State of the art –
Tema med relevans for personvern

Marit Natvig, Isabelle Tardy, Aida Omerovic, Gencer Erdogan
SINTEF IKT

Personvern – forordninger og press på forretningsmodeller
Frokostmøte og workshop

ITS Norge og SINTEF
04.05.2016

Agenda

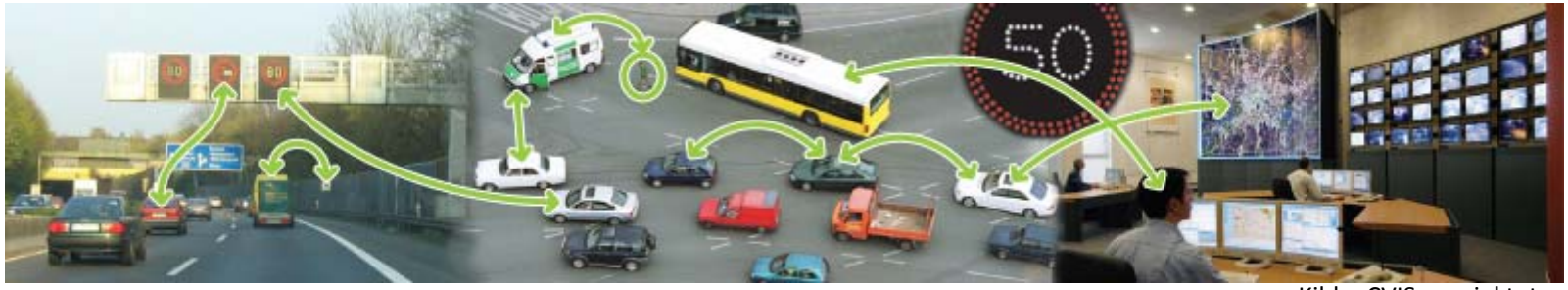
- ITS og personvern – Marit Natvig
- Trådløse nett og personvern – Isabelle Tardy
- Teknologier som fremmer personvern – Aida Omerovic
- Analysemetoder for personvern – Gencer Erdogan

ITS og personvern

Marit Natvig
SINTEF IKT
marit.natvig@sintef.no

ITS-eksempler

- Kommunikasjon mellom bil, infrastruktur og baksystemer
  - eBillettering – elektronisk billettering i kollektivtransport
  - Betaling for vegbruk - bomstasjoner og vegprising
  - Fartskontroll – i punkt eller strekningsbasert
  - Digital tachograf – sporer kjøring - lokasjon, fart, stopp, etc.
  - Flåteovervåking – sporing av kjøretøy og evt. kjøreadferd
  - Trafikkdata – innhenting av trafikktellinger, floating vehicle data, reisetid, etc.
  - Betaling for parkering
  - eCall – automatisk nødmelding initiert av sensorer
  - Pay-As-You-Drive – forsikringspremie iht kjøreadferd
  - C-ITS (Cooperative ITS) – V2x (V2V og V2I/V2R)

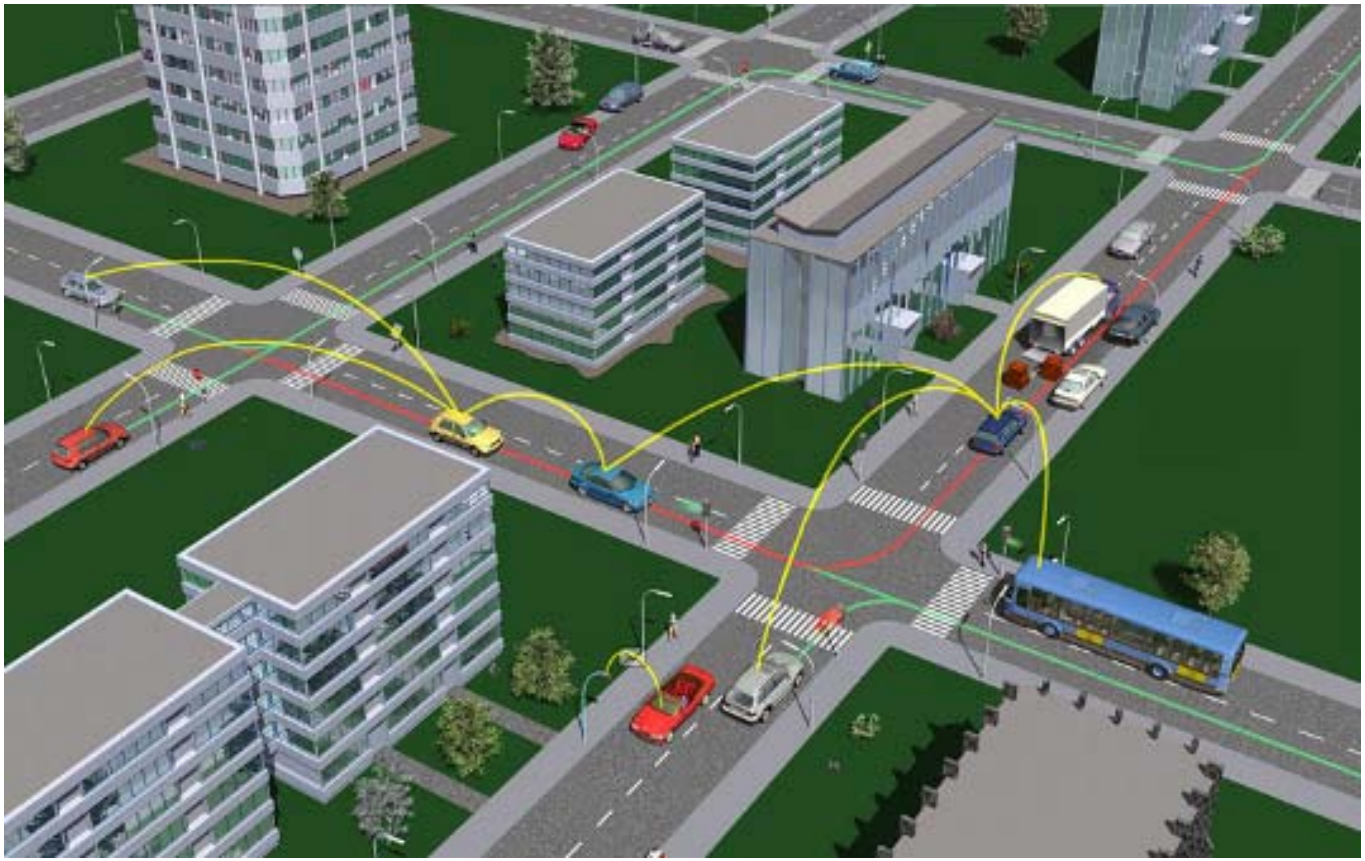


Kilde: CVIS-prosjektet

Utfordringer relatert til ITS og personvern - eksempler

- Frivillige vs. obligatoriske tjenester
  - Tjenester som er frivillige kan etter hvert bli eneste alternativ (f.eks. eBilletter)
- Lokasjonsdata
  - Enkeltregistreringer av lokasjon og tidspunkt
  - Flere registreringer som muliggjør sporing av deler av tur/rute
  - Komplette sporinger av person eller kjøretøy på hele turer/ruter
- Turdata uten lokasjonsdata (f.eks. strekning og tid)
  - Enkeltregistreringer
  - Komplette eller nesten komplette logger over bevegelser
- Data om føreradferd
  - Kjøremønster (fart, akselerasjon, bremsekraft, timer kjørt)
  - Helserelaterte data (f.eks. ulykker)
  - Data om lovbrudd (f.eks. hastighet)

C-ITS

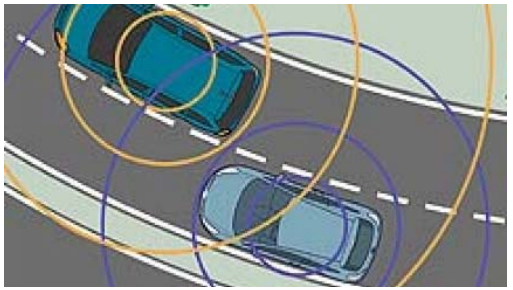


Kilde: www.worldreviews.com

Eksempler

- Brems!
- Slipp fram ambulanse!
- Hindring i veien!
- Her er det glatt!
- Jeg kommer rundt hjørnet!
- Buss med prioritering!

Personvernproblemstillinger relatert til C-ITS



- **Cooperative awareness message (CAM):**
  Kontinuerlig ukryptert info om biltype,
  posisjon, hastighet, retning, størrelse ,akselerasjon, …
- **Desentralised environment notification message (DENM):**
  Trigges av hendelse.

- Meldingene kringkastes til alle i en omkrets på opp til 1 km
- Enhetene i C-ITS-nettet (biler, vegkantutstyr, etc.) benytter mottatt informasjon til å
  - Lage seg et bilde av trafikksituasjonen
  - Handle
  - Gi advarsler/alarmer, råd, informasjon, etc.

- Bilenes ID byttes ut hyppig, men det er mulig med indirekte identifisering og sporing
- CAM/DENM ansees derfor som persondata

Juridiske utfordringer når C-ITS-[illegible] ansees som persondata

- Må vurderes i hvert enkelt tilfelle
- Må definere juridisk rammeverk og hvilke applikasjoner dette gjelder
- Må ikke bruke/prosessere data ut over det som er hensikten

- I dag:
  - Ingen lovgivning krever bruk av C-ITS
  - Personvernet kan ikke "settes til side" – bl.a. fo[illegible]ke er vesentlig[illegible]ed vanlig kjøring
  - Samtykke er i dag eneste juridiske mulighet
  - Kringkasting av informasjon må kunne skrus [illegible]g på

- DG MOVE: ITS Platform – Final report 2016. WG [illegible] Trenger ulike juridiske b[illegible]grunnelser:

C-ITS Applications	Possible legal Basis justif[illegible]ng the processing of data
Road safety	Processing is necessary to protect the **vital interests** of [illegible]ata subject(s)
Traffic efficiency	Processing is necessary for performance of a task carried out in **public interest**
Global internet services Infotainment Co-operative local services	Processing is based on **consent** and/or Processing is necessary for performance of a **contract**

Trådløse nett og personvern

Isabelle Tardy
SINTEF IKT
isabelle.tardy@sintef.no

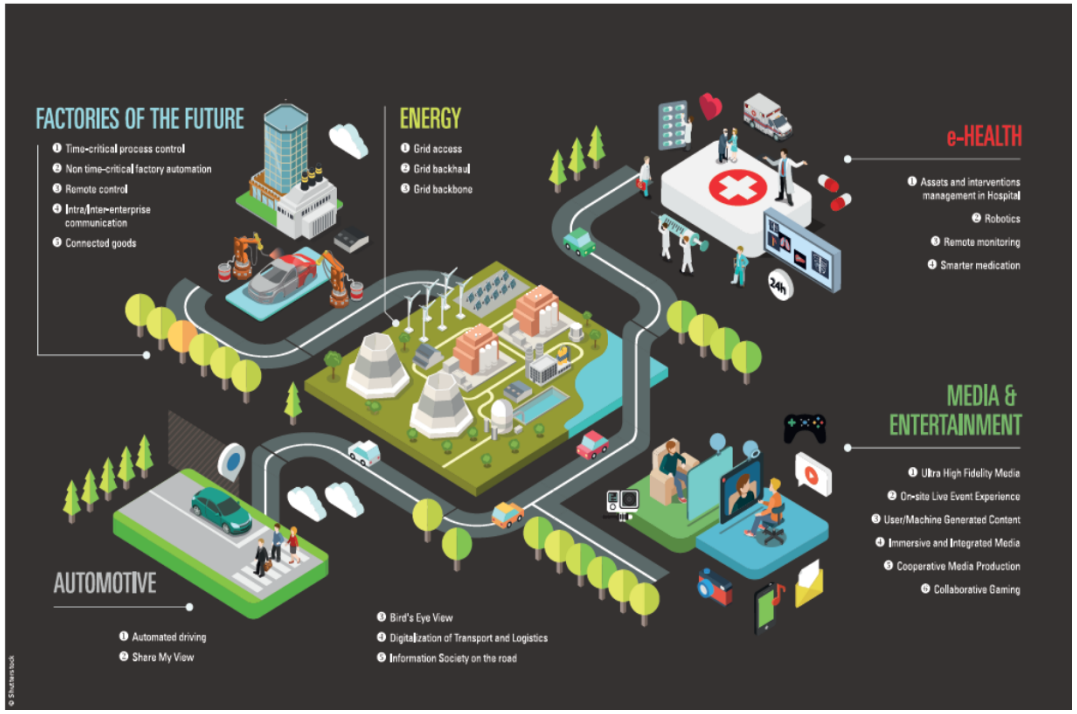
Introduksjon til trådløse nett

- Kommunikasjon mellom
  - Telefoner, smarttelefoner (dvs. personer)
  - Ting (eks. sensorer, maskiner)
- Kommunikasjoner med ulike tekniske krav, bl.a. grader av *mobilitet og forretningsmodeller*

Tjenester	Relevante trådløse nett
Mobil bredbånd -> Høy hastighet og mobilitet	3GPP: 2G (GSM), 3G (UMTS), 4G (LTE/LTE-A), 5G
Tingenes Internett -> Mange ting og pålitelig kommunikasjon -> ITS hører her foreløpig	WiFi, bluetooth + LPWAN (wireless HART, ISA100, LoRa, SigFox, LTE-M)

5G

- Hvorfor 5G?
  - Integrere vertikaler (IoT) innen eksisterende 3GPP (og WiFi) infrastrukturen
  - Utvide kanaler til millimeterbånd for å øke hastighet til alle



From "5G empowering vertical industries", a white paper from 5G-PPP, EU, 03/2016.
Se også på¨www.5gsig.no

Smart city med 5G = enda flere trådløse nett enn før, noen for kontroll, andre for kommunikasjon, både mennesker og ting skal kobles sammen

- > Både en løsning og et problem ift. sikkerhet og personvern

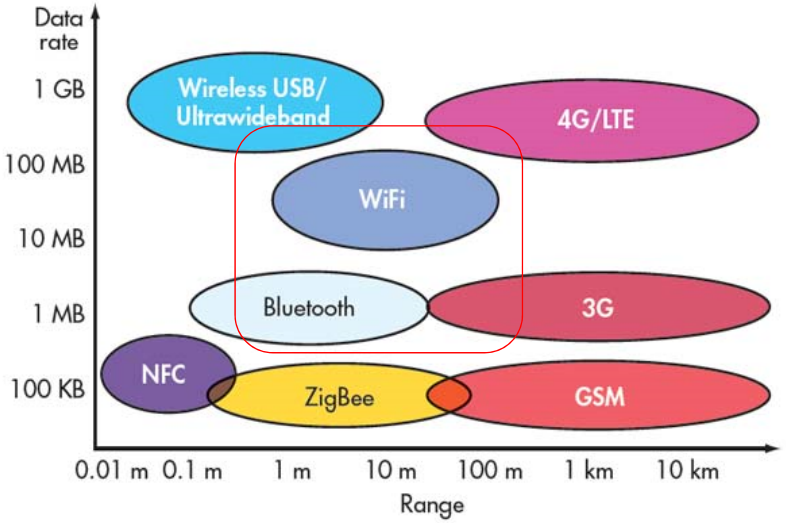
Utfordringer knyttet til trådløse nett ift. personvern

- Alle trådløse nett - 2G-5G, WiFi varianter, LPWAN, bluetooth- kringkaster sin identitet regelmessig.
  - Mange personer kan bli spionert på
    - Ref. f.eks. sak om falske basestasjoner ved stortinget des. 2014. Spesielt ubeskyttet på 2G, og 4G (tale) kan bruke 2G i dag!
- Hva kan man finne ut av et trådløsnett?
  - En mottatt signal = en transmisjon
  - Lokasjonen til transmitteren
  - Identiteten til transmitteren
  - Bølgeform (= nett teknologien)
  - I verste fall innhold
  - Kombinasjon av disse

Noen av de mest brukte nettverk: WiFi/bluetooth

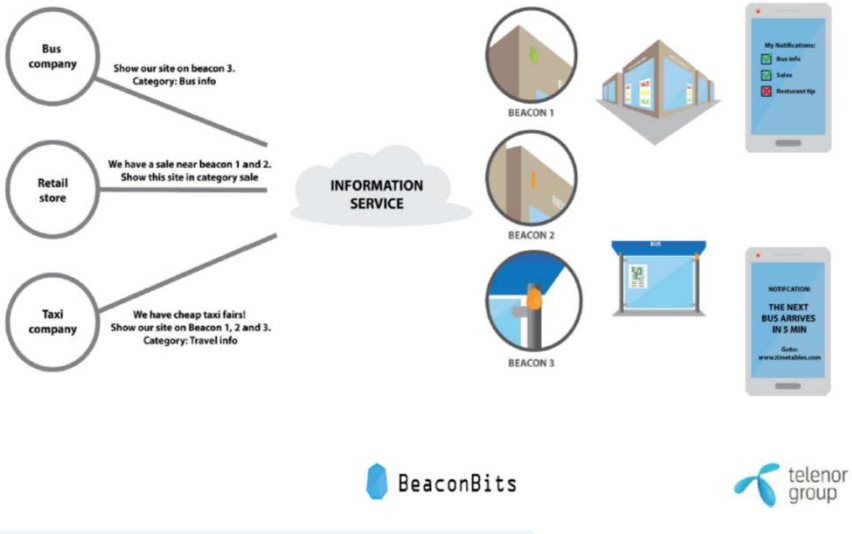
- *Alle* moderne smarttelefoner har tilkoblingsmulighet til 3GPP (opp til 4G) og bluetooth og WiFi.

- Typisk *rekkevidde* (men store variasjoner ifølge omgivelser)
  - WiFi (IEEE 802.11n): 100-200m (halvparten innendørs)
  - Bluetooth (IEEE 802.15 a): 1-100m (avhengig av utsendt effekt og versjon, opp til 200m utendørs i den aller siste versjon)
  - Hastighet er forskjellig men overlapp i rekkevidde
  - Bruk av felles frekvenser (2.4 GHz) på samme sted fører til dårligere forbindelse



Beacon: deteksjon og lokasjon

- Beacons kan være plassert i enkelte butikker, flyplasser…
- De bruker Bluetooth for å kringkaste sin egen identitet
- De blir gjenkjent av smart telefoner takket en app som svarer beacon (fra denne butikken) at smarttelefonen befinner seg i nærheten
  - *Man må i forkant gi tillatelse til både lokasjon og bluetooth teknologi på telefonen*
  - *Beacon henter ikke data, hverken lokasjon eller MAC @, det er gjerne det motsatt, telefonen sporer beacons ☺*
- Man kan få skreddersydd informasjon fra butikken ->
- app-leverandører begrenser seg ikke til å lese av kun egne beacons, men også andres. Det er etablert beacons-registre for allmenn bruk, som gir informasjon om de enkelte beacons

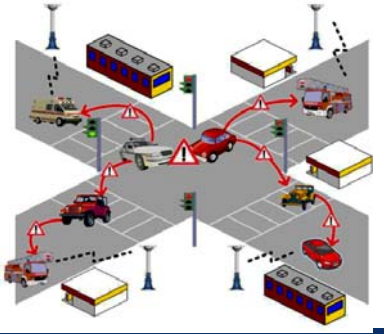


Pass på beacon app'en!

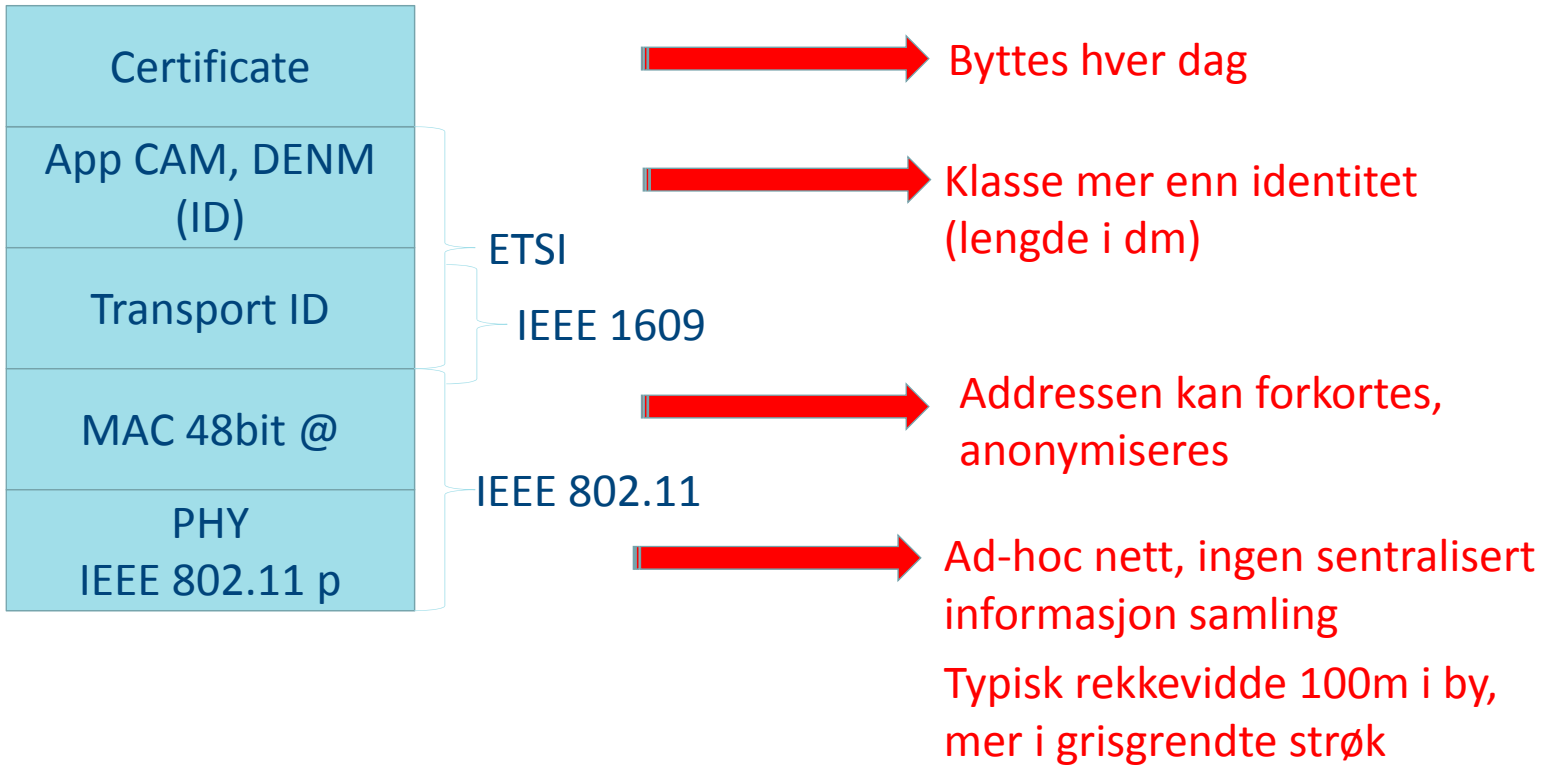
Personvern med trådløse nett, en umulig oppgave?

Privacy by design

- Bedre lokasjon kringkasting mekanismer på 3G/4G enn på 2G. Men utfordringer på WiFi og bluetooth.
- Autentisering- og aksess kontroll mekanismer, SIM-basert, login, eller?
- Bluetooth/WiFi må ikke ALLTID være på
- Pass på app'er som bruker lokasjon (eks. ifm. Beacon). Pass på at eventuell lokasjonshistorikk blir slettet.
- Private nett, a la "closed group" på LTE innendørs, private celler
- Kort distanse kommunikasjon (lav effekt, høy frekvens) for å begrense det fysiske fare området
- Ad hoc: ingen sentral enhet som vil samle og analysere transmisjonsdata



C-ITS: hva har man tenkt ift. personvern?



Teknologier som fremmer personvern

Aida Omerovic
SINTEF IKT
aida.omerovic@sintef.no

Teknologier som fremmer personvern – noen eksempler

- Anonymisering
- Kryptering
- Pseudonymisering
- Plattformer for personvern-preferanser
- Autentisering
- Metadata for tilgangsstyring
- Tilgangsstyring
- Logging av bruk og endring av data
- Minimalisering av informasjon

Andre typer tiltak – noen eksempler

- Kravhåndtering
- Arkitektur som muliggjør personvernhåndtering
  - "Privacy by design"
  - Distribuert/lokal prosessering
  - Tidlig sletting av data og bruk av aggregerte data
- Separasjon av domener (info om brukeren behandles adskilt)
- Brukervennlighet
  - Forståelig info til brukerne
  - Samtykke som er tydelig for brukeren
  - "Data subject control"
- Standardisering
- Revisjon av personvern

Analysemetoder for personvern

Gencer Erdogan
SINTEF IKT
gencer.erdogan@sintef.no

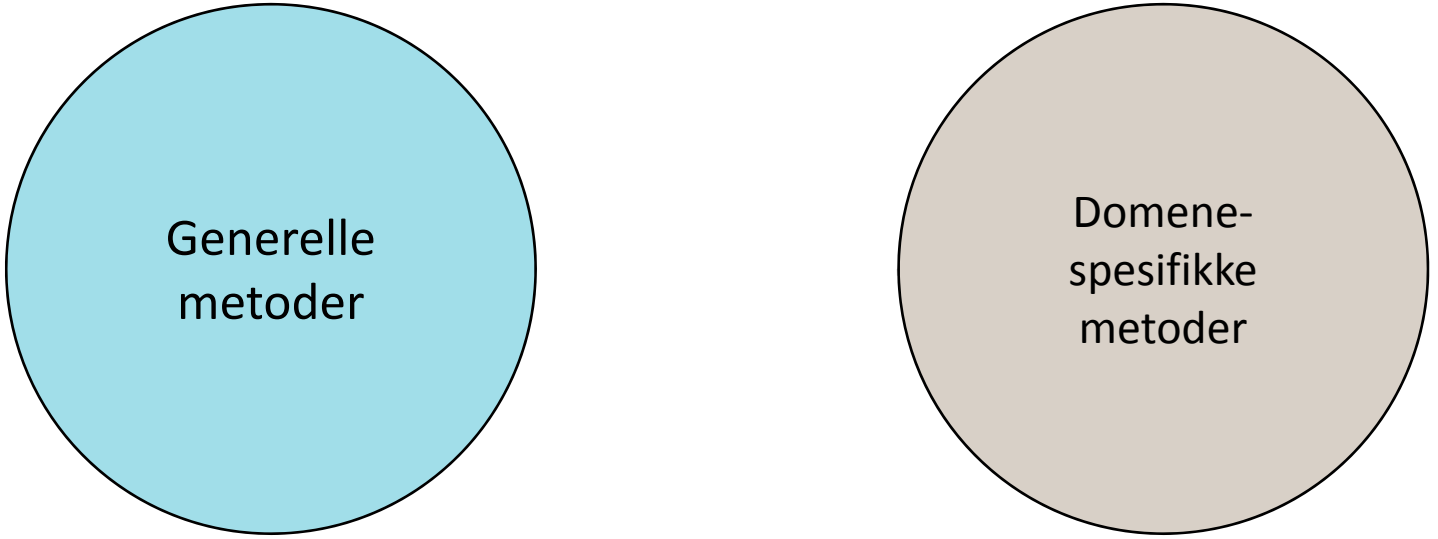
Analysemetoder for personvern: Begrep og definisjon

- Fellesbegrep i litteraturen:
  - Privacy Impact Analysis (PIA)

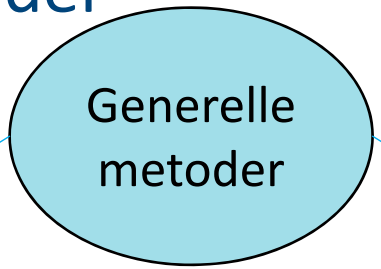
- Definisjon (forkortet)
  - PIA er en metode for å vurdere og behandle personvernrisiko [1].

[1] David Wright and Paul De Hert (Eds.). Privacy Impact Assessment. Springer 2012.

Analysemetoder



Generelle analysemetoder



- Metoder på statlig nivå
- Standarder

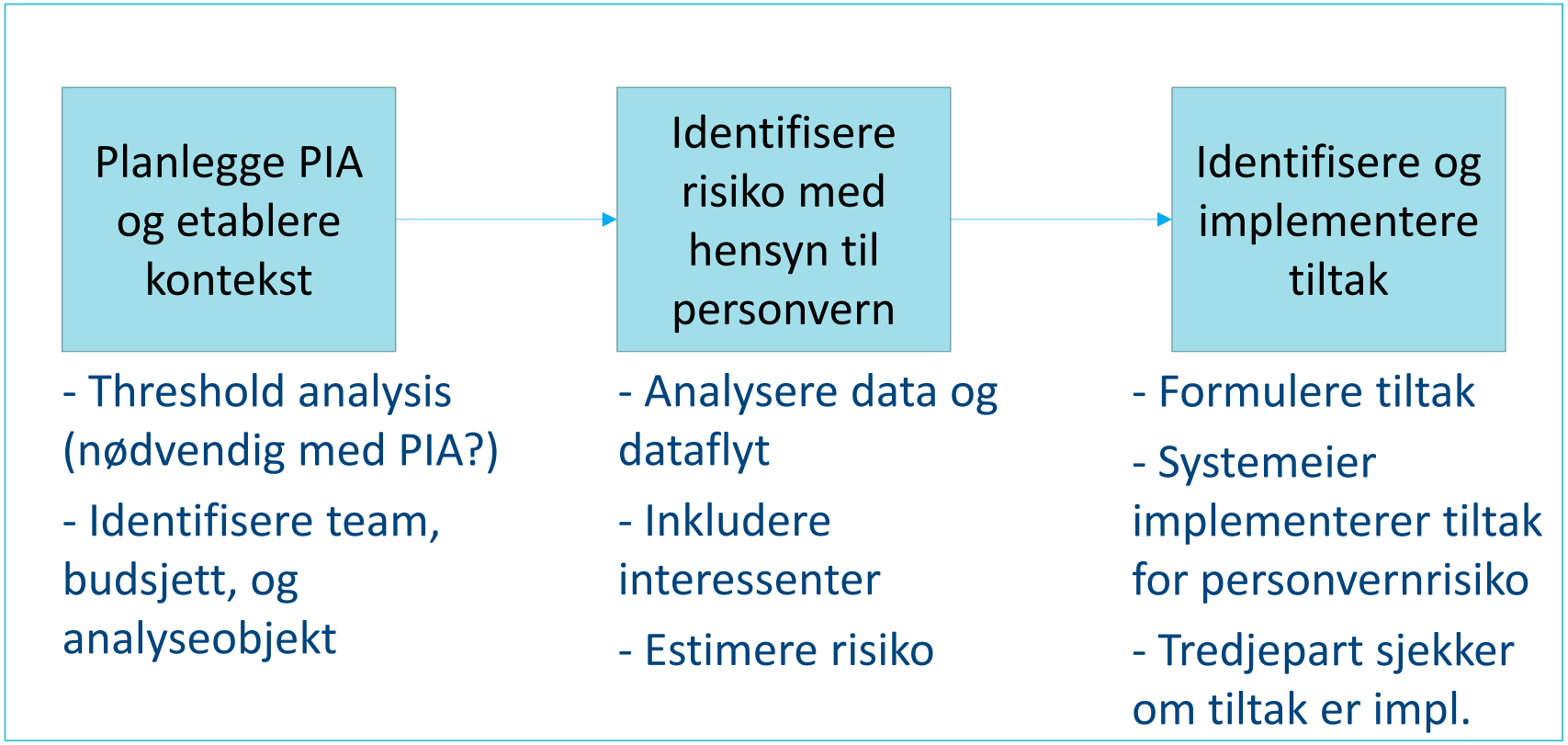
	Australia	Canada	NZ	UK	US
Systematisk prosess	X	X		X	
Kun sjekkliste			X		X
Kun til bruk i regjeringen		X			X
Inneholder et sett av prinsipper for personvern	X	X	X	X	(x)
Maler og templater	X	X	X	X	(x)
Utføres som en del av risikohåndtering	X	X	X	X	X

ISO 31000
Risk Management

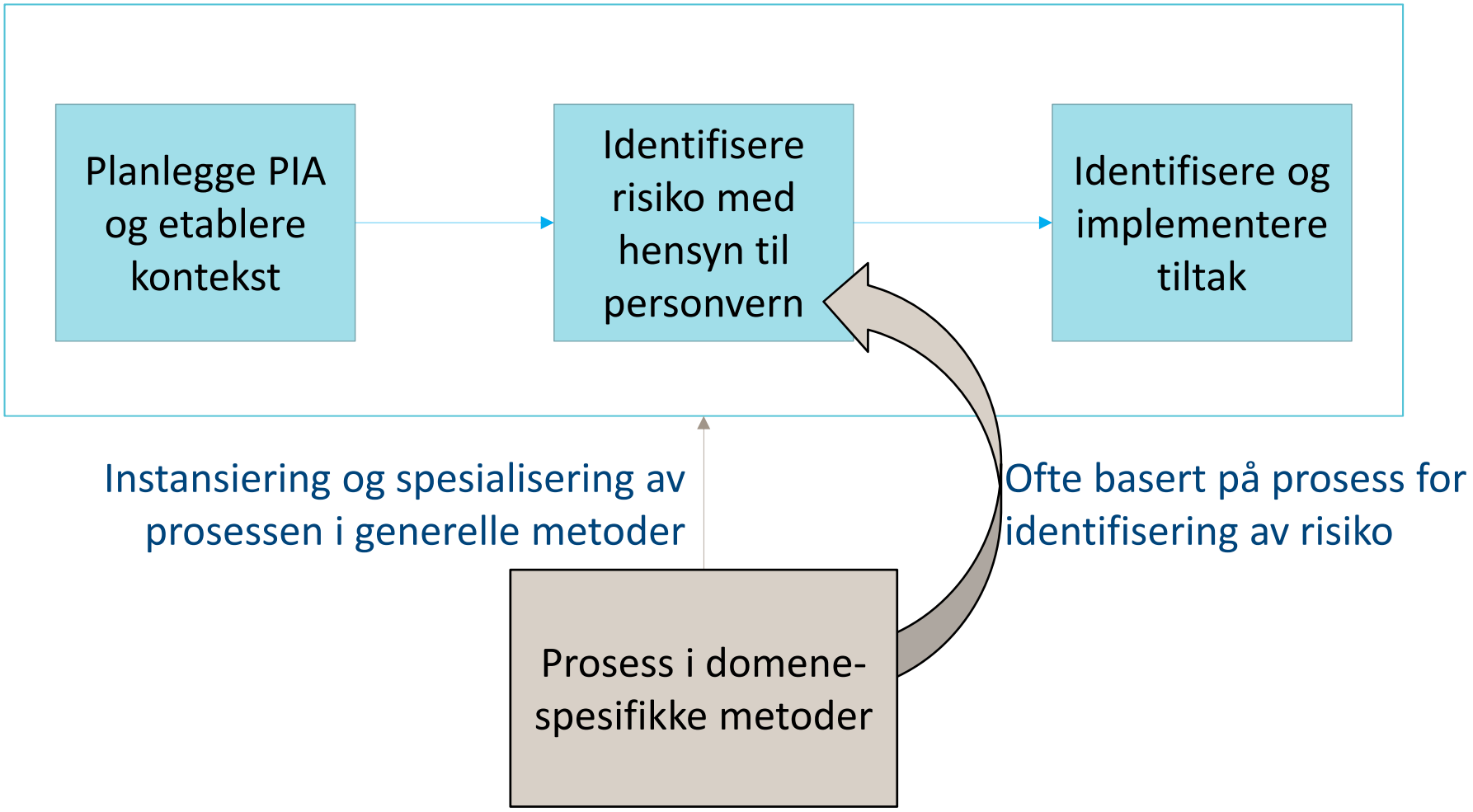
ISO 27005
Security Risk Mang.

ISO 29100
Privacy Framework

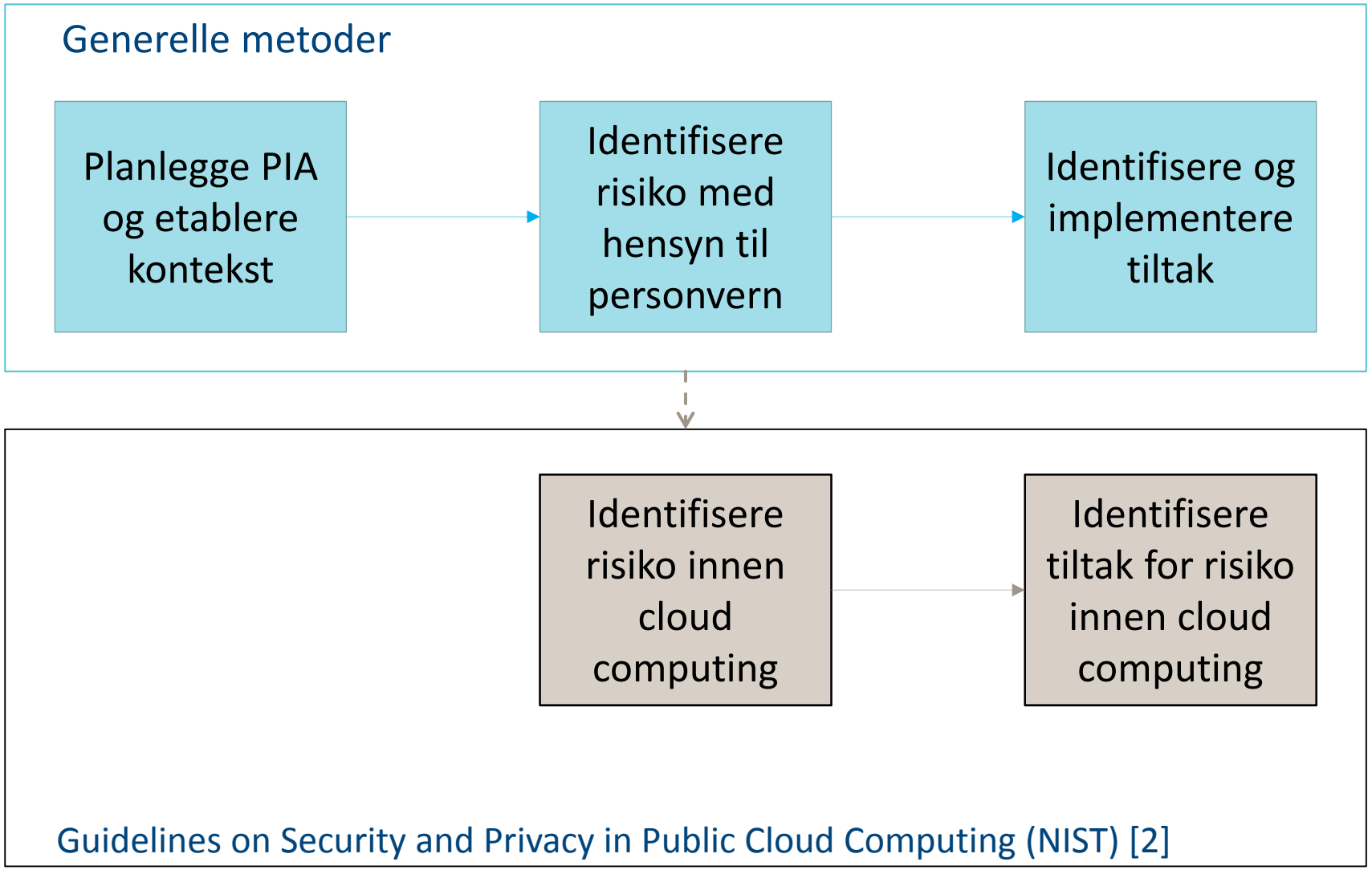
Prosess i generelle analysemetoder



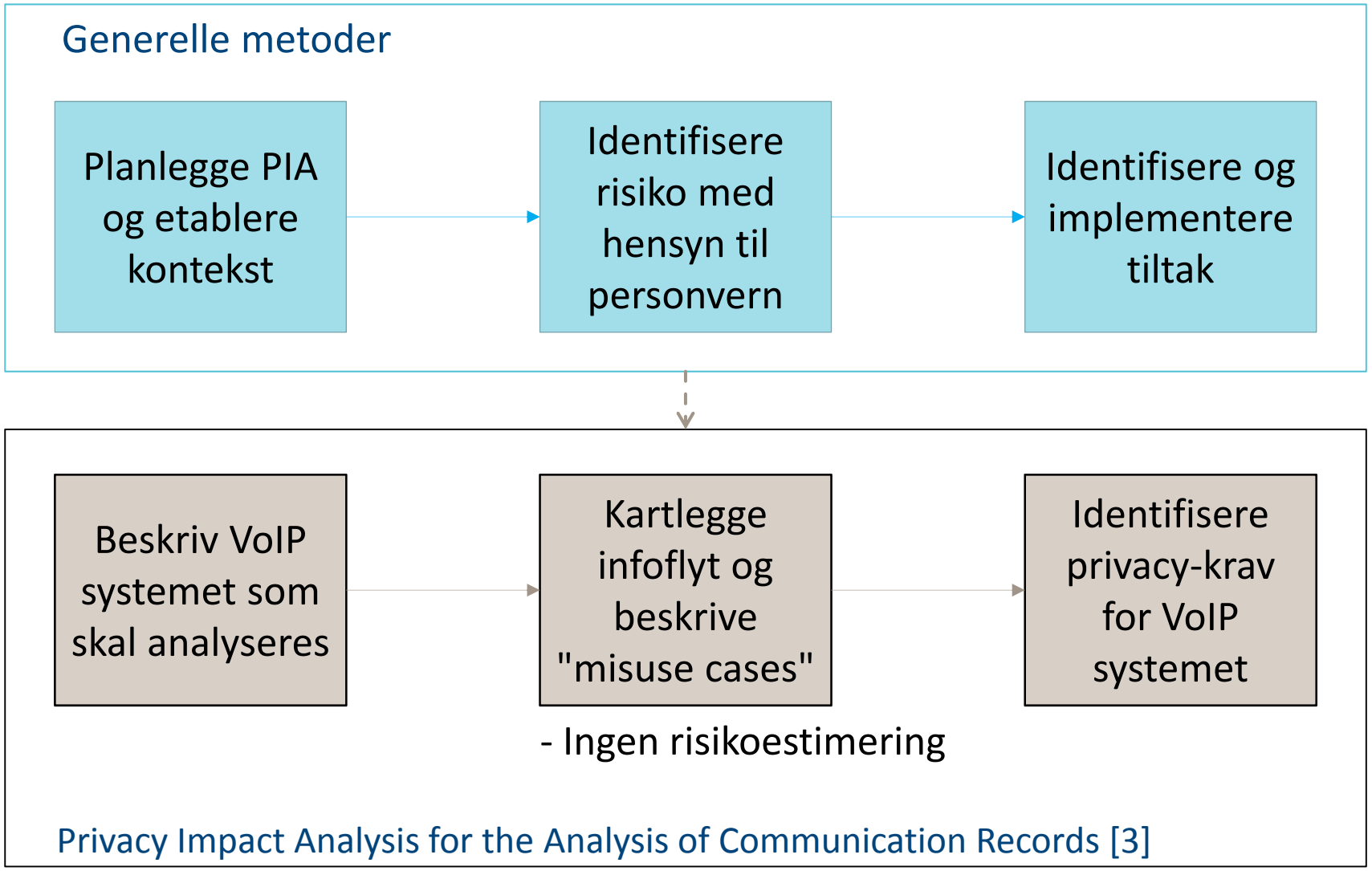
Prosess i domene-spesifikke analysemetoder



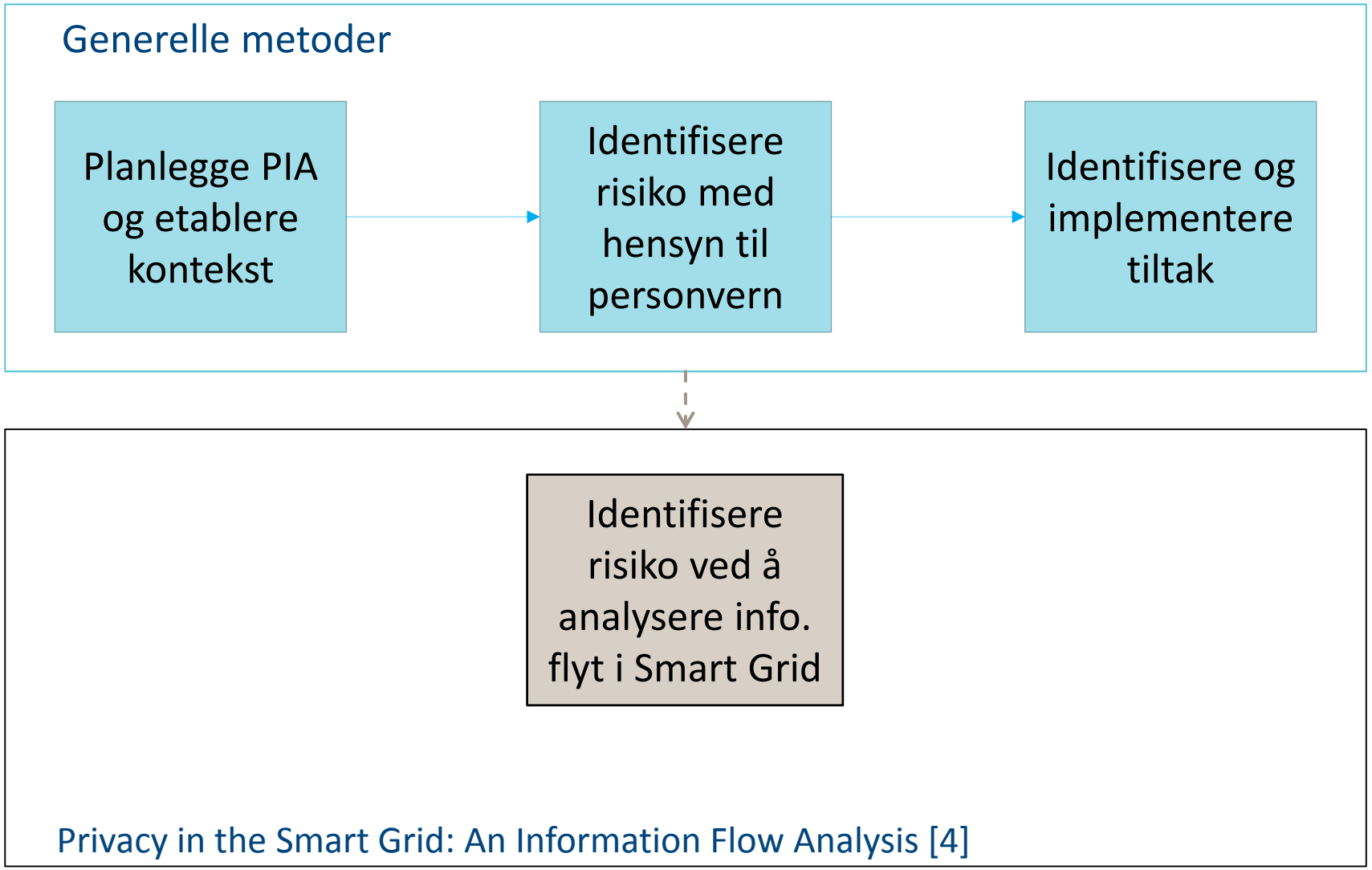
Domene-spesifikke analysemetoder: Cloud eksempel



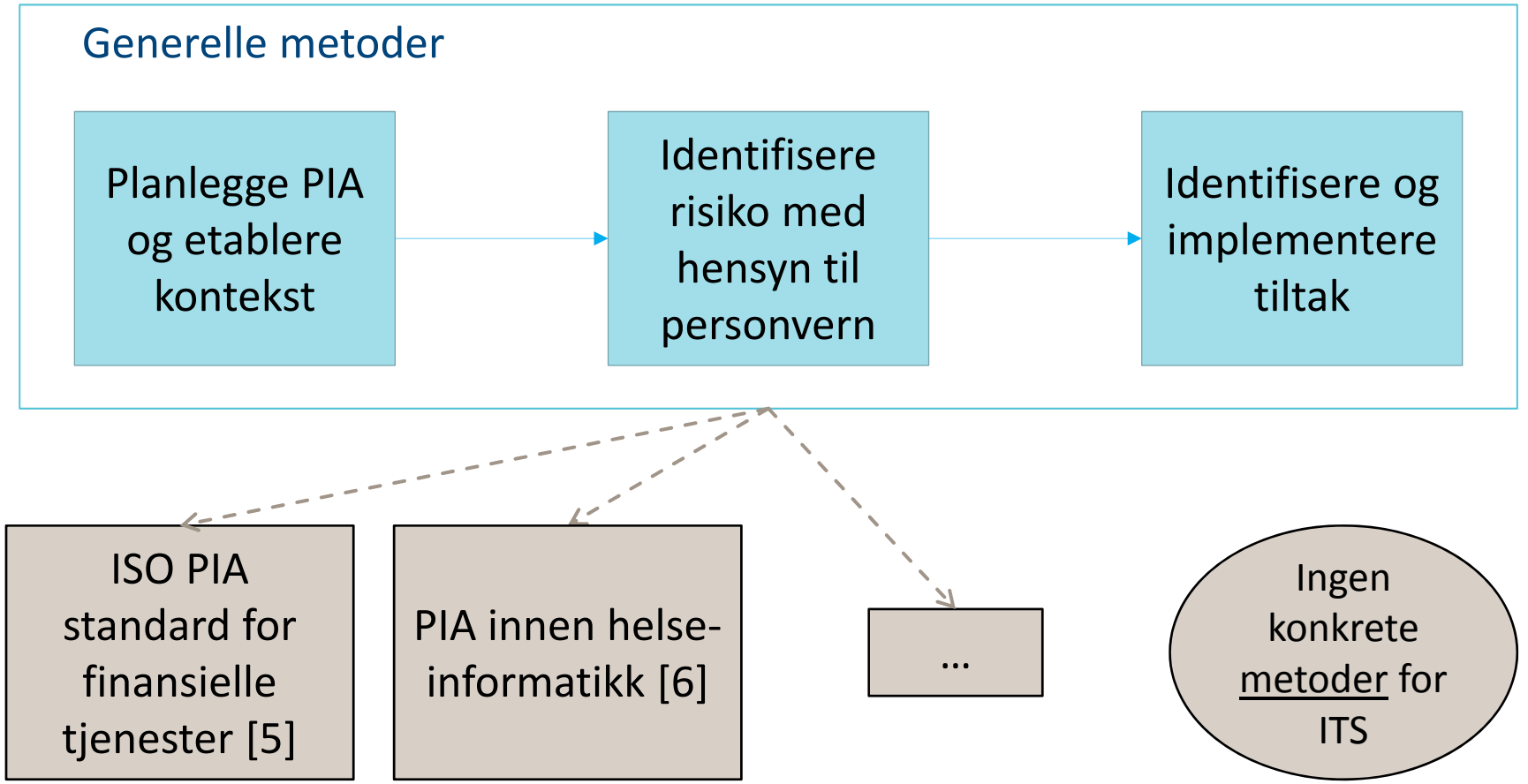
Domene-spesifikke analysemetoder: VoIP eksempel



Domene-spesifikke analysemetoder: Smart Grid eksempel



Domene-spesifikke analysemetoder



Referanser

- [1] David Wright, Paul De Hert (Eds.). Privacy Impact Assessment. Springer 2012.
- [2] Wayne Jansen, Timothy Grance. Guidelines on Security and Privacy in Public Cloud Computing. NIST Special Publication 800-144. NIST 2011.
- [3] Stefan Hofbauer, Kristian Beckers, Gerald Quirchmayr. Conducting a Privacy Impact Analysis for the Analysis of Communication Records. In Proc. 11th International Conference on Perspectives in Business Informatics Research. Springer 2012.
- [4] Deirdre K. Mulligan, Longhao Wang, Aaron J. Burstein. Privacy in the Smart Grid: An Information Flow Analysis. University of California, Berkley, 2011.
- [5] ISO 22307:2008 – Financial services – – Privacy impact assessment. ISO 2008.
- [6] C. T. Di Iorio et al. Privacy impact assessment in the design of transnational public health information systems: the BIRO project.