



Privacy in intelligent transport systems

Senior adviser Trond Foss

SINTEF

NTNU March 2019

Article 1 in The European Charter of Fundamental Rights (2009)

"The dignity of man is untouchable. It is to respect and to protect"

"Den menneskelige verdighet er ukrenkelig. Den skal respekteres og beskyttes."

What is privacy?

Privacy is about the right to a private life and the right to decide on personal information.

All people have an inviolable self-worth. As an individual, you are entitled to a private sphere that you control, where you can act freely without coercion or interference from the state or other people.

Source: Data Inspectorate



TfO 2014

The European Convention on Human Rights § 8 – 1: Right to respect for private and family life

Everyone has the right to respect for his private and family life, his home and his correspondence

3



- in other words

You decide!

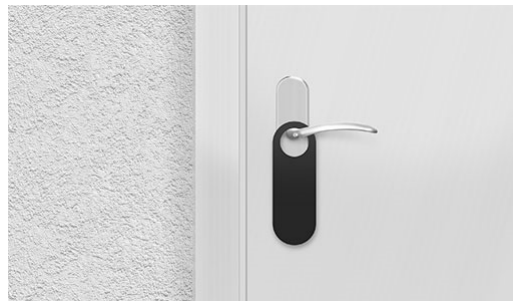


Photo: Data Inspectorate

4





It's your data – take control



DATA PROTECTION IN THE EU



5

SINTEF

Personal data



- (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Source: GDPR, § Article 4 Definitions

6

SINTEF

New Norwegian law on personal data (Personopplysningsloven)

- Came into force June 15, 2018
- The new law includes the EU General Data Protection Regulation (GDPR)
- Easier for both individuals, enterprises and organisations to act in accordance with privacy laws and regulations
- Takes into account the technological evolution



7

Foto: GÉANT Community Blog



Norwegian public transport industry norm for privacy and ICT security

Public transport privacy norm for e-ticketing supports anonymous travels by public transport where the anonymous customer has the same benefits as registered customers.


Standard
EN 15194:2012

Bransjenorm

for personvern og informasjonssikkerhet i elektronisk billettering



8



Norwegian car dealer norm for privacy

Car dealer privacy norm for new cars supports buyer and car producer awareness and consent about data collection and management of data collected by new cars.



9

Form for data collection from new cars

Informasjon om behandling av personopplysninger samlet inn gjennom bilens systemer

Bilen inneholder teknologi som kan samle inn, lagre, sende, mottar, og behandle personopplysninger. I den grad det dreier seg om personopplysninger, gjelder personopplysningsloven med forskrifter for behandlingen av disse.

Nasjonalbilde gjelder til med informasjonen mest mulig detaljert.

ULIKKE TYPER OPPLYSNINGER

OPPLYSNINGSSYSTEM. Denne bilen har et opplagsystem, inneholder den GPS. Det betyr at det kan gjøres hvor bilen kjører.

Bilen lagrer bilens data opplysninger.

Opplysninger du kan bruke til: produktutvikling, diagnostisering, handling av service, garanti, og vedlikeholdelse.

Ansikt:

Om lagrer Opplysninger: ☐ Annet: ☐ Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Informasjon om behandling av personopplysninger samlet inn gjennom bilens systemer

REGISTRERING AV KJØREHISTORIER. Denne bilen kan registrere kjøretøyets plassering og alle data som er tilgjengelig for informasjon. Dette betyr at det kan gjøres hvor bilen kjører.

Bilen lagrer bilens data opplysninger.

Opplysninger du kan bruke til: produktutvikling, diagnostisering, handling av service, garanti, og vedlikeholdelse.

Ansikt:

Om lagrer Opplysninger: ☐ Annet: ☐ Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

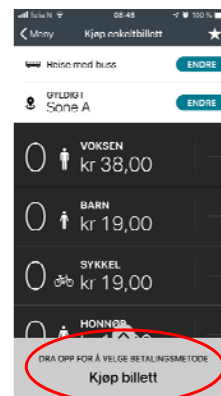
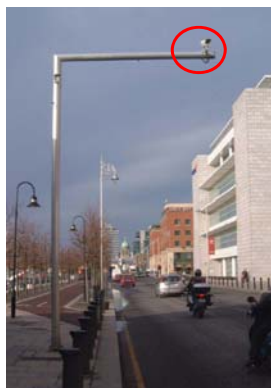
Om lagrer Opplysninger: ☐ Om lagrer Opplysninger: ☐

10

BRANSJEENDEKUTTET AV NORGE'S
BILKARANSJØRUMS, GODKJENT AV
DATATILSYNET APRIL 2017

BRANSJEENDEKUTTET AV NORGE'S
BILKARANSJØRUMS, GODKJENT AV
DATATILSYNET APRIL 2017

Many ITS applications collect personal data



11



However, the bad guy is really the car

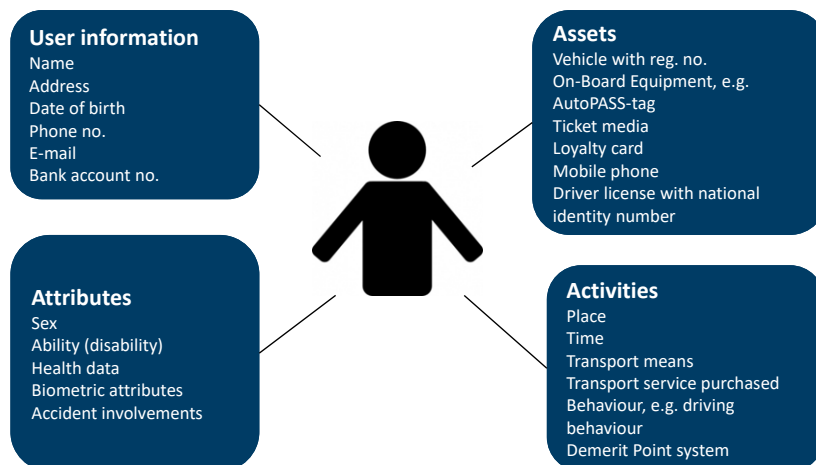


Foto: B Secure

12



Personal data related to an ITS service User



13



Where do we find the personal data?



ISO 21217 Intelligent transport systems – Communications access for land mobiles - Architecture

14



Three major challenges in ITS services?

1. Privacy

2. Security in ICT systems supporting the ITS services

3. Authorities, operators and users awareness in relation to security including privacy

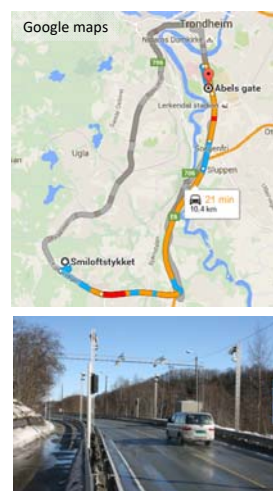


15



Examples on privacy threats

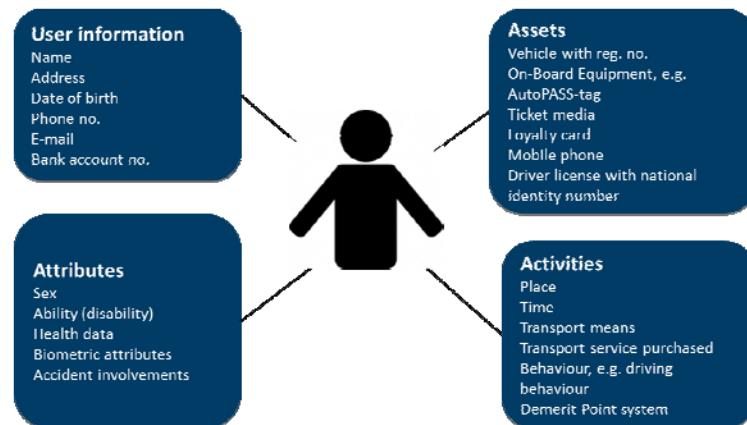
- **The ITS service User was there**
Electronic tracking of transport users (construction of travel patterns)
- **The ITS service User is there now**
Registration of the presence of a person
- **Person profiling**
Coupling of information from ITS with information in other systems



16



Some examples on where and when personal data may be collected



17



Electronic fee collection by means of an OBE and Automatic Number Plate Recognition (ANPR)

AutoPASS-tag and ANPR



18



Electronic ticketing

Contactless smartcard as ticket media



Photo: Grid Transportdesign

Mobile phone as ticket media

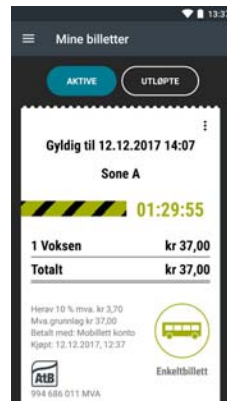


Photo: Google Play

Mobile phone as ID
(Be In – Be Out)



Photo: Wikimedia Common



Photo: techradar.com

19

NB! We have an industry norm in Norway!



Access control based on ANPR

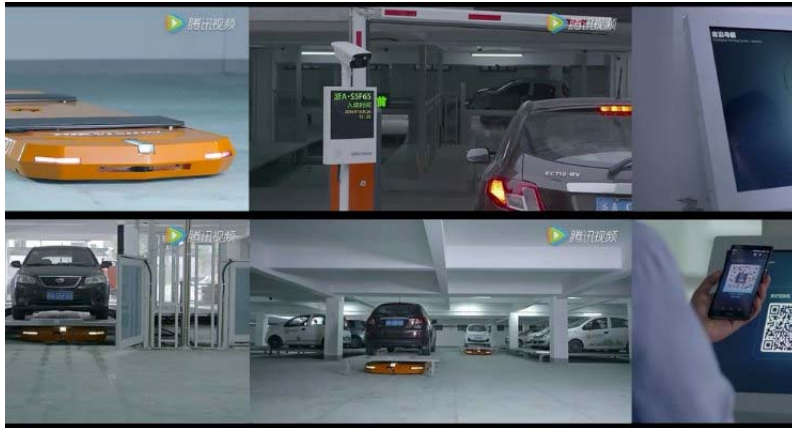


Photo: NetConnect

20



Parking payment and parking surveys based on OBE or ANPR



21

Photo: linkedin.com



Traffic data collection based on OBE, ANPR and mobile phones ID

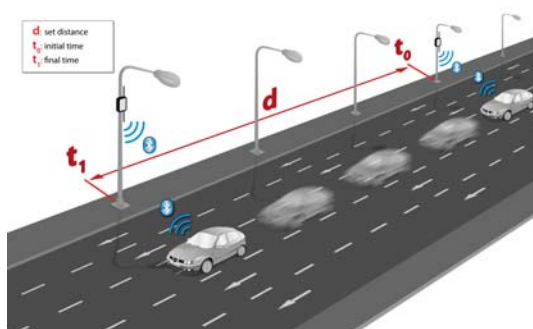


Photo: IcyApril



Photo: pixapay.com

22



Enforcement of Payment of fees, taxes and insurance based on ANPR



Foto: NRK/NRK

Control of :

- Annual vehicle fee
- Insurance
- EU vehicle control



23



Mobile unit for collection of traffic data (ASSET – EU prosjekt)



Foto: ASSET

ASSET mobile unit is equipped with 3D-camera, infrared camera and ordinary camera for collection of data from individual vehicles:

- Number plate data
- Time and place for road use
- Type of vehicle
- Vehicle dimensions
- Speed
- Headway
- Picture of vehicle front including number plate
- Usage of safety belt



24



Personal advertising based on ANPR

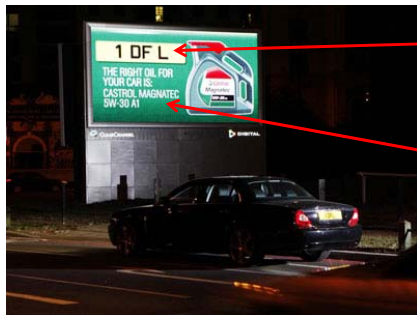


Foto: www.safespeed.org.uk/

- A hidden camera reads the number plate and access the UK vehicle register to find the car make and model
- The driver is informed about which oil type to use for his vehicle referring to the license plate number of the vehicle

25

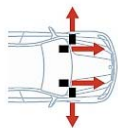


Enforcement of non-performing loans based on ANPR

The New York Times

February 28, 2010

Speed Reading: A Quicker Way to Reel In Delinquent Borrowers



Vehicles equipped with forward- and side-facing digital cameras capture images of license plates, even up to 80 miles per hour.

The images are sent to a laptop computer in the car, where character recognition software converts the license plate image to letters and numbers.

The plate number is checked against a database (of up to 100,000 entries) with the numbers of vehicles whose loans are delinquent.

If a match is found in the database, the computer displays a screen with the car's make, model, vehicle identification number and loan information.

When the identification is confirmed, the car can be towed away. Some special tow trucks can lift a car and drive off in 10 seconds.

RC357H4U

RC ? 4U

RC ! 4U

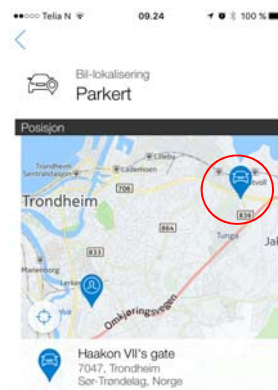


The New York Times
RECOMMEND

26



Fleet management with vehicle tracking, real time applications, stolen vehicles and smart apps (e.g. Volvo OnCall)



Volvo OnCall

27



Jamming of GPS – privacy or crime?



Mange peker på at stadig flere virksomheter med en bilflotte, og ikke bare bedrifter, bruker GPS-styring. Da er det ikke uventet at arbeidstakere vil hindre å bli overvåket, skriver en leder i Follo. Eivind Fjærli i Lyster.

GPS-JAMMERE

Tyver, taxi-sjåfører og radiosendere

Mange mulige svar på hva som jammer GPS-ene våre.

Teknisk Ukeblad 12. mars 2014

28



Location based services

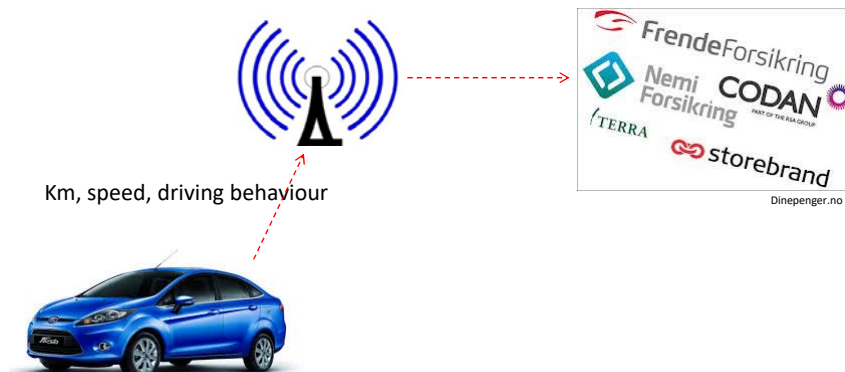


- Information about
 - Services
 - Points of Interest
 - Public transport
- Driver assistance systems, e.g. route guidance

29



Pay as you drive



30



Security in ITS sub-systems

Potential attackers:

- Hackers
- Activists
- Terrorists
- Criminal organisations
- ITS service Users
- Operators
- Authorities
- Foreign powers

*Attacks
against sub-
systems and
interfaces*



ISO 21217 Intelligent transport systems - Communications access for land mobiles - Architecture

31



How to get access to the vehicles internal ICT system?



www.canbushack.com



www.hackaday.com



www.caranddriver.com



Volvo On Call

Beskrivelse

Starting from model year 2012, Volvo now brings you the ability to access your vehicle from your iPhone, iPad or iPod touch. Volvo onCall Telematics unit. If your vehicle conforms with these requirements you will, depending on your model be able to

- See vehicle dashboard values, such as fuel level, trip meters, and more, in the App.
- Control your fuel fired parking heater, if the vehicle is equipped with a fuel fired parking heater.
- Locate your vehicle on a map or using the vehicle signal horn and turn indicators.
- See the current status of doors, windows and locks for your vehicle.
- Lock and unlock the vehicle.
- Request road side assistance from the App.
- Have an electronic driving journal, that will create trip reports for every trip made with the vehicle.

iTunes Appstore

32





Teknisk Ukeblad 8. mai 2017

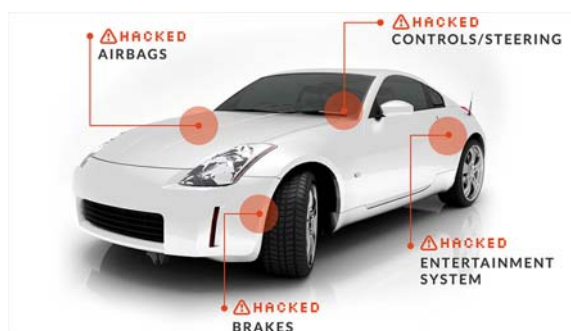
Fast Chrysler måtte tilbakekalle 1,4 millioner biler etter at Charlie Miller og Chris Valasek hacket seg inn i en bil og tok kontroll over både bremses og styring.
(Bilde: JOE RAEDLE/Scamper)

HACKING AV BIL

Mannen som hacket en Jeep advarer: – Alle biler lar seg hacke

– Det er vanskelig å hacke en bil. Men det burde være enda vanskeligere, mener Charlie Miller.

33



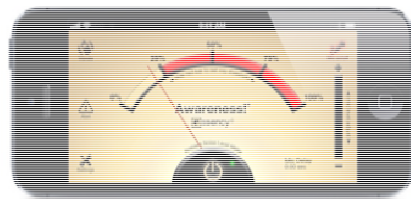
34



What is the awareness of authorities, operators and users?

Literature review shows that :

- The awareness of safety and security in intelligent transport systems is limited and there is a gap that should be closed
- The awareness on privacy is better which probably is caused both by laws and regulations and more attention regarding privacy in other sectors, e.g. the health sector.



35



Could privacy be ensured in intelligent transport systems?

36



'The simplest is often the best'

*Avoid as far as possible
collecting and/or using data
that could be linked to a
person*



*In worst case, - encrypt or
make the data anonymous*

37



Privacy by design shall be the default methodology



*Specification and development of ITS applications should
take place in close cooperation with the Data
Inspectorate*

38



Three very important principles

CIA



- **C**onfidentiality – data shall be protected against non-authorised access (Konfidensiell)
- **I**ntegrity – data shall not be changed between authorised sender and authorised receiver of the data (Integritet)
- **A**vailability – data shall be available when the ITS application requires the data (Tilgjengelighet)

39



Other principles

- User consent of the use of personal data
- Deletion of data as soon as they have served their purpose
- Transparency for the Transport user
- Transport user involvement
- Easy accessible and understandable description of the purpose of the data management
- Minimisation of the data collection
- Limited use of the collected data
- Personal data shall be correct, relevant, timely and complete
- The data shall be protected against loss and non-authorised access, deletion and changes
- Revisions shall be carried through
- Training of personal handling the data



40



Could privacy be ensured in intelligent transport systems?

The answer is Yes, if

Thank you for your attention!

trond.foss@sintef.no