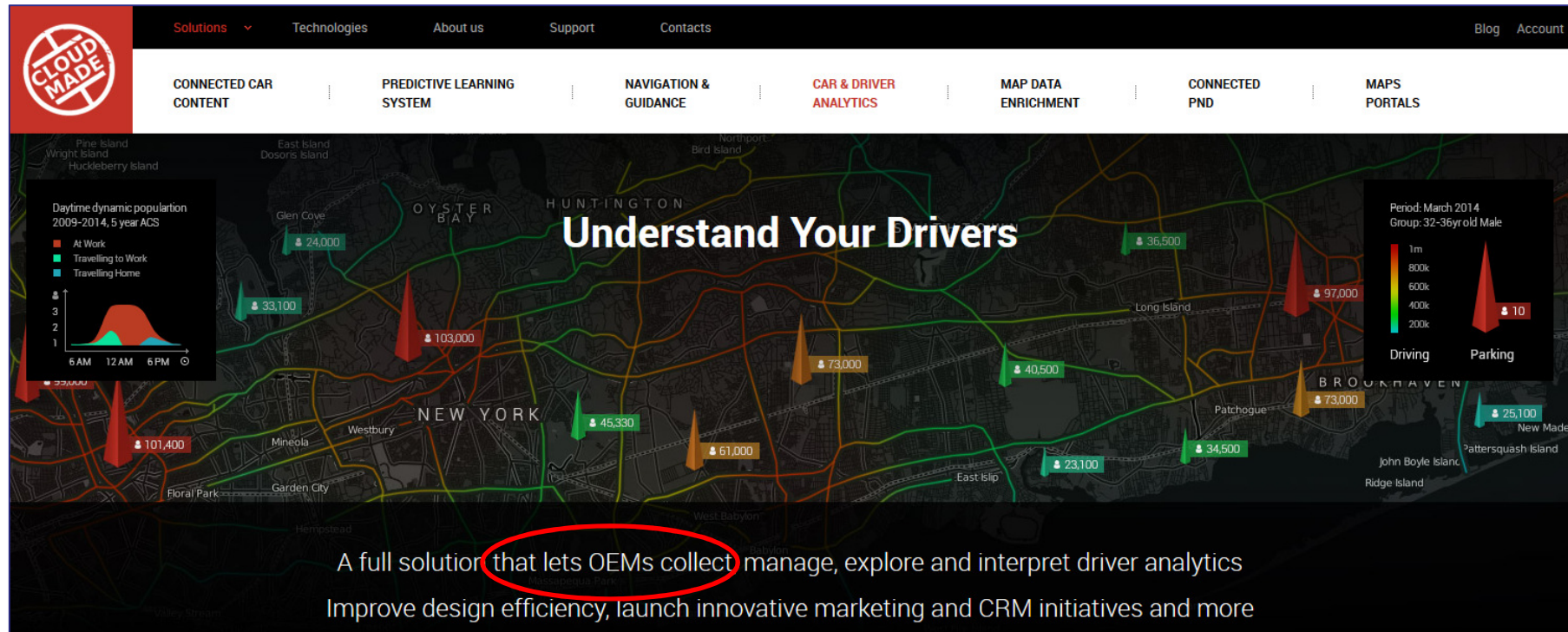
Dewri et al.: Inferring Trip Destinations  
from Driving Habits Data, WPES 2013

- tracking by knowing one location and speed across route

Gao et al.: Elastic Pathing: Your Speed is Enough to Track You, UbiComp 2014



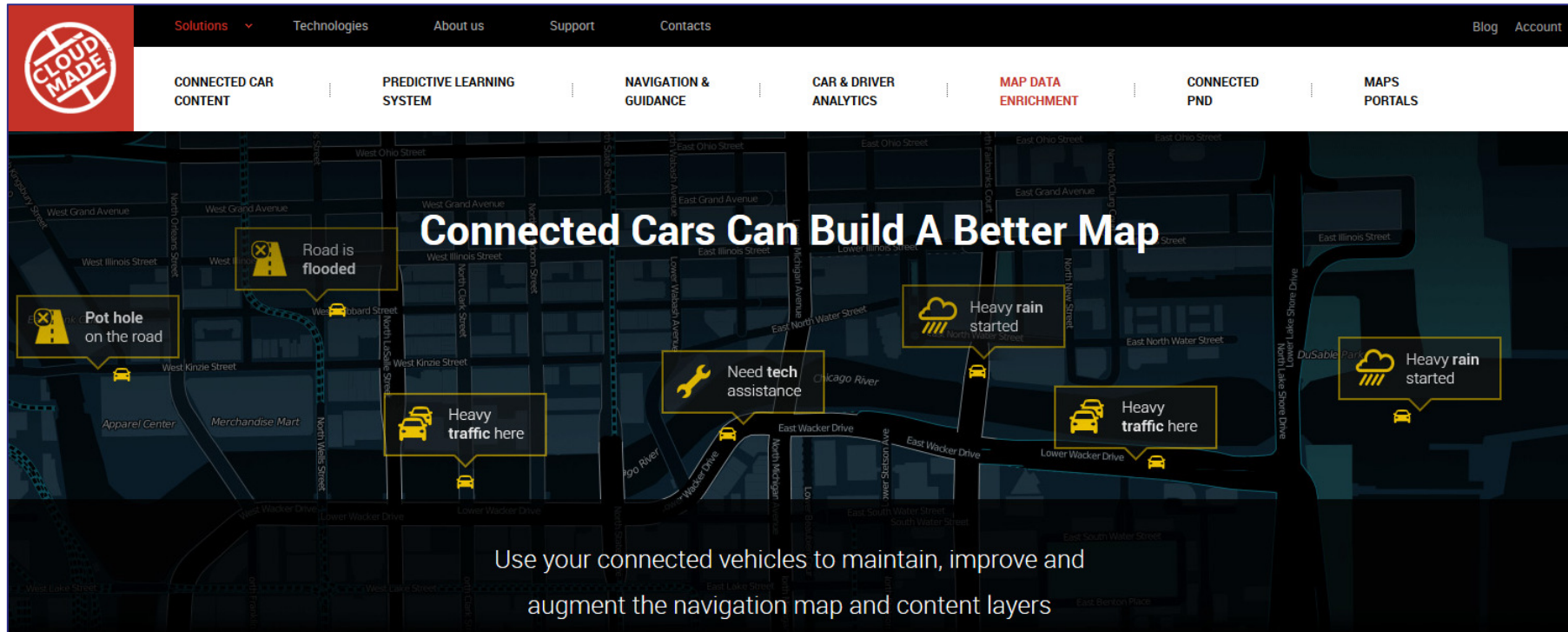
# Driver Analytics



<http://cloudmade.com/solutions/car-driver-analytics>



# *Driver Analytics und Big Data*



The screenshot shows the CloudMade website interface. The top navigation bar includes links for Solutions, Technologies, About us, Support, and Contacts. Below this, a secondary navigation bar lists various services: CONNECTED CAR CONTENT, PREDICTIVE LEARNING SYSTEM, NAVIGATION & GUIDANCE, CAR & DRIVER ANALYTICS, MAP DATA ENRICHMENT (highlighted in red), CONNECTED PND, and MAPS PORTALS. The main content area features a dark-themed map of a city grid. Overlaid on the map are several yellow callout boxes with icons and text: 'Pot hole on the road' (with a car icon), 'Road is flooded' (with a water icon), 'Heavy traffic here' (with a car icon), 'Need tech assistance' (with a wrench icon), 'Heavy rain started' (with a cloud and rain icon), and another 'Heavy rain started' (with a cloud and rain icon). The text 'Connected Cars Can Build A Better Map' is prominently displayed in the center of the map. Below the map, the text reads: 'Use your connected vehicles to maintain, improve and augment the navigation map and content layers'.


<http://cloudmade.com/solutions/map-data-enrichment>






## ***Personal Navigation Devices Social Graph included***

**Connected PNDs Without The Costs**

2.5 mi to "Shell" \$3.15 

800m to a quiet rest stop 

150m to "Cup" 8 friends liked 

Weather at Destination  
Clear Skies, 64°F

Traffic delay  
in 5 miles

**Re-Route**

Deliver rich content from global providers using WiFi or Bluetooth connections

Add advanced features like predictive destinations, customized search and analytics

<http://cloudmade.com/solutions/connected-pnd>

## Challenges to Data Protection – new global players

WIRED

GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION MAGAZINE

INNOVATION INSIGHTS

community content

carplay

open automotive alliance

Windows for the car

### Consumers Are in the Connected Car Seat in 2015

BY TIM KELLY, ZUBIE 01.28.15 | 1:45 PM | PERMALINK

“Three Giants ...  
we’ll soon find out  
who takes the cake”

... This year alone, three giants – Microsoft, Google and Apple – have announced their forthcoming “connected car” platforms. Apple already has CarPlay, Google seems to have something in the works with its Open Automotive Alliance, and Microsoft revealed its “Windows for the car.” They all aim to bring the functionality of your mobile device right to your vehicles center console and we’ll soon find out who takes the cake.



Open Automotive Alliance

Apple CarPlay



Windows Embedded

<http://www.wired.com/2015/01/consumers-are-in-the-connected-cars-driver-seat-in-2015/>

# Challenges to Data Protection – remote "kill switch"

## Terrified driver almost crashes car when loan company hit 'kill switch' for missing repayments

**Mirror**

18:11, 26 SEP 2014 | UPDATED 18:35, 26 SEP 2014 | BY CHRISTOPHER BUCKTIN

Heartless creditors LOCKED T. Candice Smith's steering wheel and stopped her engine as she drove down a busy Las Vegas highway



Scared: T. Candice Smith

A terrified driver nearly **crashed her car** when it suddenly shut down on a motorway - only to find her LOAN COMPANY had used a remote kill switch after she missed a payment.

T. Candice Smith was driving with her friend down a three-lane Las Vegas interstate when her steering wheel began to lock up.

The car's engine then stopped causing the vehicle to come to a stop.

<http://www.mirror.co.uk/news/technology-science/terrified-driver-crashes-car-loan-4325955>



"used a remote kill switch after she missed a payment"





# *Challenges to Data Protection: remotely disabling vehicles*

**The Register®**  
*Biting the hand that feeds IT*

**Business ▶ Government**

## **I want to remotely disable Londoners' cars, says Met's top cop**

Psst, chief. You've probably not heard of backdoors – this is a seriously bad idea



A Met Police helmet. Pic: Shutterstock

22 Sep 2016 at 15:04, [Gareth Corfield](#)

Metropolitan Police commissioner Sir Bernard Hogan-Howe wants the capital's cops to be able to remotely disable people's cars, he told the London Assembly's police and crime committee today.

[http://www.theregister.co.uk/2016/09/22/met\\_police\\_commissioner\\_i\\_want\\_remotely\\_kill\\_car\\_electronics/](http://www.theregister.co.uk/2016/09/22/met_police_commissioner_i_want_remotely_kill_car_electronics/)

Desire of police  
institutions:  
“remotely disable  
people’s cars”



## ***Research Goals***

### **SeDaFa project goals**

- data minimizing access on car generated data
- enabling self-protection for data subjects
- due consideration of technological, legal and user aspects

### **SeDaFa research questions**

1. How can the risk of privacy breaches of car users be determined?
2. How can car users be informed about data protection aspects in an appropriate manner?
3. How can car users gain self-determined control over the access to their data?

Slide initially by Christoph Krauß (SeDaFa project)

## ***Research Approach***

### **Chosen approach for interdisciplinary research**

- list data types processed by smart cars and infrastructure
- collect list of involved entities (data subjects, controllers,...)
- define use cases to guide evaluation e.g.
  - car sharing services, garage accessing OBD data, LBS, Android Auto, distributed search for parking space
- describe legal setting, focus on upcoming GDPR
- assess necessary protection level and derive data protection requirements deploying the Standard Data Protection Model (SDM)
- propose methods to fulfil the requirements

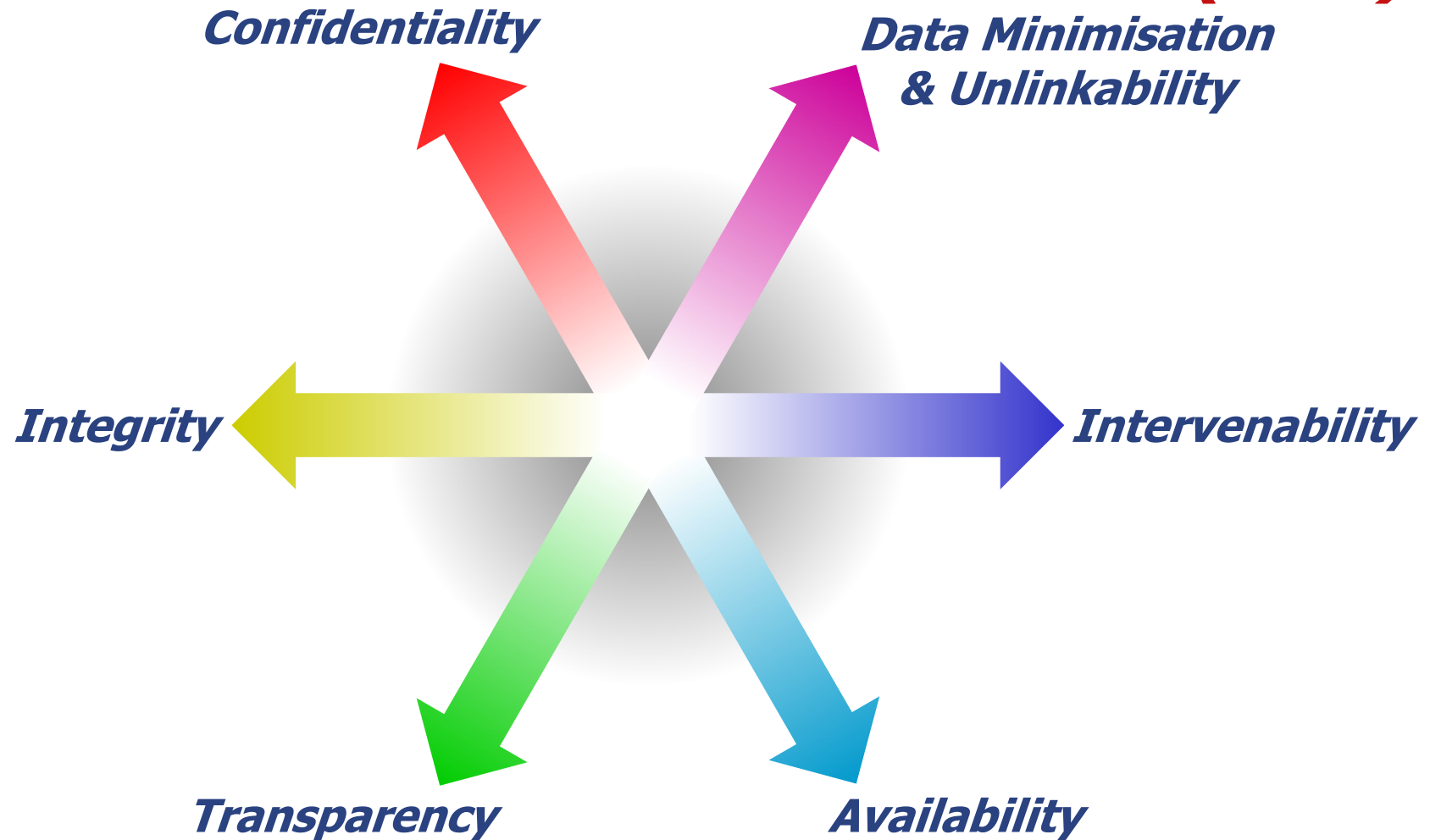
## ***Connected Cars: involved entities***

- car manufacturer
- car dealer, garage
- provider of hard- and software for cars and service provider
- network provider (e.g. 3G, 4g, 5G networks)
- app programmer
- car owners:
  - private person
  - employers
  - lessor (e.g. leasing banks)
  - rental services
  - shipping companies

- insurance companies
- other contractual parties (e.g. advertising clients)
- security authorities
- other public authorities

- data subjects according to GDPR definition:
  - car owner (private person)
  - drivers
  - previous car owner
  - car passenger
  - pedestrians & other persons

# ***Data Protection Goals & Standard Data Protection Model (SDM)***



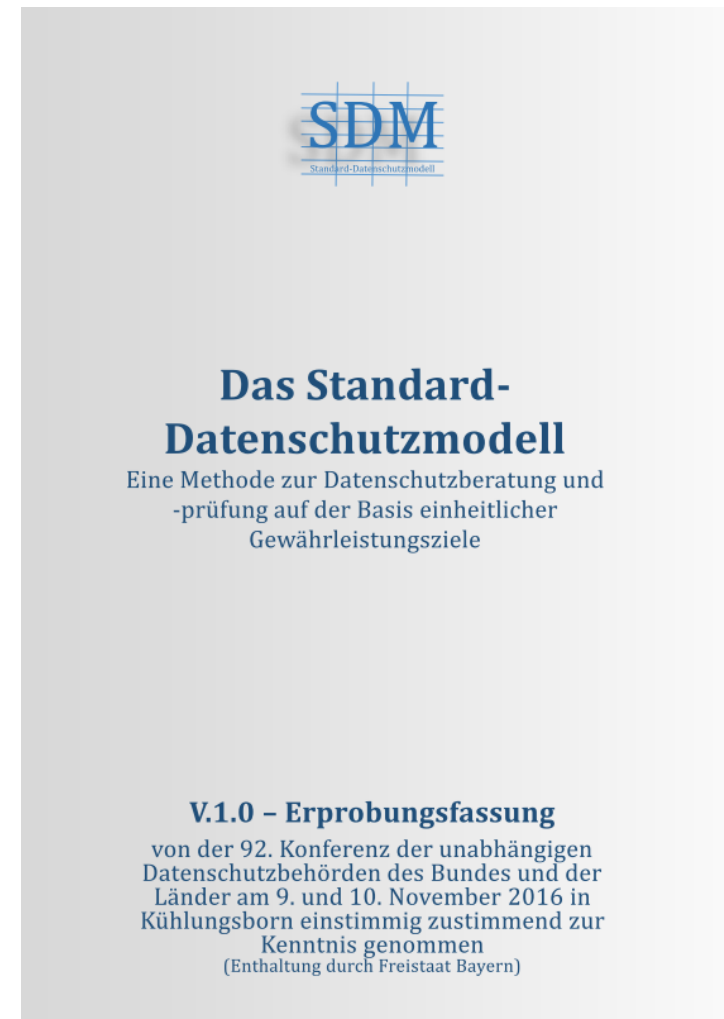


# ***More about the Standard Data Protection Model***

- Content
  - Methodology
  - Data Protection Goals
  - In progress: catalogues with measures
- V.1.0 recommended for intensified testing by the conference of German data protection authorities on federal and state level, November 10<sup>th</sup>, 2016.
- English translation: planned

German version:

[https://www.saechsdsb.de/images/stories/sdb\\_inhalt/schwerpunkt/SDM-Methode\\_V\\_1\\_0.pdf](https://www.saechsdsb.de/images/stories/sdb_inhalt/schwerpunkt/SDM-Methode_V_1_0.pdf)



## ***Requirements examples***

- The catalogue of high level requirements is under current refinement and internal discussion within the project.
- The following requirements reflect ULD's positions.
- Many requirements directly rephrase legal necessities (legal ground needed, possibility to withdraw consent at any time and data controller must have process in place to deal with withdrawal, ...).
- The focus for this presentation resides on privacy-related requirements.

## ***Transparency 1 documentation***

- Documentation MUST exist – appropriately understandable for users and sufficiently informative for experts
- Where other entities act as controllers, the documentation MUST suffice their needs to ensure compliant processing and documentation towards data subjects (e.g. car rental services, employers providing cars to employees, ...)

## ***Transparency 2 accessing documentation***

- Information necessary to fulfil transparency **MUST** be available in the car
- Interfaces of the car **SHOULD** enable users to access the information
- Where data protection impact assessment is necessary due to specific processing a summary **SHOULD** be available



## ***Intervenability 1 general principle***

- Procedures MUST be in place to influence / correct / update the personal data itself and the process of processing of personal data (change management)
- It MUST be possible to follow requests for deletion or rectification
- Requests for deletion MUST be followed in appropriate time and where data has been transferred to other entities these entities must be notified about the request, Art. 17 GDPR

## ***Intervenability 2 right to access***

- Procedures **MUST** be in place to ensure that requests for right of access / deletion can be handled appropriately
- Where processing is done under pseudonym right of access / deletion **SHOULD** be possible under pseudonym
- Systems **SHOULD** support privacy rights e.g. where data is manually deleted locally in the car and data is typically mirrored to a third parties' server as standard option data should be deleted on the server as well (privacy by default)
- Interfaces of the car **SHOULD** enable users to access and manage their personal data

## ***Intervenability 3 influencing the system***

- The data subject **MUST** have possibilities to influence the processing of personal data
- The data subject **SHOULD** have the possibility to deactivate the collection and processing of personal data without loosing core functionalities of the system
- Where options to configure the processing of personal data exist, the default settings **MUST** foresee that only personal data which are necessary for each specific purpose of the processing are processed, Art. 25 (2) GDPR (privacy by default)

## ***Data Minimisation & Unlinkability 1***

- Unlinkability includes aspects of purpose limitation: These are MUST-requirements under the GDPR
- Storing data at central entities SHOULD be avoided to prevent profiling and purpose creep, e.g. rather allow driver to select data transfers locally in the car than routing all data via servers and services of the manufacturer by default
- Separate processing for separate purposes SHOULD be preferred to allow for individual treatment of data, e.g. individual deletion periods by purpose

## ***Data Minimisation & Unlinkability 2***

- System SHOULD allow for anonymisation and pseudonymisation of data – design processes and data structure appropriately (privacy by design)
- Anonymisation SHOULD be preferred over pseudonymisation

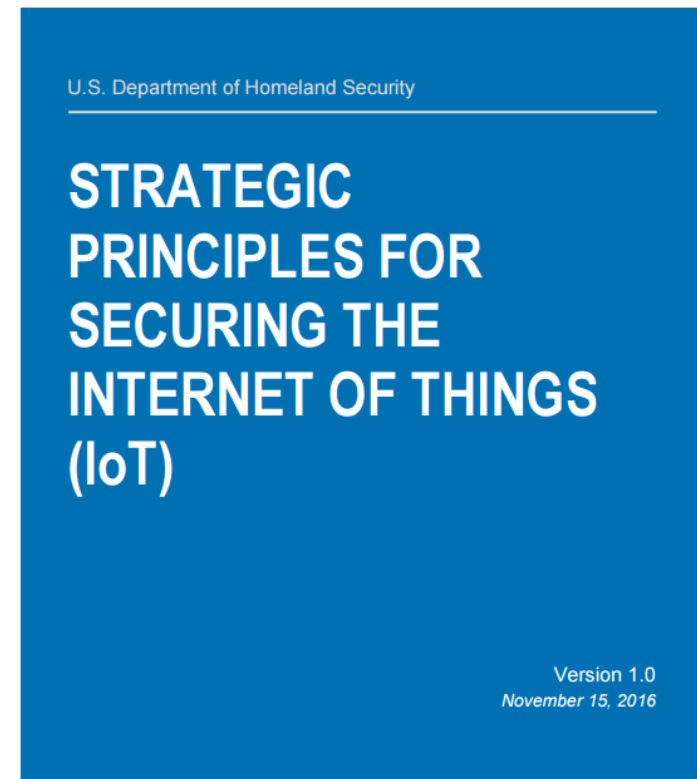


## ***IT Security: Confidentiality, Integrity, Availability***

- Deploy appropriate IT security measures and treat personal data as assets to protect, e.g.
  - role and access management,
  - encrypted transfer and storage.
- Data protection specific aspects may include
  - data portability – allow import and export of personal data and to mitigate them to another provider, Art. 20 GDPR
  - balance integrity requirements with intervenability, e.g. between backups and the right to deletion / rectification

## ***Support by IT security experts for some Protection Goals***

- Connected cars are part of the internet of things (IoT)
- Security requirements for IoT meet many of the privacy aspects
- Even a papers of typical security authorities stress
  - consideration of confidentiality and security in design phase
  - transparency – also along the supply chain of IoT products(Whenever one needs a supporting paper form an entity known for not being run by privacy activists.)



## ***Disclaimer***

- All statements reflect the position of the ULD or the personal opinion of the author where the author takes the position in favour of data protection and informational self-determination.
- Statements and positions are not made on behalf of the research projects SeDaFa, iKoPA or Privacy&Us or on behalf of the respective project partners.

## ***Funding Notice***

The results presented are based on research from these projects:



Selbstdatenschutz im  
vernetzten Fahrzeug

GEFÖRDERT VOM



Bundesministerium  
für Bildung  
und Forschung

funded by the  
German Federal Ministry  
of Education and Research

[www.sedafa-projekt.de](http://www.sedafa-projekt.de)



integrierte  
Kommunikationsplattform für  
automatisierte Elektrofahrzeuge

GEFÖRDERT VOM



Bundesministerium  
für Bildung  
und Forschung

funded by the  
German Federal Ministry  
of Education and Research

<https://fgvt.htwsaar.de/public/index.php/ikopa-2015-2018/>



Privacy & Us



funded by  
MSCA-ITN-2015-ETN –  
Marie Skłodowska-Curie  
Innovative Training Networks  
Project Number: 675730

[www.privacyus.eu](http://www.privacyus.eu)

## ***Thank you for your attention Questions? Comments?***

Harald Zwingelberg

Unabhängiges Landeszentrum für Datenschutz  
Schleswig-Holstein (ULD)

<https://www.datenschutzzentrum.de/>

E-Mail: [uld6@datenschutzzentrum.de](mailto:uld6@datenschutzzentrum.de)

Phone: +49 431 988-1222

