SINTEF

A10670 - Åpen

Rapport

Personvern og trafikk: Personvernet i intelligente transportsystemer (ITS)

Forfattere
Liv Øvstedal
Lone-Eirin Lervåg
Trond Foss

SINTEF Teknologi og samfunn
Transportforskning
November 2010

SINTEF

SINTEF Teknologi og samfunn
Transportforskning

Postboks: 4760 Sluppen
Postadresse: 7465 Trondheim
Besøksadresse: S P Andersens veg 5
7031 Trondheim
Telefon: 73 59 03 00
Telefaks: 73 59 46 56

Foretaksregisteret: NO 948 007 029 MVA

SINTEF RAPPORT

TITTEL

Personvern og trafikk: Personvernet i intelligente transportsystem (ITS)

FORFATTER(E)

Liv Øvstedal, Lone-Eirin Lervåg og Trond Foss

OPPDRAGSGIVER(E)

Statens vegvesen Vegdirektoratet

RAPPORTNR.	GRADERING	OPPDRAGSGIVERS REF.	
SINTEF A10670	Åpen	Marianne Stølan Rostoft	
GRADER. DENNE SIDE	ISBN	PROSJEKTNR.	ANTALL SIDER OG BILAG
Åpen	987-82-14-04890-2	50373700	86 + vedlegg
ELEKTRONISK ARKIVKODE		PROSJEKTLEDER (NAVN, SIGN.)	VERIFISERT AV (NAVN, SIGN.)
A10670 Personvern i intelligente transportsystem 2010.docx		Liv Øvstedal Liv Øvstedal	Dag Bertelsen Dag Bertelsen
ARKIVKODE	DATO	GODKJENT AV (NAVN, STILLING, SIGN.)	
503737.03	2010-11-02	Ragnhild Wahl, forskningssjef Ragnhild Wahl	

SAMMENDRAG

Rapporten belyser mulige konflikter mellom målene i Personopplysningsloven og bruk av ITS-løsninger for å oppnå vegmyndighetenes mål om en sikker og effektiv transport på veg. Dette er ett av flere tema i et prosjekt SINTEF gjennomfører som del av Statens vegvesens etatsprosjekt om personvern og trafikk.

Den første delen av rapporten beskriver ulike ITS-løsninger i vegtransportsystemet ut fra hva slags personopplysninger som benyttes, hvem det blir samlet inn personopplysninger om, hvordan disse behandles og hvem som er behandlingsansvarlige og databehandlere. De fleste bruksområdene involverer ulike teknologier og mange aktører. Det er også innenfor samvirkende system man forventer de største positive effektene av ITS-løsninger på effektivitet og sikkerhet på veiene. Dette gjør det imidlertid vanskelig å komme fram til en enkel klassifisering som grunnlag for risikovurdering.

Deretter presenteres risikovurdering av behandlingen av personopplysninger for et utvalg bruksområder: Automatisk nummerskiltgjenkjenning, sporing av kjøretøy, lokasjonsbaserte tjenester og intelligente fartstilpasningssystem. Dette er bruksområder der personvernimplikasjonene er vurdert som vesentlige, men av forskjellig karakter.

Den siste delen av rapporten beskriver ulike personvernfremmende teknologier (privacy enhanching technologies/PET) og hvordan disse kan benyttes i transportsektoren for å bidra til en forsvarlig behandling av personopplysninger fra trafikantene.

STIKKORD	NORSK	ENGELSK
GRUPPE 1	Samferdsel	Transport
GRUPPE 2	Transportpolitikk	Transport policy
EGENVALGTE	Personvern	Privacy protection
	Intelligente transportsystem	Intelligent Transport Systems

Forord

Denne rapporten belyser problemstillinger knyttet til personvernet i intelligente transportsystem. Dette er et av flere tema som inngår i et prosjekt SINTEF gjennomfører som del av Statens vegvesens etatsprosjekt Personvern og trafikk. Kontaktpersoner hos Statens vegvesen har vært Marianne Stølan Rostoft og Kjersti Bakken i Vegdirektoratet. Det er opprettet en referansegruppe for Statens vegvesens etatsprosjekt med følgende deltakere:

Sveinung Stangeland, Politidirektoratet

Hågen Thomas Ljøgodt / Rune Vidar Bråthen, Datatilsynet

Mona Høegh Amundsen, DSB

Christine Hafskjold, Teknologirådet

Tore Vaaje, Gjensidige Forsikring

Bård Morten Johansen, Trygg Trafikk

Vi takker for nyttige innspill underveis i prosjektet. SINTEF-prosjektet består av tre delprosjekt der ulike sider ved personopplysninger i trafikk belyses. Prosjektleder hos SINTEF var Trond Foss i perioden 2008 – juni 2009 og Liv Øvstedal i perioden juli 2009 – 2010. I tillegg har prosjektgruppa hos SINTEF bestått av prosjektmedarbeidere Lone-Eirin Lervåg og Solveig Meland, med god støtte fra faglige rådgivere Lillian Fjerdingen (til 2009) og Martin Gilje Jaatun.

Trondheim, november 2010

Ragnhild Wahl

Ragnhild Wahl

Forskningssjef

INNHOLDSFORTEGNELSE

Ord og uttrykk

Nedenfor presenteres noen forkortelser, ord og uttrykk som benyttes i rapporten.

ASA	Automatisk fartstilpasningssystem, synonymt med ISA.
ATK	Automatisk trafikkontroll (i punkt eller på strekning).
Automatisk nummerskiltgjenkjenning	Automatisk kameraovervåking (foto eller video) der bilder av registreringsskiltet sjekkes mot en database.
AutoPASS	AutoPASS betegner et system for elektronisk betaling i bomstasjoner basert på kommunikasjon mellom en RFID-brikke i kjøretøyet og veikantutstyr. Statens vegvesen eier AutoPASS-brikkene og tilhørende utstyr i Norge.
Behandlingsansvarlig	Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.
eCall	eCall er et system for automatisk varsling av trafikkulykker, eksempelvis basert på at utløsing av kollisjonsputene automatisk aktiverer dataoverføring om bilens posisjon til en alarmsentral.
GPRS	General Packet Radio Service er en standard for trådløs dataoverføring med mobilkommunikasjon over GSM mobiltelefonnettet.
GPS	Global Positioning System, fastsettelse av geografisk posisjon ved hjelp av et satellittnettverk.
IKT	Informasjons- og kommunikasjonsteknologi
Interoperabilitet	Betegner at ulike system kan fungere sammen og kommunisere med hverandre.
ISA	Intelligent fartstilpasningssystem, synonymt med ASA
ITS	Intelligente transportsystem; system og tjenester der informasjons- og kommunikasjonsteknologi anvendes i transportmiddel eller nettverk som frakter personer eller gods.
Lokasjonsbaserte tjenester	Lokasjonsbaserte tjenester er informasjons- og underholdningstjenester basert på muligheten for å bestemme den geografiske posisjonen til en person eller et objekt, tilgjengelig på pc eller mobile enheter. Eksempler kan være tjenester som oppdager nærmeste minibank, lokasjonen til en venn, eller rutetider som gjelder for den holdeplassen du står på.
Lokasjonsopplysninger	Opplysninger om posisjon (tid og sted).
OBD-II	On-board Diagnostics System (i kjøretøy) er system der den innebygde elektronikken i kjøretøyet kan diagnostisere om kjøretøyet har behov for reparasjon, slik at bileier eller verksted kan få tilgang til informasjonen.
Personopplysning	Opplysninger og vurderinger som kan knyttes til en enkeltperson.
PET	Privacy enhancing technology; personvernfremmende teknologi
RFID	Radiofrekvensidentifikasjon
Tiltrodd tredjepart	En tiltrodd tredjeparter en aktør som yter sikkerhetstjenester

	(nøkkelhåndtering etc.), og som er formelt og kommersielt uavhengig av alle de andre aktørene i systemet.
VADIS	Vehicle and Driver Inspection system; Statens vegvesens kontrollsystem for utekontroller
WIM-teknologi	Weighing in motion; automatisk veiing av kjøretøy i fart.

Sammendrag

Intelligente transportsystem (ITS) forventes å bidra vesentlig til transportpolitiske mål i Nasjonal transportplan om et sikkert, effektivt, miljøvennlig og tilgjengelig transportsystem for alle. De bidrar til effektive løsninger innenfor områder som trafikantinformasjon, trafikk- og flåtestyring, førerstøttesystem, navigasjon, overvåking og kontroll, drift av infrastruktur og betalingssystem. Felles for ITS-løsningene er at de baserer seg på elektronisk innsamling og bruk av data. Rapporten belyser mulige konflikter mellom de nye teknologiske mulighetene ITS -løsningene representerer og målene i personopplysningsloven. Dette er ett av flere tema i et prosjekt SINTEF gjennomfører som del av Statens vegvesens etatsprosjekt om personvern og trafikk.

Den første delen av rapporten beskriver et utvalg ITS-løsninger i vegtransportsystemet, der vi identifiserer vesentlige faktorer for personvernet: Hva slags personopplysninger registreres, om hvem, hvordan behandles disse, og hvem er behandlingsansvarlig og databehandlere. De fleste personopplysninger som registreres i veitransporten er ikke sensitive, men helseopplysninger og mistanke om straffbare forhold er aktuelle for noen anvendelser (eCall, alkolås, automatisk trafikkontroll, intelligente fartstilpasningssystem osv.) Personopplysninger som registreres kan ha konsekvenser for personlig økonomi. Noen opplysninger er i seg selv relativt uskyldige, men omfanget av registreringene kan oppleves å true den enkeltes privatliv og integritet. Data om tid og sted (posisjon) registreres i passeringssnitt (automatisk trafikkontroll, automatisk nummerskilt-gjenkjenning, elektronisk betaling i bomstasjoner) eller kontinuerlig (lokasjonsbaserte tjenester, sporing av kjøretøy, flåtestyring osv.). Andre løsninger kan oppleves nærgående fordi de i tillegg registrerer atferd (kameraovervåking, registrering av data i bilen, intelligente fartstilpasnings-system) og fordi man ikke nødvendigvis er klar over at man blir registrert. Flere ITS-løsninger involverer ulike teknologier og mange aktører, og kan anvendes på forskjellige måter som i ulik grad involverer personopplysninger. Gjennomgangen viste at det var vanskelig å finne fellestrekk som kjennetegner hvilke system som kommer i konflikter med Personopplysningsloven.

Dette viser at både utformingen av det intelligente transportsystemet og hvordan vi bruker teknologien kan være avgjørende for risikonivået. Slike system representerer en infrastruktur for registrering som kan bli brukt på andre måter og av andre aktører i framtida. Derfor fastslår regjeringen i Nasjonal transportplan at personvernhensyn skal være *premiss* for planlegging, utforming og videreutvikling av informasjonssystemene i transportsektoren, slik at mulighetene for misbruk av personinformasjon reduseres eller elimineres.

Den enkelte virksomhet har ansvar for hvordan de tar i bruk ITS-løsninger, med krav om å gjennomføre *vurdering av konsekvensene* for personvernet før teknologien tas i bruk. Lagring av personopplysninger innebærer en viss risiko for at opplysningene kan komme på avveie eller benyttes på en annen måte enn tiltenkt. Virksomheten må vurdere om formålet med tiltaket kan oppnås med mindre omfattende eller ingen personopplysninger. Dette innebærer også organisatoriske og tekniske rutiner for å unngå å registrere personopplysninger som ikke er strengt tatt nødvendige, at opplysningene ikke registreres flere steder enn nødvendig, at tilgangen til registre begrenses og at opplysningene slettes så snart som mulig. Videre må virksomheten vurdere om tiltaket har grunnlag i lov eller bygger på samtykke av den registrerte, om den registrerte har tilstrekkelig informasjon, og om det vil ha konsekvenser for den registrerte å nekte å oppgi opplysninger osv. Når dette er kartlagt må formålet med tiltaket veies i forhold til konsekvensene for personvernet.

Den enkelte virksomhet har ansvar for en forsvarlig behandling av personopplysningene. For å opprettholde et akseptabelt risikonivå er det nødvendig å gjennomføre tiltak på grunnlag av gjentatte risikovurderinger for den aktuelle virksomheten og anvendelsen. En *risikovurdering* av behandlingen av personopplysninger beskriver først og fremst datasikkerheten – sikkerheten for at dataene er riktige, tilstrekkelige og tilgjengelige for behandling når de skal være det, samtidig som de er sikret mot innsyn, kopiering eller endring av personer som ikke skal ha tilgang til

informasjonene. En risikovurdering tar utgangspunkt i de *opplysningene* som blir behandlet, peker på mulige *uønskede* hendelser, *sannsynligheten* for uønskede hendelser og *konsekvensene* hvis disse hendelsene skjer. En vurdering av sannsynlighet og konsekvens gir resulterende *risikonivå*. Dersom resulterende risikonivå er høyere enn akseptabelt risikonivå må det gjennomføres tiltak for å opprettholde akseptabelt risikonivå.

Den neste delen av rapporten presenterer risikovurdering for noen bruksområder der personvernimplikasjonene ble vurdert å kunne være vesentlige, men av forskjellig karakter. Automatisk nummerskiltgjenkjenning, sporing av kjøretøy og lokasjonsbaserte tjenester handler på forskjellig vis om når en person, eller en gjenstand som knyttes til en person, har vært hvor. Intelligente fartstilpasningssystem som innebærer lagring av data, forteller i tillegg noe om atferden til personen. Gjennomgangen av hendelser, konsekvens og sannsynlighet bekrefter at intelligente transportsystem medfører utfordringer for personvernet. For de vurderte bruksområdene bidrar flere identifiserte hendelser til potensielt høy risiko; at informasjon blir utlevert til uvedkommende, at det innhentes flere opplysninger enn nødvendig, eller at data er ikke tilgjengelig slik at den som er registrert selv kan kontrollere opplysningene. For sporing av kjøretøy og intelligente fartstilpasningssystem med lagring av data, er det også identifisert en risiko for at informasjonen ikke slettes så snart som mulig. For intelligente fartstilpasningssystem med datalagring, er det i tillegg identifisert en potensiell risiko for at informasjon formidles mellom tjenesteleverandører. For disse områdene vil det være behov for tiltak for å opprettholde akseptabelt risikonivå.

Den siste delen av rapporten beskriver personvernfremmende teknologier (privacy enhancing technologies, PET) som transportsektoren kan benytte for å bidra til forsvarlig behandling av personopplysninger fra trafikantene. Dette er teknologiske og organisatoriske tiltak som begrenser andres mulighet til å identifisere den enkelte og til å sammenstille mye data om en person. Utgangspunktet er rutiner for dataminimering; unngå å registrere personopplysninger, unngå å lagre data, lagre opplysninger på færrest mulig steder, samt sletterutiner for tidligst mulig sletting av data. *Anonymisering* er teknologier der hensikten er at informasjonen ikke kan knyttes til en bestemt person. Automatiske sletterutiner er sentralt, for å sikre at lagrede data anonymiseres for statistikkformål eller fjernes, når behovet for å knytte opplysningene til person ikke lenger er til stede. Graden av *pseudonymisering* avhenger av innsatsen som kreves for å koble person og data. *Autentisering* verifiserer at du er den du oppgir å være, basert på noe man vet (passord, pin-kode), har (legitimasjon, smartkort) eller er (biometri). *Tilgangsforvaltning* begrenser tilgang til opplysninger ut fra behov, og inkluderer teknikker for å loggføre at databehandling er i samsvar med forutsetningene. *Kryptering* kan benyttes for alle disse løsningene.

ITS-løsninger gir trafikantene store fordeler med hensyn til komfort, effektivitet og sikkerhet, og løsningene vil i mange tilfeller tas godt i mot av brukerne. Sterke drivkrefter bidrar til utviklingen, både myndigheter, fagmiljø og markedskrefter. Samvirkende system og kobling av ulike registre forventes å ha størst effekt for å nå transportpolitiske mål. Økt bruk av elektronisk registrering og lagring av data gjør at det samles inn store mengder data i forbindelse med transport. Dette kan stimulere aktører til å benytte eller dele data til andre formål enn det som opprinnelig var tenkt, noe som ikke er forenlig med målene i Personopplysningsloven. Samtidig er det vanskelig for den enkelte trafikant å skaffe seg oversikt over omfanget av persondata som behandles, samt risiko og konsekvenser knyttet til dette.

Gjennomgangen viser at personvern er et fellesgode som ikke reguleres godt av markedskreftene. Dette kan indikere behov for en tydeligere myndighetsrolle. Det er behov for felles retningslinjer, bransjestandarder og krav der transportsektoren sees i sammenheng, slik at kravene står i forhold til hverandre. Innsikt i problemstillingene er viktig for valg og design av løsninger. Det er også slik at man må ha kunnskap om personvernfremmende teknologier og bruke dem riktig, for å oppnå ønsket effekt. Tekniske muligheter må balanseres mot personvernhensyn, og debatten må holdes levende og bygge på en samlet vurdering av ulike samfunnseffekter.

Summary

A safe, efficient, sustainable transport system accessible for all, are main goals for the National transport plan (white paper). Intelligent transport systems (ITS) are expected to contribute substantially towards these goals. ITS brings forward efficient solutions for transport information, payment systems, traffic monitoring, transport fleet monitoring, driver support systems, and management of infrastructure. Common for ITS solutions is that they are based on electronic collection and use of data.

These new technological possibilities with increasing data collection and storing also raise challenges. This report looks at possible conflicts between the opportunities ITS represents and the aim of protecting personal data as presented in national and international privacy protection laws. This is one of three reports SINTEF conduct as part of the National Public Roads Authorities programme on privacy protection in transport.

The first part of the report describes a selection of ITS solutions in road transport, identifying central factors for privacy protection: Who do we collect data about, what kind of personal data are collected, how they are processed and by whom, and which enterprise is in charge. Most data collected are not sensitive, but may have consequences for private economy. Health data and suspicion on criminal offence may be included for some solutions (eCall, alcohol lock, automatic traffic control, intelligent speed adapters etc.). Several ITS solutions track where you are when, and the amount of these data may threat the private sphere (automatic traffic control, automatic number plate recognition, electronic toll payment, services based on location data, transport fleet monitoring and vehicle tracking). Other solutions feel intruding because data on behaviour is registered as well (camera surveillance, electronic data storing in vehicle, intelligent speed adapters) and because the person not necessarily is aware of being monitored. Several of the ITS solutions include different application areas, technologies and actors, and the implications for privacy protection vary between different applications. Therefore it is difficult to range the different ITS solutions according to the risk they may represent of intruding privacy.

Since the actual application rather than the ITS solution in itself is decisive for the kind of risk it represents, it is important to consider the risks the actual application presents in selecting and designing the ITS-solution. When applying a new tool this is the responsibility of each enterprise. On national level this is a responsibility for planning, designing and development of information systems in the transport sector.

The next part of the report presents risk assessments of some ITS solutions. Since we where not able to categorize ITS solutions according to risk, we selected applications were privacy implications, in different ways, seem likely. Automatic number plate recognition, vehicle tracking, and services based on location data, register when a person or a car is where (location), and for intelligent speed adapters with data storage data on behaviour is processed as well.

A risk assessment looks into the incidents that may happen, the likelihood of these incidents, and the consequences for privacy. This assesses the processing of personal data in the system, which data to collect needs to be assessed at an earlier stage. This review of incidents, probability and consequences confirms that ITS solutions cause challenges to privacy protection. For all four applications the following incidents cause potential risks; information revealed to unauthorized persons, collecting more data than necessary, and data not available for control for the person being registered. For vehicle tracking and intelligent speed adapters with data storage, there is also a risk of data not being deleted as soon as possible. Passing on information between different service providers, is another identified possible misuse. To maintain acceptable risk levels, repeated risk assessments should lead to implementing tailored measures.

The last part of the report describe privacy enhancing technologies, which is one of the strategies the transport sector may apply to contribute to responsible processing of personal data. These are technological and organizational measures aiming at data minimizing, limiting the possibility for others to identify an individual, and to access much data about an individual. Depersonalized data, authentication, authorization, and encryption techniques are briefly described.

ITS solutions benefit the travellers and are mostly well appreciated, contributing to better comfort, efficiency and safety. There are several strong drivers for implementing more and new solutions; authorities, research community, and marked. Cooperative systems involving several registers, is expected to contribute most effective towards transport policy goals. The increase in electronic data collection and storage provides a dilemma for privacy protection.

Privacy protection and privacy enhancing technologies are common goods, which are not well regulated by the marked. This may indicate that authorities need to take responsibility. Within the transport sector there is a need for information, insight and training, and for the harmonisation of requirements and practices. Technological possibilities need to be balanced against the concern of privacy protection, and the debate must be kept alive considering effects on the different aspects of society.

1 Bakgrunn

Denne rapporten handler om bruk av personopplysninger i intelligente transportsystem (ITS). Forhold som drøftes er om personopplysninger behandles, i tilfelle hvilke og hvordan, og hvordan dette kan utgjøre en risiko for personvernet. Vi presenterer risikovurdering av behandlingen av personopplysninger for noen anvendelser av ITS. Vi beskriver også personvernfremmende teknologier som kan bidra til å redusere risikonivået.

Dette kapittelet gir en innføring i bakgrunnen for problemstillingen gjennom å beskrive hvordan ITS spiller en viktig rolle i veisektoren, samt å presentere hovedtrekkene i Personopplysningsloven. Vi beskriver en rekke ITS-anvendelser og mulige bruksområder i kapittel 2 og presenterer risikovurdering av behandlingen av personopplysninger for noen av disse i kapittel 3. Kapittel 4 presenterer personvernfremmende teknologier og noen muligheter dette gir innenfor transportsektoren, mens kapittel 5 oppsummerer noen hovedpunkter.

1.1 Rapporten inngår i etatsprosjektet Personvern og trafikk

Rapporten dokumenterer én av flere aktiviteter i Statens vegvesens etatsprosjekt om personvern. Personvern og trafikk er et 3-årig forsknings- og utviklingsprosjekt i Statens vegvesen der hensikten er å utvide kunnskapen om problemstillinger knyttet til personvern innenfor transportsektoren. Etatsprosjektet belyser gjennom ulike problemstillinger hvordan anvendelse av informasjons- og kommunikasjonsteknologi (IKT) i transportsystemet kan generere nye muligheter for konflikter mellom målene i Personopplysningsloven og veimyndighetenes mål om en sikker og effektiv transport på vei. Statens vegvesen ønsker å bidra til at samferdselsmyndigheter oppnår mer kunnskap om grensesnittet mellom personvern og trafikk, slik at eventuelle konflikter håndteres lettere. SINTEF, TØI og IRIS er engasjert til å belyse ulike problemstillinger innenfor etatsprosjektet.

I prosjektet SINTEF gjennomfører for Statens vegvesen innenfor etatsprosjektet, belyser vi tre tema: Den første rapporten (Øvstedal 2009) handler om hvordan personopplysninger behandles innenfor ulike transportområder i dag, og om det er forskjeller mellom transportformene. Denne rapporten handler om behandling av personopplysninger i intelligente transportsystem. Det tredje temaet vi tar opp er hvordan kunder og brukere (trafikanter) oppfatter den personlige integriteten i transport (rapporten utgis senere).

Mange transportsystem er avhengige av IKT for å fungere sikkert og effektivt, der informasjonssikkerheten må være tilfredsstillende mht. konfidensialitet, integritet og tilgjengelighet. I noen system vil informasjonen som behandles omfatte opplysninger som kan knyttes til et bestemt individ. Med behandling menes innsamling, registrering, sammenstilling, lagring og utlevering, eller en kombinasjon av slike bruksmåter. Personopplysninger innhentes på mange måter innenfor alle transportformer. Formålet kan være sikkerhet, trygghet (security), effektivitet, lønnsomhet, eller bedre tilbud og informasjon til trafikantene.

IKT kan bidra positivt til flere transportpolitiske mål som bedre sikkerhet, mer miljøvennlig transport og effektive trafikkløsninger. Det utvikles teknologibaserte system for kontroll, overvåking og styring av transportsystem og kjøretøy som kan gi oss informasjon automatisk. Økt innsamling av informasjon kan imidlertid brukes til sporing og overvåking av personer, noe som kan utgjøre en trussel for personvernet, og den teknologiske utviklingen går fort. Både i forhold til lover, forskrifter og organisering kan det være en utfordring for samfunnet å henge med og å være ”føre var”. Hovedmålet med behandlingen av informasjon som kan knyttes til et individ kan være

å redusere risikoen i transportsystemet, men en konsekvens kan være at man kommer i konflikt med kravene i Personopplysningsloven og i forskriftene. Med risiko menes her ikke bare risikoen for en hendelse som medfører fare for trafikantenes liv og helse, men også risiko for hendelser som kan påføre trafikantene økonomiske tap eller krenkelse av personvernet.

1.2 Målsetting

I *denne rapporten* er temaet risikovurdering av behandlingen av personopplysninger i intelligente transportsystem (ITS), i forhold til hvilke personopplysninger som behandles, og hvordan de behandles. Rapporten har som mål å beskrive:

- Hvordan anvendelse av IKT i transportsystem (begrenset til veisektoren) kan generere nye muligheter for konflikter mellom målene i Personopplysningsloven og dens forskrifter, og veimyndighetenes mål om en sikker og effektiv transport på vei.
- En risikovurdering av de anvendelser av IKT i transportsystem som skaper de største konfliktene mellom lovens og forskriftenes mål og veimyndighetenes mål.

Prosjektet SINTEF gjennomfører har en bredere problemstilling. I *andre deler* av prosjektet som rapporteres for seg, belyses temaene behandling av personopplysninger i transportsektoren og brukernes aksept av tiltak:

- På hvilken måte behandles opplysninger som kan knyttes til et enkeltindivid i de ulike transportsystemene i dag, og finnes det vesentlige ulikheter innenfor ulike transportmodi og driftsorganisasjoner?
- Hva er akseptabelt risikonivå sett fra myndighetene, eiere og drivere av transportsystem, og fra kundene og forbrukernes side?
- Hva er forholdet mellom vurdert risiko og akseptabel risiko? Hvilke tiltak kan være aktuelle for å kompensere for eventuelle avvik mellom vurdert og akseptabelt risikonivå?

1.3 Anvendelse av intelligente transportsystem i transportsektoren

Samferdselsområdet er preget av rask teknologisk utvikling på mange felt, og det har etter hvert blitt et sterkt fokus på intelligente transportsystem (ITS) som virkemiddel for å oppnå sikrere, mer effektiv og komfortabel transport.

> *Begrepet ITS brukes om system og tjenester hvor informasjons- og kommunikasjonsteknologi anvendes i transportmiddel eller nettverk som frakter personer eller gods (Bang og Wahl 2007).*

Det foregår allerede en utstrakt bruk av slike system innenfor transportsektoren, blant annet for å styre og overvåke trafikk. ITS kan grupperes i seks sentrale anvendelsesområder; trafikantinformasjon, trafikk- og flåtestyring, førerstøttesystem og navigasjon, overvåking og kontroll, drift av infrastruktur og betalingssystem (Bang og Wahl 2007). Disse er gjengitt i figuren nedenfor, hvor de vertikale båsene kategoriserer systemene i anvendelsesområder, mens de horisontale linjene illustrerer noen viktige grunnsteiner for ITS-løsninger.

Figur 1: Anvendelsesområder for ITS-løsninger (kilde: Bang og Wahl 2007).

Sterke drivkrefter

ITS anses å ha et betydelig urealisert potensial med tanke på å løse mange av utfordringene vi står overfor i transportsektoren i dag. Bak utviklingen av nye teknologiske løsninger, finner vi sterke drivkrefter, deriblant EU-kommisjonen, myndighetene, Statens vegvesen og befolkningen generelt.

EU-kommisjonen har gjennom mange år gitt betydelig økonomisk støtte til forskning, utredning og innføring av ITS. I desember 2008 presenterte kommisjonen ITS Handlingsplan for 2009-2014, samt forslag til direktiv som skal forplikte medlemslandene til oppfølging av politikken (ITS Action Plan). Handlingsplanen trekker opp prioriteringer og satsingsområder for årene framover, og målet med planen er å akselerere og koordinere utnyttelse av ITS på veitransportområdet og for grenseflater med andre transportformer. Planen trekker frem seks satsingsområder med tilhørende tiltak, hvor to av satsingsområdene er: *Optimere bruk av vei-, trafikk- og reiseinformasjon* og *Datasikkerhet og personvern* (se ***Tabell 1*** på neste side).

Samferdselsdepartementet la i 2010 fram en overordnet ITS-strategi for transportsektoren i Norge, der alle transportformer inkluderes. Nasjonal Transportplan for perioden 2010-2018 spår at den teknologiske utviklingen og økt satsing på ITS vil bidra til store endringer i transportsektoren i årene framover. Med riktig anvendelse av de teknologiske mulighetene, vil ITS gi et verdifullt bidrag til å nå de transportpolitiske målene i Nasjonal Transportplan med hensyn til framkommelighet, sikkerhet, miljø og universell utforming (Stortingsmelding nr 16 2008-2009, Wahl m.fl. 2007).

Statens vegvesens strategi for ITS bygger på de transportpolitiske målene i Nasjonal Transportplan. Følgende visjon for ITS i det veibaserte transportsystemet er formulert (Statens vegvesen 2007):

> *Statens vegvesen skal gjennom målrettet bruk av ITS bidra til å unngå alvorlig skade på mennesker eller miljø som følge av transport. Vegtrafikksystemet skal være forutsigbart og tilgjengelig for alle.*

Videre er det utarbeidet en handlingsplan (Statens vegvesen 2010) som innebærer utvikling av infrastruktur for å kunne ta i bruk ITS, utvikling av ITS-tjenester mot 2013 og omfattende styring av transportsystemet ved bruk av ITS mot 2019. Eksempler på løsninger som ønskes tatt i bruk er automatisk trafikkontroll på strekninger (streknings-ATK), intelligente fartstilpassere (ISA)[1],

[1] På norsk brukes intelligent fartstilpasning (ISA) og automatisk fartstilpasning (ASA) synonymt.

alkolås, sanntidsinformasjon om reisetider og kjøreforhold, samordnede betalingsløsninger og intelligente ”park and ride”-løsninger.

Tabell 1: ITS Handlingsplan for 2009-2014 fra EU-kommisjonen (kilde: ITS Norge 2009)

1. Optimere bruk av veg-, trafikk- og reiseinformasjon (data)
a) Fremskaffe trafikkinformasjonstjenester fra privat sektor b) Fremskaffe trafikkavviklingsinformasjon (traffic regulation data) fra transportmyndighetene c) Garantere offentlige myndigheters tilgang til sikkerhetsrelatert informasjon innsamlet av private firmaer d) Garantere private selskapers tilgang til relevante offentlige data e) Optimere fangst og tilgjengelighet av vegnetts- og fremkommelighetsdata f) Spesifisere data og prosedyrer for minimum, gratis trafikkinformasjonstjenester g) Fremme utvikling av nasjonale, multimodale reiseplanleggere
2. Kontinuitet av tjenester for persontrafikk- og godsstyring i europeiske korridorer og sammenhengende byområder.
a) Spesifisere standarder for dør-til-dør informasjonsflyt, trafikkstyring, reiseplanlegging og hendelseshåndtering b) Støtte godstransport med eFreight og bruk av gods-sporing med RFID og EGNOS/GALILEO posisjonsbestemmelse. c) Støtte bred utnyttelse av en oppdatert europeisk ITS rammearkitektur og utvikling av en ITS rammearkitektur for transportmobilitet i by, inkludert en samordnet tilnærming til reiseplanlegging, transportetterspørsel, trafikkstyring, trafikkberedskap, vegprising og bruk av parkering og offentlige transportanlegg (transport facilities) d) Implementering av interoperabilitet for elektroniske bompengesystemer
3. Trafikksikkerhet og samfunnssikkerhet (security) på veg
a) Fremme utnyttelse/utbredelse av avanserte førerstøttesystemer og sikkerhetsrelatert ITS, inkludert at de fabrikkinstalleres i nye biler (etter typegodkjenning) og om relevant; ettermonteres. b) Støtte til innføring av eCall c) Utvikling av regelverk for trygge brukergrensesnitt og integrering av flyttbare enheter d) Utvikling av passende tiltak, inkludert ”best praksis” veiledere for ITS rettet mot sårbare trafikantgrupper e) Utvikling av passende tiltak, inkludert ”best praksis” veiledere for sikre parkeringsplasser for lastebiler og næringstransport og telematikkbaserte parkerings- og reserveringssystemer
4. Kobling (integration) av kjøretøyene til transportinfrastrukturen
a) Etablering av arkitektur for en åpen kjøretøybasert tjenesteplattform for ITS, inkludert standard grensesnitt b) Utvikling og evaluering av samvirkende systemer (cooperative systems) c) Spesifikasjon av kommunikasjon bil-vegkant, bil-bil og vegkant-vegkant for samvirkende systemer d) Definisjon av et mandat for europeiske standardiseringsorganisasjoner for å utvikle harmoniserte standarder for ITS, spesielt for samvirkende systemer
5. Datasikkerhet og personvern
a) Vurdere sikkerhets- og personvernaspekter relatert til behandling av data for ITS og foreslå tiltak i full overensstemmelse med Fellesskapets lovgivning b) Behandle ansvarsforhold tilhørende til bruken av ITS anvendelser og spesielt førerstøtte og kjøretøybaserte systemer.
6. Europeisk samarbeid og koordinering
a) Forslag om et juridisk rammeverk for koordinert utnyttelse av ITS i hele Europa b) Utvikling av en verktøykasse for beslutningstøtte for investering i ITS anvendelser og tjenester c) Utvikling av retningslinjer (guidelines) for offentlig finansieringsbidrag fra EU og nasjonale kilder til ITS, utstyr og tjenester d) Etablering av spesiell ITS samarbeidsplattform for medlemslandene og regionale/lokale politiske myndigheter for å fremme initiativer for ITS på området by-mobilitet.

ITS baserer seg på innsamling, tilrettelegging og formidling av data i elektronisk form. Den voldsomme utviklingen av teknologiske løsninger og økt utbredelse av ITS i samfunnet, medfører nye muligheter for registrering, sporing og lagring av data om reisende. Dette gir nye utfordringer og problemstillinger med hensyn til personvern og individets frihet.

I en intervjuundersøkelse gjennomført av Bjørnskau m.fl. (2007) pekte flere aktører, deriblant Datatilsynet, ut veisektoren som den transportgrenen som har valgt løsninger med størst kapasitet for lagring av informasjon om reisende.

Brukeraksept

Det synes å være bred aksept for behandling av personopplysninger i tilknytning til intelligente transportsystem. Flere undersøkelser viser at det er liten motstand mot bruk av ITS, når dette bidrar til at man oppnår individuelle fordeler, som forbedret trafikkinformasjon, bedre trafikkflyt og mer effektive betalingsløsninger. Befolkningen er mer reservert overfor tiltak som medfører kollektive fordeler som for eksempel økt trafikksikkerhet. Størst skepsis er knyttet til løsninger som har til hensikt å håndheve fartsovertredelser og registreringer på bakgrunn av kommersielle interesser (Ravlum 2004).

Det finnes mange eksempler på at trafikanter er villig til å la myndigheter og andre få opplysninger om seg selv, dersom dette gjør at de oppnår fordeler. Bilførere med intelligent fartstilpasser (ISA) og atferdsregistrator godtar at data om deres atferd og reisemønster blir registrert, mot at de selv oppnår billigere forsikringspremie (Bjørnskau m.fl. 2007, Berg m.fl. 2008). Slike eksempler kan vi også finne innenfor bomveisystem og elektroniske betalingstjenester, hvor den reisende godtar behandling av personopplysninger fordi det gjør reisen billigere, mer effektiv eller komfortabel for den enkelte trafikant.

Bjørnskau m.fl. (2007) viser også til norske og europeiske undersøkelser som viser at kameraovervåkning på offentlige steder har generell høy aksept i befolkningen.

1.4 Personopplysningsloven

Behandling av personopplysninger er i Norge regulert gjennom Personopplysningsloven og tilhørende forskrifter, samt det europeiske direktivet:

- LOV 2000-04-14 nr 31: Lov om behandling av personopplysninger (Personopplysningsloven)
- FOR 2000-12-15 nr 1265: Forskrift om behandling av personopplysninger (Personopplysningsforskriften)
- Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og fri utveksling av slike opplysninger (Personverndirektivet EU-direktiv 95/46/EF).
- Konvensjonen om beskyttelse av menneskerettighetene og de grunnleggende friheter, Roma 1950 (Den europeiske menneskerettskonvensjonen)

Personopplysningsloven gjelder for behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler, og annen behandling av personopplysninger når disse inngår eller skal inngå i et personregister. Loven gjelder ikke behandling av personopplysninger som den enkelte foretar for rent personlige eller andre private formål (§ 3).

Formål

Formålet med loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger (§ 1).

Definisjoner av sentrale begrep

Loven gir en rekke definisjoner av sentrale begrep (§ 2), se tabell 2:

Tabell 2: Definisjon av sentrale begrep i Personopplysningsloven.

Begrep	Definisjon
Personopplysning	*Opplysninger og vurderinger som kan knyttes til en enkeltperson*
Behandling av personopplysninger	*Enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller kombinasjon av slike bruksmåter.*
Personregister	*Registre, fortegnelser m.v. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen.*
Behandlingsansvarlig	*Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.*
Databehandler	*Den som behandler personopplysninger på vegne av den behandlingsansvarlige*
Registrert	*Den som en personopplysning kan knyttes til.*
Samtykke	*En frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv*
Sensitive personopplysninger	*Opplysninger om:* *a) Rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning* *b) At en person har vært mistenkt, siktet, tiltalt eller dømt for straffbar handling* *c) Helseforhold* *d) Seksuelle forhold* *e) Medlemskap i fagforeninger*

Alminnelige regler for behandling av personopplysninger

Hovedprinsippet er at det er lov å samle inn og registrere personopplysninger dersom ett av følgende vilkår er oppfylt (§ 8):

- Den registrerte har gitt samtykke
- Behandling av personopplysninger er hjemlet i særlov
- Det er nødvendig for å

- oppfylle en avtale med den registrerte
- oppfylle en rettslig forpliktelse
- ivareta den registrertes vitale interesser
- utøve en oppgave av allmenn interesse
- utøve offentlig myndighet
- ivareta en berettiget interesse, der hensynet til den registrertes personvern ikke overstiger denne interessen

For sensitive personopplysninger gjelder andre vilkår i tillegg til disse som er nevnt her. Fødselsnummer og andre entydige identifikasjonsmidler kan bare benyttes når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå dette.

Loven definerer noen krav til behandling av personopplysninger i § 11. Den behandlingsansvarlige må sørge for at personopplysninger:

- bare nyttes til uttrykkelig angitte formål som er saklig begrunnet
- ikke brukes til formål som er uforenlig med det opprinnelige formålet, uten at den registrerte samtykker
- er tilstrekkelige og relevante for formålet med behandlingen
- er korrekt og oppdatert, og ikke lagres lenger enn det som er nødvendig

Senere behandling av personopplysningene for historiske, statistiske eller vitenskaplige formål anses ikke uforenlig med de opprinnelige formålene med innsamlingen av opplysningene, dersom samfunnets interesse i at behandlingen finner sted klart overstiger ulempene den kan medføre for den enkelte. Det skal da sørges for at opplysningene ikke lagres på måter som gjør det mulig å identifisere den registrerte lenger enn nødvendig.

Behandlingsansvarlig og databehandler skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. Personopplysninger kan ikke behandles på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige, og opplysningene kan heller ikke uten slik avtale overlates andre for lagring eller bearbeidelse. Den behandlingsansvarlige må påse at det etableres tilstrekkelige rutiner for internkontroll.

Informasjon og rettigheter

Alle har rett til å få vite hva slags behandling av personopplysninger en behandlingsansvarlig foretar. Man kan kreve informasjon om hvem som er behandlingsansvarlig, hvem som har daglig ansvar for å oppfylle den behandlingsansvarliges plikter, formålet med behandlingen, beskrivelser av hvilke personopplysninger som behandles, hvor opplysningene er hentet fra og om (og evt. til hvem) personopplysningene vil bli utlevert.

Den som blir registrert har krav på å få vite hvilke opplysninger om den registrerte som behandles og sikkerhetstiltakene ved behandlingen. Den registrerte har også rett til å kreve manuell behandling av personopplysninger, til å reservere seg mot direkte markedsføring og til retting av mangelfulle personopplysninger. Den registrerte kan kreve at opplysninger som er sterkt belastende skal sperres eller slettes dersom det ikke strider mot annen lov og er forsvarlig ut fra en samlet vurdering av andre behov.

Den behandlingsansvarlige har informasjonsplikt overfor den registrerte, både når det samles inn informasjon fra den registrerte selv, og når det samles inn opplysninger fra andre enn den registrerte. Det finnes enkelte unntak fra retten til informasjon, bl.a. når det gjelder forebygging og etterforskning av straffbare handlinger m.m.

Personopplysningsforskriften

Det foreligger en egen forskrift om behandling av personopplysninger, samt en veileder for risikovurdering av informasjonssystem.

1.5 Personvern – vern om personopplysninger

Hensynet til personvernet er nært knyttet til enkeltindividets behov og muligheter for privatliv, selvbestemmelse (autonomi) og selvutfoldelse (Den europeiske menneskerettskonvensjonen, EUs personverndirektiv 95/46/EF). Personverninteressene kan utrykkes som en rekke hensyn, som dels kan være innbyrdes motstridende:

- Det *integritetsfokuserte personvernet* uttrykker innbyggernes ønske om å ha kontroll over opplysninger om seg selv (informasjonsintegritet) og opprettholde en privatsfære (selvbestemmelse, innsyn og kunnskap). Stikkord er territorial integritet (beskyttelse av individers geografiske territorium), kroppslig integritet, psykisk integritet (selvbilde, ære, omdømme) og kommunikasjonsintegritet (at kommunikasjon ikke overvåkes av utenforstående). Taushetspliktbestemmelser er et eksempel.
- Det *maktfokuserte personvernet* fokuserer på maktbalansen mellom enkeltindividet og offentlige eller private aktører; overdreven markedsmakt, myndighetsutøvelse og arbeidsgivermakt. Tema er bestemmelse over tilgangen til informasjon om egen person, innsyn og kunnskap, borgervennlig forvaltning, forholdsmessig kontroll og overvåking. Automatisk trafikkontroll er et eksempel.
- Det *beslutningsfokuserte personvernet* tar utgangspunkt i at personopplysninger er grunnlag for beslutninger i privat og offentlig virksomhet. For at beslutningene skal være riktige og rettferdige må opplysningene være relevante, tilstrekkelige og korrekte. Dette representerer interesser i innsyn, opplysnings- og behandlingskvalitet, og i brukervennlig og borgervennlig forvaltning. Tildeling av skoleskyss er eksempel på en beslutning som skal bygge på tilstrekkelige og oppdaterte (korrekte) opplysninger.

Type personopplysninger (intime, sensitive, stigmatiserende), omfanget av opplysningene, hvor mange det gjelder og hvordan opplysningene evt. formidles til uvedkommende (risiko for kobling mot andre data) har betydning for konsekvensene av manglende personvern. Det er ikke nødvendigvis de opplysningene loven definerer som sensitive som er de folk flest er opptatt av å beskytte. Hvem det gjelder er også viktig. Undersøkelser viser at flertallet aksepterer mye, mens de som allerede er sårbare grupper i samfunnet er mer skeptiske til registreringer samtidig som de også er mer utsatt for registrering, behandling og påfølgende beslutninger på grunnlag av personopplysninger.

Personvernet veies mot andre formål i hver enkelt sak og situasjon. Et viktig spørsmål er da om man skal basere avveiningen på flertallets aksept eller på sårbare grupper som i størst grad vil oppleve konsekvensene av de beslutningene man tar.

2 Beskrivelse av intelligente transportsystem med personvernimplikasjoner

Dette kapittelet beskriver ulike anvendelser av ITS i veisektoren. Noen system har flere bruksområder og er aktuelle både for offentlige og private aktører. Teknologien som anvendes i systemene er gjerne basert på radiofrekvensidentifikasjon (RFID), lokaliseringsteknologi ved bruk av mobilkommunikasjon og satellittsystem, eller kameraovervåking.

Underveis i arbeidet har vi forsøkt å kategorisere ITS-løsningene gjennom å identifisere noen vesentlige faktorer med hensyn til personverninteresser; hva slags personopplysninger som behandles, hvor i systemet personopplysninger lagres og behandles, personregistre som kan være involvert, hvem som er behandlingsansvarlig og databehandler, samt hvem som blir berørt av løsningen. Gjennomgangen viste at det var vanskelig å finne fellestrekk med tanke på hvilke system som utgjør størst risiko for konflikter med Personopplysningsloven. Vi har valgt å beskrive et utvalg uten å gruppere dem, og har begrenset utvalget til system som vi mener kan ha implikasjoner for personvernet.

2.1 Kameraovervåking

Kameraovervåking brukes i stor utstrekning for å overvåke transportsystemet, både med fotografering (fotobokser) og videokamera. Hensikten er som regel å ivareta sikkerheten på offentlige områder, gjennom å hindre at uønskede hendelser oppstår, eller ved etterforskning av straffbare handlinger i etterkant av en hendelse.

Kameraovervåking benyttes blant annet på terminalområder, til overvåking av infrastruktur, om bord i kollektivtransportmidler, og i forbindelse med ulike ITS-løsninger.

Flere busselskaper bruker kameraovervåking på sine kjøretøy for å ivareta sikkerheten til sjåfører og passasjerer. Datatilsynet tillater bruk av kamera i sjåførsonen og ved inngangs-/utgangspartiene, men mener at overvåking av passasjerområdet ikke er forenelig med hensynet til brukernes personvern.

NSB og AS Sporveisbussene har klaget Datatilsynets avgjørelse om ikke å tillate overvåking av publikumsområdene om bord i transportmiddelet, inn for Personvernnemda. Personvernnemda avgjorde at overvåking av passasjerområdene kan tillates, og begrunner dette med at personvernulempene er beskjedne fordi opptakene kun blir avspilt ved mistanke om straffbare forhold. Overvåking av passasjerområdene og avspilling av opptakene krever imidlertid konsesjon (www.datatilsynet.no).

Kameraovervåking brukes også for å identifisere personer/kjøretøy som passerer bomstasjoner uten gyldig betaling (avsnitt 2.5), i forbindelse med automatisk nummerskiltgjenkjenning (avsnitt 2.2) og ved automatisk trafikkontroll (avsnitt 2.3).

Hva slags personopplysninger behandles?

Kameraovervåking resulterer i foto eller videoopptak som muliggjør identifisering av personer, deres atferd, samt hvor de befinner seg på et gitt tidspunkt.

Hvor i systemet lagres og behandles personopplysninger?

Opptakene lagres i fotobokser og videokamera, og lagres og behandles hos den virksomheten som benytter kameraovervåking, eller hos en tredjepart som er satt til å drifte dette (f.eks. et vekterselskap). For noen anvendelser behandles opplysningene hos Statens vegvesen og politiet.

Personregistre som kan være involvert

Kameraovervåking av infrastruktur, ombord i kollektivtransportmidler og på terminalområder involverer vanligvis ikke personregistre. Unntaket er overvåking ved bomstasjoner, trafikkontroll og automatisk nummerskiltgjenkjenning. Disse forholdene er omtalt i egne avsnitt.

Behandlingsansvarlig og databehandler

Foretaket som gjennomfører kameraovervåking er behandlingsansvarlig som bestemmer hvordan personopplysninger skal brukes og håndteres. Eventuelt vekterselskap eller andre som er satt til å drifte systemet og har tilgang til dataene defineres som databehandlere.

Hvem blir berørt?

Kameraovervåking berører alle som beveger seg i det området som blir overvåket. Trafikanten kan selv være uvitende om at overvåking foregår, selv om man plikter å informere om at et område er overvåket.

Videoopptak fra offentlige områder brukes bl.a. til etterforskning av kriminelle handlinger, og vi ser eksempler på at denne type opptak brukes til å etterlyse personer gjennom media.

Tabell 3: Oppsummering av forhold som berører personvern ved kameraovervåking.

Oppsummering: Kameraovervåking	
Type personopplysninger	*Videoopptak som muliggjør identifisering av personer, hvor de befinner seg på et gitt tidspunkt, samt atferd.*
Hvor i systemet lagres og behandles personopplysninger?	*Videoopptak lagres og behandles hos den aktøren som foretar kameraovervåkning, eventuelt hos en tredjepart som er satt til å drifte systemet.*
Personregistre som kan være involvert	*Tradisjonell kameraovervåking av infrastruktur, kollektivtransport eller terminalområde involverer i utgangspunktet ikke personregistre. Unntaket er overvåking i forbindelse med bomstasjoner, automatisk nummerskiltgjenkjenning og ved automatisk trafikkontroll (se eget avsnitt).*
Behandlingsansvarlig	*Aktøren som foretar kameraovervåking er behandlingsansvarlig.*
Databehandler	*Databehandlere kan være selskap som drifter systemet eller håndterer personopplysningene på vegne av behandlingsansvarlig.*
Hvem blir berørt (brukere)?	*Alle som befinner seg i det området som overvåkes berøres av systemet.*

2.2 Automatisk nummerskiltgjenkjenning

Registreringsnummer for kjøretøy brukes til kontroll av trafikk og trafikanter, for eksempel ved passering av bomstasjon, ved fartskontroll og kontroll av betalte avgifter etc. Med automatisk fotografering/kameraovervåking og sjekking mot database, kan denne type kontroller gjennomføres på en effektiv måte.

I Norge er automatisk nummerskiltgjenkjenning blant annet benyttet i parkeringsanlegg. Systemet kan også være aktuelt for betaling og adgangskontroll i miljøsoner (Øvstedal 2009). For å effektivisere kontroll av godstransport (se avsnitt 2.11) er innføring av automatisk nummerskiltgjenkjenning et viktig tiltak. I Storbritannia brukes det i stor utstrekning for å registrere nummerskiltet på passerende biler (Bjørnskau m.fl. 2007). Hensikten er primært å spore opp stjålne kjøretøy, men systemet er også brukt til sporing av annen kriminalitet.

Hva slags personopplysninger behandles?

Ved bruk av automatisk nummerskiltgjenkjenning identifiseres kjøretøy og bileier, og i noen tilfeller registreres kjøretøyets posisjon på et gitt tidspunkt.

Hvor i systemet lagres og behandles personopplysninger?

Hvordan personopplysninger lagres og behandles vil være avhengig av formålet med nummerskiltgjenkjenningen. Ofte vil data måtte lagres både i veikantutstyret (for eksempel fotoboksen) og i et sentralsystem hvor dataene behandles.

Personregistre som kan være involvert

Kjøretøyregisteret benyttes for å identifisere bilens eier og evt. kontaktinformasjon for å sende ut betalingsinformasjon. Dersom løsningen skal brukes til bekjempelse av kriminalitet, f.eks. for å avdekke stjålne kjøretøy, må det involveres egne registre knyttet til dette.

Behandlingsansvarlig og databehandler

Hvem som er behandlingsansvarlig og databehandler vil være avhengig av formålet med registreringen. Dersom automatisk nummerskiltgjenkjenning brukes for å håndheve trafikkregler eller bekjempe kriminalitet, er gjerne myndigheter eller politi behandlingsansvarlig. Private driftsselskap kan være behandlingsansvarlig når systemet brukes for å administrere for eksempel parkering eller betaling i bomstasjoner.

Hvem blir berørt?

De fleste bilister berøres av automatisk nummerskiltgjenkjenning, etter hvert som dette blir en utbredt metode for å overvåke og kontrollere trafikk og trafikanter. I enkelte tilfeller vil det kun være aktuelt å registrere kjøretøy som bryter trafikkreglene (for eksempel passerer bomstasjonene uten å betale eller overskrider fartsgrensen i spesielle målepunkt), men i de fleste tilfeller vil det være aktuelt å gjøre en screening av alle kjøretøy for å plukke ut dem man ønsker å undersøke nærmere.

Tabell 4: Oppsummering av forhold som berører personvern ved automatisk nummerskiltgjenkjenning.

Oppsummering: Automatisk nummerskiltgjenkjenning	
Type personopplysninger	*Identifisering av kjøretøy og eier, samt i enkelte tilfeller også posisjonering av kjøretøy på gitt tidspunkt.*
Hvor i systemet lagres og behandles personopplysninger?	*I veikantutstyr og sentralsystem. Hvordan opplysninger behandles avhenger av formålet med registreringen.*
Personregistre som kan være involvert	*Kjøretøyregisteret, Folkeregisteret, kunderegister. Registre over autoriserte personer eller kjøretøy (adgangskontroll). Eventuelle register over straffbare forhold, for eksempel database med stjålne kjøretøy.*
Behandlingsansvarlig	*Avhengig av formålet med registreringen. Kan være både myndigheter og private aktører.*
Databehandler	
Hvem blir berørt (brukere)?	*De fleste bilister.*

2.3 Automatisk trafikkontroll i punkt eller på strekning

Automatisk trafikkontroll (ATK) brukes til å kontrollere kjørehastighet. Hensikten med systemet er å øke trafikksikkerheten ved å hindre eller redusere antall fartsovertredelser.

Det gjennomføres som et samarbeid mellom politiet og Statens vegvesen, der Statens vegvesen sørger for oppsett og drift av utstyr, samt å sette i gang kontroller etter anmodning fra politiet. Politiet har ansvar for når kontrollene gjennomføres og for å følge opp de straffbare forholdene som blir avdekket.

Figur 2: Fotoboks brukt til automatisk trafikkontroll

ATK har tradisjonelt vært brukt for å måle kjøretøyets hastighet i ett punkt, og bare de som overskrider fartsgrensen er blitt fotografert. I Norge og andre nordiske land blir det tatt bilde av kjøretøyet og bilføreren (der passasjerer sladdes), og bilføreren holdes juridisk ansvarlig[2].

Strekningsbasert ATK innebærer at alle kjøretøyene blir registrert og fotografert i to punkt, der gjennomsnittshastigheten mellom disse punktene gir grunnlag for evt. bøtelegging. Dersom man har overholdt fartsgrensen, slettes dataene umiddelbart. Strekningsbasert ATK er i dag innført på tre strekninger[3] i Norge.

[2] I enkelte land, blant annet Nederland, tas det bilde av kjøretøyets registreringsnummer og bileier holdes ansvarlig. Dette er et enklere system teknisk og med hensyn til personopplysninger, men kan være i strid med folks oppfatning av rettferdighet og rettssikkerhet.

[3] Systemet ble testet ved Lillehammer i forbindelse med nullvisjonsprosjektet. Strekningsbasert ATK er innført på E18 i Bamble og E6 ved Øyer i 2009 (Fornyings- og administrasjonsdepartementet 2009), og på Rv3 i Østerdalen i mai 2010.

Andre eksempler på bruksområder er automatisk overvåking av kollektivfelt, avstand til neste kjøretøy og kjøring mot rødt lys i signalanlegg, men disse benyttes ikke i Norge i dag.

Hva slags personopplysninger behandles?

Automatisk trafikkontroll innebærer identifisering av kjøretøy og fører ved bruk av fotografi, samt registrering av tid, sted og omfang av eventuell trafikkforseelse. Informasjon om straffbare handlinger regnes som sensitive personopplysninger.

Hvor i systemet lagres og behandles personopplysninger?

Personopplysninger lagres lokalt i de enkelte fotoboksene, og behandles hos Vegvesenet og hos politiet. Politiet sender forenklet forelegg i posten til bilens eier. Når boten er vedtatt, innfordres den av Statens Innkrevingssentral (som er underlagt Finansdepartementet).

Personregistre som kan være involvert

Kjøretøyregisteret brukes for å identifisere eier av kjøretøy ved utsendelse av forenklet forelegg. Data fra trafikkontrollene må også samordnes med registeret for prikkbelastning.

Behandlingsansvarlig og databehandler

Statens vegvesen er behandlingsansvarlig. Politiet er databehandler som håndterer personopplysninger.

Hvem er berørt?

I første omgang blir trafikanter som ikke overholder fartsgrensen (eller andre trafikkregler) berørt av tiltaket. Ved streknings-ATK blir det tatt bilde av alle trafikantene, men lagring skjer kun ved overtredelser. Testing av utstyret viser at sletting av data fungerer tilfredsstillende (Fornyings- og administrasjonsdepartementet 2009), men teknisk sett muliggjør systemet en omfattende overvåking av alle trafikanter.

Tabell 5: Oppsummering av forhold som berører personvern ved automatisk trafikkontroll.

Oppsummering: Automatisk trafikkontroll i punkt eller på strekning	
Type personopplysninger	*Identifisering av kjøretøy og fører ved fotografering, registrering av tidspunkt, sted og omfang av eventuelle trafikkforseelser. Mistanke om straffbare handlinger regnes som sensitive personopplysninger.*
Hvor i systemet lagres og behandles personopplysninger?	*Lokalt i veikantutstyret, hos Statens vegvesen og hos politiet.*
Personregistre som kan være involvert	*Kjøretøyregisteret og register for prikkbelastning.*
Behandlingsansvarlig	*Statens vegvesen er behandlingsansvarlig.*
Databehandler	*Politiet er databehandler.*
Hvem blir berørt (brukere)?	*Først og fremst trafikanter som ikke overholder trafikkreglene (fartsgrense). Streknings-ATK vil innebære fotografering av alle kjøretøy som passerer, men lagring vil kun skje ved trafikkforseelser.*

2.4 Elektronisk billettering

Figur 3.: Bruk av kortleser med elektronisk billett (kilde: www.ruter.no)

Elektronisk billettering er tatt i bruk av kollektivselskaper i flere fylker. Systemet fungerer ved at passasjerene har en billett med elektronisk lagret informasjon (Smartkort). Den reisende overfører et beløp til kortets ”konto” i forkant av reisen.

Hensikten med elektroniske billetteringssystem er å oppnå mer effektive salgsprosesser og forenklet administrasjon. Samtidig muliggjør systemet utstrakt registrering og kartlegging av reiseatferd til enkeltpassasjerer. Den reelle faren for at reisedata skal kunne misbrukes, avhenger i stor grad av kollektivselskapenes rutiner for håndtering av disse dataene (St.meld. 16 2008-2009).

Datatilsynet har stilt som krav til elektroniske billetteringssystem at det skal finnes mulighet for å reise anonymt uten at reisemønsteret blir lagret, og dette alternativet skal være lett tilgjengelig. Videre stilles en rekke krav til informasjonssikkerhet og til at passasjerene anonymiseres ved analyser av reisemønster og når betaling for reisen skal deles mellom flere transportører. Videre påpekes det at detaljert logging av reisemønster kun skal skje når kunden aktivt ber om dette selv (Datatilsynet 2007).

Hva slags personopplysninger behandles?

Ved elektronisk billettering registreres navn, adresse og nødvendige kredittopplysninger i et kunderegister, som en del av avtalen mellom kunden og kollektivselskapet. I tillegg registreres nødvendige reiseopplysninger som dato, klokkeslett, rute, holdeplass/sone for påstigning og avstigning. I en intervjuundersøkelse blant aktører i transportbransjen, uttalte kollektivselskap at

de hadde ønske om også å benytte personnummer for å sikre at faktura sendes til korrekt mottaker (Øvstedal 2009).

Hvor i systemet lagres og behandles personopplysninger?

Informasjon om navn, adresse og kredittopplysninger lagres i et kunderegister hos kollektivselskapet eller et administrasjonsselskap. Reiseopplysninger som dato, klokkeslett, rute og påstigning/avstigning lagres på kortet og i en sentral database hos kollektivselskapet/administrasjonsselskapet. Flere selskap ønsker også å tilby den reisende en oversikt over tidligere reiser på internett (”min side”).

Hvor lenge de registrerte opplysningene lagres, varierer noe for de ulike billetteringssystemene. Hos enkelte selskap slettes dataene som er lagret på kortet etter 20 minutter, mens andre løsninger lagrer de ti siste bevegelsene, blant annet for å kunne håndtere beregning av billettpris ved overgang mellom transportmidler. Reiseopplysninger i databasen hos kollektivselskapet må oppbevares så lenge det er nødvendig for at kunden skal kunne klage på eventuelle transaksjoner som ikke stemmer.

Elektronisk billettering kan medføre informasjonsutveksling mellom ulike registre som lagrer data på ulike fysiske steder.

Personregistre som kan være involvert

Kollektivselskapene/administrasjonsselskapene oppretter egne kunderegister. Det har også vært uttalt ønske om å hente informasjon om personnummer, navn og adresse fra folkeregisteret for å lette faktureringen.

Behandlingsansvarlig og databehandler

Kollektivselskapene, eller eventuelt et administrasjonsselskap, er behandlingsansvarlig.

Hvem er berørt?

Bruk av elektroniske billetteringssystem er frivillig, og det finnes i dag alternativer for passasjerer som ønsker å reise anonymt. Behandling av personopplysninger skjer når man velger å inngå avtale om bruk av såkalte Smartkort (elektroniske billetter).

Tabell 6: Oppsummering av forhold som berører personvern ved elektronisk billettering.

Oppsummering: Elektronisk billettering	
Type personopplysninger	*Passasjerens navn, adresse, kredittopplysninger, samt reiseinformasjon som dato, klokkeslett, rute og holdeplass eller sone for påstigning/avstigning.*
Hvor i systemet lagres og behandles personopplysninger?	*Reiseopplysninger lagres på den elektroniske billetten (Smartkortet) og i en sentral database hos selskapene. Personopplysninger lagres også i et kunderegister. Personopplysninger behandles i kollektivselskapene, eller eventuelt i et administrasjonsselskap for ulike operatører.*
Personregistre som kan være involvert	*Kollektivselskapene og administrasjonsselskapene oppretter egne kunderegister. Man ønsker imidlertid å kunne bruke folkeregisteret for å sikre riktig mottaker av faktura.*
Behandlingsansvarlig	*Kollektivselskap eller administrasjonsselskap*
Databehandler	*Evt. selskap som behandler dataene på vegne av behandlingsansvarlig.*
Hvem blir berørt (brukere)?	*Kollektivtrafikanter som velger å inngå avtale om bruk av elektronisk billettering.*

2.5 Elektronisk betaling av bompenger

Ved elektronisk betaling av bompenger, foregår toveiskommunikasjon mellom bomstasjonen og AutoPASS-brikken i bilen. AutoPASS-brikken er en aktiv RFID-enhet med radiosender som sender ut signaler over relativt lang avstand. Bomsystemet registrerer brikkens identitet og lagrer informasjon om tidspunkt for passering av den aktuelle bomstasjonen.

Det finnes etter hvert en rekke helautomatiske bompengeanlegg i Norge[4], hvor man ikke har et reelt alternativ for å reise anonymt[5]. Dersom man ikke har AutoPASS-avtale, blir bilens registreringsnummer fotografert og bileier får tilsendt faktura i posten. I de øvrige bomsystemene kan man velge å reise anonymt, ved å betale kontant ved passering av bomstasjonen.

Politiet kan i enkelte tilfeller kreve tilgang til opplysningene som er lagret.

På sikt legges det opp til samordnet betalingssystem for bompenger i Europa. Dette gir store tekniske muligheter for lagring av data og sporing av enkelttrafikanter.

Hva slags personopplysninger behandles?

Det registreres og lagres opplysninger om sted og tidspunkt for passering, samt identifisering av brikke/kjøretøy. I tillegg opererer bompengeselskapene med et kunderegister som inneholder

[4] Følgende bompengeanlegg var helautomatiske per juni 2009: Bomringer i Oslo og Bærum, Bergen, Haugesund og Tønsberg, rv. 2 Kløfta-Nybakk (Akershus), rv. 45 Gjesdal (Rogaland), Imarsundforbindelsen (Møre og Romsdal), Eiksundsambandet (Møre og Romsdal), Halsnøysambandet (Hordaland), rv. 55 Fatlatunnelen (Sogn- og Fjordane) og rv. 9 Setesdalsvegen (Vest-Agder). Etter dette har det kommet flere anlegg med automatisk innkreving, eksempelvis i Kristiansand og Trondheim. Kilde: www.autopass.no.

[5] Kunden kan velge AutoPASS-avtale der opplysningene om passering slettes senest 24 timer etter godkjent passering, se www.autopass.no.

informasjon for utsendelse av faktura (navn, adresse, bilens registreringsnummer). Dataene som behandles er ikke sensitive.

Hvor i systemet lagres og behandles personopplysninger?

Passeringsdata lagres i driftsselskapenes sentralsystem og (kun kort tid) i det lokale veikantutstyret.

Tidligere ble de siste passeringene lagret i AutoPASS-brikkene som en kvittering for kunden, slik at kunden kunne be om at dataene i driftsselskapets sentralsystem kontrolleres mot informasjon i brikken (www.autopass.no).

Figur 4: AutoPASS-brikken (kilde: www.autopass.no)

Det praktiseres ulike retningslinjer for oppbevaring og sletting av passeringsopplysninger avhengig av hvilken betalingsform som benyttes, eksempelvis (Øvstedal 2009, www.autopass.no):

- Forskuddsbetalte avtaler (klippekort) omfatter avtaler der kunden på forhånd betaler for et visst antall passeringer. Passeringsopplysningene slettes senest juni året etter at passeringen har skjedd. Salgsdokumentasjon for selve avtalen oppbevares i ti år i samsvar med krav til bokføring.
- Avtale med sletting av passeringsopplysninger gjelder forskuddsbetalte avtaler, der opplysninger om passeringene slettes senest 24 timer etter godkjent passering. Da kan passeringsdata ikke framskaffes seinere, for eksempel i forbindelse med en klage. Dersom avtalen misligholdes - for eksempel ved manglende betaling - vil "anonymiteten" opphøre.
- Etterskuddsfakturering eller betaling med kredittkort omfatter kunder som passerer bommen uten forhåndsinngått avtale og uten å benytte myntinnkast. Det tas da bilde av bilens registreringsnummer, og dette lagres inntil tjenesten er betalt. I utgangspunktet samles passeringer i opptil tre måneder før faktura sendes ut, men man har også mulighet til å betale avgiften på en servicestasjon i nærheten. Data vil da bli slettet i løpet av 24 timer i sentralsystemet og 72 timer i det lokale veikantutstyret. Skattedirektoratet mener passeringsopplysningene ved etterskuddsbetaling skal oppbevares i ti år i samsvar med krav til bokføring, mens datatilsynets utgangspunkt er at opplysningene skal slettes når fakturaen er betalt.

Personregistre som kan være involvert

Driftselskapene opererer med kunderegister over sine abonnenter. I tillegg må de ha tilgang til kjøretøyregisteret for å sende faktura til bileiere som passerer bomstasjonen uten AutoPASS-avtale og uten å benytte eventuelt manuell betaling.

Behandlingsansvarlig og databehandler

Statens vegvesen og bompengeselskapet er delt behandlingsansvarlig ved elektronisk betaling av bompenger.

De ansatte i driftsselskap og underleverandører som håndterer personopplysninger i forbindelse med fakturering, kundehenvendelser m.m. vil være databehandlere.

Hvem er berørt?

Systemet berører alle som kjører bil i områder med helautomatiske bomstasjoner og alle som velger å benytte AutoPASS-avtale i de øvrige elektroniske bomsystemene.

Tabell 7: Oppsummering av forhold som berører personvern ved elektronisk betaling av bompenger.

Oppsummering: Elektronisk betaling av bompenger	
Type personopplysninger	*Identifisering av brikke/kjøretøy, passeringsinformasjon (tid og sted), samt informasjon for utsendelse av faktura (navn, adresse og bilens registreringsnummer).*
Hvor i systemet lagres og behandles personopplysninger?	*Lokalt i veikantutstyret og i driftsselskapenes sentralsystem. Betalingsform avgjør hvor lenge opplysningene blir oppbevart.*
Personregistre som kan være involvert	*Kjøretøyregisteret. Kunderegister.*
Behandlingsansvarlig	*Statens vegvesen og bompengeselskap.*
Databehandler	*De ansatte hos driftsoperatører og forhandlere som håndterer personopplysninger.*
Hvem blir berørt (brukere)?	*Alle biltrafikanter i områder med helautomatiske bomstasjoner, og alle som velger å benytte seg av AutoPASS-avtale i de øvrige bompengesystemene.*

2.6 Utvidet bruk av AutoPASS-teknologi

Vegdirektoratet har utarbeidet en strategi for videre bruk av AutoPASS-teknologi og ønsker å tilrettelegge for å bruke AutoPASS til utvikling av nye tjenester innenfor veitrafikken. Følgende hovedmål for AutoPASS er presentert (Statens vegvesen 2009[6]):

> *I 2019 skal AutoPASS være et sikkert, effektivt, obligatorisk og brukervennlig system for utførelse av offentlige forvaltningsoppgaver mellom offentlige vegmyndigheter og alle norske kjøretøy på det norske vegnettet.*

[6] Per juni 2009 er dokumentet ferdigstilt, men ikke vedtatt av Vegdirektøren.

Det er allerede etablert flere prøveordninger for andre anvendelser enn bompengebetaling, og Statens vegvesen mottar jevnlig henvendelser fra aktører som ønsker å ta i bruk brikkene for kommersielle formål. AutoPASS-teknologien har vært prøvd ut i forbindelse med fergebetaling, betaling i enkelte parkeringsanlegg, adgangskontroll og til gjennomføring av reisetidsmålinger. Systemet har også vært vurdert for "park and ride"-løsninger.

Statens vegvesen har som mål å ta i bruk AutoPASS-systemet for å løse en rekke forvaltningsoppgaver innenfor etaten (Statens vegvesen 2009):

- **Bompengeinnkreving:** AutoPASS benyttes hovedsakelig til bompengeinnkreving i dag. Det jobbes med å redusere innkrevingskostnader og forbedre brukervennligheten. Videre er det målfestet at alle nye bompengeanlegg skal benytte AutoPASS-systemet.
- **Miljøavgifter:** Ved eventuell etablering av lavutslippssoner (LEZ), vil alle tunge kjøretøy som ikke oppfyller tilstrekkelig EURO-klassifisering bli ilagt en avgift for ferdsel innenfor sonen. AutoPASS kan benyttes til kontroll og innkreving av slike avgifter.
- **Veiprising (rushtidsavgift):** AutoPASS-systemet skal være klargjort for å håndtere denne type avgifter.
- **Trafikkinformasjon:** En løsning for sanntidsregistrering av reisetider basert på AutoPASS-teknologi er testet ut med positive resultater. Passeringstidspunkt for et tellepunkt skrives til brikken. Ved neste tellepunkt kan dette leses og ny passeringstid skrives inn. Statens vegvesen besluttet våren 2008 å videreføre dette ved å etablere systemet for flere hovedveistrekninger.
- **Tungbiloblat:** Etablering av lavutslippssoner og målsetting i NTP om å intensivere tungbilkontroller generelt, taler for innføring av elektronisk oblat for tungbiler. Dette gir også mulighet for fraktovervåking gjennom elektronisk varsling til veimyndigheter om farlig last i tunneler og andre kritiske anlegg. AutoPASS-teknologi kan muligens brukes til dette formålet.
- **Alminnelig elektronisk oblat:** AutoPASS-teknologi kan erstatte oblatet som klistres på bilens nummerskilt, for å vise at kjøretøyet har betalt årsavgift, oppfylt EU-kontroll og har orden på forsikring og heftelser, samt ordninger knyttet til prøvekjennemerker.

Utvidet bruk av AutoPASS-teknologi, forutsetter at man etablerer et nytt organisatorisk rammeverk for AutoPASS-ordningen. Statens vegvesen anbefaler at man utreder et alternativ hvor service, håndtering av pengestrømmer og utstederfunksjonen sentraliseres og det etableres et offentlig aksjeselskap som har ansvar for utvikling og forvaltning av systemet i henhold til nye internasjonale krav og nye operatører. Selskapet kan både drifte nye bompengeanlegg og tilrettelegge for offentlige tjenester ved utvidet bruk av AutoPASS-teknologi, uten at dette belaster eller medfører risiko for bompengeselskapene. Statens vegvesen mener det er hensiktsmessig å opprette et nytt felles brikkeregister i strategiperioden (Statens vegvesen 2009).

Målsettingen er at AutoPASS-brikken skal bli obligatorisk i tunge kjøretøy i første omgang, og i alle norske kjøretøy på sikt. Samtidig legges det til rette for at man skal kunne ta i bruk såkalte "anonymbrikker" og "gjestebrikker".

Hva slags personopplysninger behandles?

AutoPASS-systemet behandler personopplysninger som navn, adresse og nødvendige kredittopplysninger, samt brikkeidentifikasjon og kjøretøyets registreringsnummer. I tillegg vil

det registreres passeringsdata som dato, klokkeslett og stedfesting. Det kan også være aktuelt å foreta logging og registrere kjørelengde basert på passeringsdata.

Dersom AutoPASS-brikkene skal brukes som oblater, vil det også være aktuelt å lagre andre type data, som betalt årsavgift, oppfylt EU-kontroll, om man har orden på forsikringsforhold og heftelser, samt informasjon knyttet til prøvekjennetegn. For godstransport kan det være aktuelt med elektronisk fraktinformasjon og opplysninger om kjøretøyenes tekniske egenskaper.

Det er ingen tvil om at det er et stort potensial for å benytte AutoPASS til en rekke ulike formål, og i mange tilfeller vil det være personverninteresser som begrenser hvilke personopplysninger som behandles i forbindelse med de ulike systemene. Reisetidsmålinger og tellinger kan gjennomføres uten at det lagres data som kan knyttes direkte til kjøretøy eller person.

Hvor i systemet lagres og behandles personopplysninger?

Informasjon kan lagres i AutoPASS-brikken, i veikantutstyret og i sentralsystemet (datasystemet som tar i mot passeringsdata fra veikantutstyret). Per i dag er det Statens vegvesen som eier brikkene og veikantutstyret, mens de ulike aktørene eier sentralsystemet og har det fysisk plassert hos seg.

I løpet av en tiårsperiode ønsker Statens vegvesen å erstatte dagens brikker med en multifunksjonsbrikke som kan fungere som elektronisk oblat i det norske veitransportsystemet. Nye anvendelsesområder for AutoPASS og eventuelle krav om europeisk interoperabilitet kan utløse behov for å utvikle sentralsystemet, men omfanget av dette er vanskelig å anslå i dag.

Personregistre som kan være involvert

I forbindelse med bompengeinnkreving benyttes kjøretøyregisteret for å identifisere kjøretøy (og eiere) som passerer uten å betale avgift. I tillegg ønsker Statens vegvesen å samle informasjon om brikkeidentifikasjon i et felles brikkeregister. Ved utvidet bruk av AutoPASS-systemet kan det være aktuelt å ta i bruk en rekke nye registre, avhengig av bruksområde.

Behandlingsansvarlig og databehandler

Ved bruk av AutoPASS-systemet for bompengeinnkreving, er det i dag Statens vegvesen og de lokale bompengeselskapene som er behandlingsansvarlig. Dersom man tar i bruk nye anvendelsesområder for systemet, vil antall personer og aktører som håndterer personopplysninger øke, og det kan bli vanskeligere for brukerne å skaffe seg oversikt over hvem som har tilgang til data som samles inn om den enkelte trafikant. Hvem som er behandlingsansvarlig og hvem som er databehandlere avhenger av hvilken organisering og hvilke løsninger som velges.

Hvem blir berørt?

Dersom bruk av AutoPASS-brikker blir obligatorisk vil alle trafikanter i kjøretøy berøres. Det kan imidlertid utvikles egne "anonymbrikker" for å sikre muligheten for å ferdes anonymt[7] i veitrafikksystemet.

Tabell 8: Oppsummering av forhold som berører personvern ved utvidet bruk av AutoPASS.

Oppsummering: Utvidet bruk av AutoPASS	
Type personopplysninger	*Navn, adresse, kredittopplysninger, brikkeidentifikasjon, kjøretøyets registreringsnummer, passeringsinformasjon (dato, klokkeslett, sted), logging og kjørelengde. Avhengig av hvilke løsninger som velges kan man også registrere informasjon om betaling av årsavgift, oppfylt EU-kontroll, forsikringsforhold og heftelser, prøvekjennetegn. For godstransportører kan det også være aktuelt med informasjon om lasten og kjøretøyets tekniske beskaffenhet (EURO-klassifisering).*
Hvor i systemet lagres og behandles personopplysninger?	*I AutoPASS-brikken, veikantsystemet og sentralsystemet hos de ulike operatørene.*
Personregistre som kan være involvert	*Kjøretøyregisteret. Statens vegvesen ønsker å opprette et sentralt brikkeregister.*
Behandlingsansvarlig	*I dag er Statens vegvesen og det lokale bompengeselskapet behandlingsansvarlig. Antall personer og aktører som håndterer personopplysninger vil sannsynligvis øke når nye anvendelsesområder for AutoPASS tas i bruk.*
Databehandler	
Hvem blir berørt (brukere)?	*På sikt vil alle trafikanter i kjøretøy berøres.*

2.7 Intelligente fartstilpasningssystem (ISA) med lagring av data

Intelligente fartstilpasningssystem[8] (Intelligent Speed Adaptation, ISA) er satellittbaserte gps-system som kobler koordinatfestet fartsgrenseinformasjon med posisjon for kjøretøyet og varsler føreren dersom fartsgrensen på stedet overskrides. ISA-systemene er enten *passive* system som kun gir føreren informasjon om at farten er for høy, eller *aktive* system som griper inn og korrigerer kjøretøyets hastighet i henhold til stedets fartsgrense, eksempelvis økt motstand på gasspedalen eller fartssperre. Hensikten med ISA-systemet er å hjelpe trafikanter til å overholde fartsgrensene, og studier viser at systemet har god effekt på trafikksikkerhet (Carsten and Tate 2005; Carsten m.fl. 2008).

Statens vegvesen ønsker også å teste ut dynamisk ISA, som varsler nedsatt hastighet på grunn av spesielle vær- eller trafikkforhold (for eksempel ved veiarbeid, hendelser, tett tåke, glatt veibane etc.).

[7] Per i dag er dette ikke et reelt anonymt tilbud, men gir *pseudonymitet*. I og med at brikken registreres på samme måte ved hver passering, vil det være mulig å bygge opp en trafikantprofil, selv om denne ikke knyttes til en bestemt person.

[8] På norsk brukes begrepene *intelligent fartstilpasning* eller *automatisk fartstilpasning*, tilsvarende de engelske begrepene Intelligent Speed Adaptation ISA og Automated Speed Adaptation ASA, definert som: "Various concepts aiming at limiting the vehicle speed in relation to different reference speeds (static, variable or dynamic) via various user interfaces (informative, supportive or compulsory)" (fra utkast juli 2010 til revidert NVF ITS Terminology).

Figur 5: Skjerm som viser visuell varsling av fartsgrense.

I utgangspunktet er ISA et førerstøttesystem uten personvernimplikasjoner, så lenge data om førerens atferd ikke lagres. Det er imidlertid vanlig å kombinere ISA med en lagringsenhet som kontinuerlig logger og lagrer data om bilens posisjon, hastighet, akselerasjon, retardasjon, samt fartsnivå i kurver. *Bruk av ISA med lagringsenhet* (atferdsregistrator) muliggjør ulike former for overvåking, både for persontransport og næringstrafikk. I tillegg til at atferdsdata lagres i utstyr i bilen, finnes det *kommunikasjonsløsninger* og programvare som gjør at informasjon kan sendes fra bilen til en ytre kilde.

Et eksempel på dette er system som sender sms til bileier dersom fartsgrensen overskrides. Denne type system kan være attraktivt for foreldre som ønsker å forsikre seg om at ungdommer med ferske førerkort kjører forsiktig når de låner bilen. En kan også tenke seg system som kontinuerlig sender informasjon om posisjon og hastighet, slik at man kan spore kjøretøy og atferd i sanntid. Bruk av ISA er også foreslått som mulig sanksjon overfor trafikanter som blir tatt i fartskontroll (Nasjonal tiltaksplan for trafikksikkerhet på veg 2010-2013).

Foreløpig er ISA-systemene kun tatt i bruk i liten skala i Norge, og det er vanskelig å forutse alle aktuelle løsninger og bruksområder. Statens vegvesen har vedtatt å innføre ISA i sine nye kjøretøy. Det er tydelig at dette er et system med stort trafikksikkerhetspotensial, men det gir også muligheter for personvernimplikasjoner. Hvem skal få tilgang til opplysninger som er lagret i atferdsregistratoren? Hva med ny eier ved kjøp og salg av bruktbil? Kan man bli ilagt fartsbot basert på ISA-systemets registreringer? Hvem som skal ha tilgang til data og hvordan de kan benyttes vil være viktige spørsmål å utrede før ISA-systemet implementeres i stor skala.

Hva slags personopplysninger behandles?

I et ISA-system med atferdsregistrator registreres opplysninger om posisjon, hastighet, fartsgrense og kjørestil (akselerasjon, retardasjon, fartsnivå i kurver). Enkelte løsninger kan lagre data på en måte som ikke identifiserer posisjon, kun hastighet i forhold til fartsgrense på et gitt sted.

Hvor i systemet lagres og behandles personopplysninger?

Hvor personopplysninger blir lagret og behandlet, er litt avhengig av hvilken type løsning som benyttes. Når Statens vegvesen installerer ISA i sine tjenestekjøretøy, vil behandling av data bli satt ut til en ekstern aktør. Denne vil samle data fra alle atferdsregistratorene og levere resultatene til Statens vegvesen på aggregert nivå, slik at det ikke blir mulig å identifisere enkeltkjøretøy eller fører. I et slikt tilfelle lagres data i hver enkelt atferdsregistrator og hos den valgte aktøren som innhenter data og presenterer statistikken for Statens vegvesen.

Når ISA-systemene blir brukt i private kjøretøy, er det mer uklart hvor data behandles. I utgangspunktet lagres alle data i bilens atferdsregistrator, men det er mulig å overføre data til eksterne aktører for ulike formål.

Personregistre som kan være involvert

I utgangspunktet benyttes ikke personregister i forbindelse med ISA-system.

Dersom ISA-systemene blir svært utbredt, kan det komme forespørsler fra aktører som ønsker å opprette nye registre eller koble data mot eksisterende registre. Det er ikke vanskelig å tenke seg at for eksempel forsikringsselskap ville vært interessert i å opprette kunderegister med kjøreprofil knyttet til den enkelte fører, for å differensiere sine forsikringspremier.

Behandlingsansvarlig og databehandler

For ISA-system er det uklart hvem som er behandlingsansvarlig i de ulike tilfellene. Aktører som tilbyr tjenester som baserer seg på lagring eller behandling av personopplysninger, vil være behandlingsansvarlig.

I det nevnte eksempelet med Statens vegvesen, vil vegvesenet som dataeier være behandlingsansvarlig og bestemmer hvordan og med hvilke hjelpemidler dataene skal behandles. I tillegg kan ekstern aktør (verksted eller leverandør) være databehandler. Det vil være ansatte hos den eksterne aktøren som har tilgang til data på kjøretøynivå.

ISA-system i privatbilen kommer i utgangspunktet ikke inn under personopplysningsloven, da det ikke er forbudt å registrere eller lagre data til private formål.

Hvem blir berørt?

Så lenge ISA-systemet ikke er obligatorisk sikkerhetsutstyr i bil, berører ordningen ansatte hos arbeidsgivere som har pålagt sine arbeidstakere å benytte ISA i tjenestekjøretøyene og førere som frivillig installerer systemet i sitt kjøretøy.

En av utfordringene med ISA-systemet, er at man som fører ikke nødvendigvis merker at atferden logges – og dermed kan man overvåkes uten at man er klar over det. Systemet berører dermed alle som kjører en bil med ISA-system.

Tabell 9: Oppsummering av forhold som berører personvern ved ISA med atferdsregistrator.

Oppsummering: ISA med atferdsregistrator	
Type personopplysninger	*Opplysninger om posisjon, hastighet, fartsgrense og kjørestil. Enkelte løsninger kan lagre data på en måte som ikke identifiserer posisjon, kun hastighet i forhold til fartsgrense på et gitt sted.*
Hvor i systemet lagres og behandles personopplysninger?	*Data lagres i atferdsregistratoren. Hvor personopplysninger behandles utover dette er avhengig av type system. Teknologien muliggjør mange ulike bruksområder og behandling av personopplysninger hos ulike aktører.*
Personregistre som kan være involvert	*Ingen personregister er involvert i utgangspunktet. Dersom ISA blir svært utbredt, er det sannsynlig at det kommer forespørsler fra aktører som ønsker å opprette eller koble data mot eksisterende system.*

Behandlingsansvarlig Databehandler	*Hvem som blir behandlingsansvarlig og databehandlere er avhengig av type løsning som benyttes. ISA-systemene kan benyttes til mange ulike formål, og det kan derfor være uklart hvem som er behandlingsansvarlig og databehandler i de ulike tilfellene.*
Hvem blir berørt (brukere)?	*Per i dag er brukerne stort sett arbeidstakere hos arbeidsgivere som har installert ISA i sine tjenestekjøretøy. I tillegg vil det etter hvert være førere som installerer ISA frivillig. Førere som låner en bil med ISA-system, kan få atferden logget uten selv å være klar over det.*

2.8 Alkolås med logging og/eller varsling

Et alkolåssystem har som formål å hindre personer med promille i å kjøre bil. En tilleggsfunksjon kan være at den registrerer, og eventuelt varsler omgivelsene, dersom en fører likevel kjører med promille.

Alkolåsen er et alkometer som er koblet til bilens tenningslås, slik at det ikke er mulig for føreren å starte bilen før vedkommende har foretatt en pusteprøve. Når føreren ikke har promille, startes bilen på vanlig måte. Dersom føreren har promille høyere enn gjeldende promillegrense, utløses en startsperre slik at bilen ikke lar seg starte. Det finnes flere produsenter og ulike typer alkolåser. De enkleste variantene utløser en startsperre, uten at data om pusteprøven loggføres (www.mhf.se).

De fleste produktene har imidlertid en eller annen form for lagring av data, for bruk i forbindelse med yrkestransport og som alternativ til inndragning av førerkort. Noen system lar seg overprøve av føreren, men det blir da loggført at føreren har kjørt eller startet bilen i alkoholpåvirket tilstand eller at alkometeret ikke har vært i bruk.

Alkolåsen kan kombineres med ulike varslingssystem, for eksempel ved at lysene og bilhornet aktiveres på en måte som gjør omgivelsene oppmerksom på at noe er galt. I fremtiden kan man også tenke seg system hvor nærmeste politikontor varsles når alkolåsen overprøves.

Flere bilprodusenter tilbyr alkolås som ekstrautstyr. Det er også mulig å kjøpe utstyr for ettermontering. Statens vegvesen har innført alkolås som standardutstyr på sine tjenestebiler.

Norske myndigheter vurderer å bruke systemet som et alternativ til inndragning av førerkort for promilledømte. I Sverige benyttes alkolås som tiltak overfor personer som er dømt for promillekjøring. I slike tilfeller benyttes en alkolås som krever at føreren leverer pusteprøve både før kjøreturen og underveis. Dersom føreren har promille eller unnlater å ta prøven, begynner bilen å tute, samtidig som det logges et avvik som senere varsles myndighetene[9]. En del svenske kommuner har også påbudt bruk av alkolås i busser som benyttes til skoletransport.

Hva slags personopplysninger behandles?

De produktene som loggfører data, vil lagre informasjon om tidspunkt for blåseprøve, samt om føreren har hatt promille.

[9] Informasjon fått per e-post fra Sahra Kers, Transportstyrelsen i Sverige, 3. juli 2009.

Hvor i systemet lagres og behandles personopplysninger?

Dataene lagres i en dataenhet i kjøretøyet. Det er også mulig å overføre informasjon til en sentral enhet, enten manuelt eller automatisk. Dette er aktuelt når alkolås benyttes for kvalitetssikring av yrkestrafikk og i forbindelse med alkolåsprogram (alternativ til inndragning av førerkort).

Personregistre som kan være involvert

For alkolåsprogram (promilledømte) benyttes tilknyttede personregistre. For andre bruksområder benyttes i utgangpunktet ikke personregistre i forbindelse med alkolås.

Behandlingsansvarlig og databehandler

Når alkolås benyttes i forbindelse med yrkestrafikk vil arbeidsgiver være behandlingsansvarlig. Det vil sannsynligvis være snakk om et svært begrenset antall personer som får tilgang til denne informasjonen.

Når alkolås benyttes som alternativ til inndragning av førerkort, er myndighetene behandlingsansvarlig for data som registreres.

For egen bruk av alkolås hos privatbilister er det ikke relevant å definere behandlingsansvarlig og databehandler.

Hvem blir berørt?

Ansatte i bedrifter som benytter alkolås i sine kjøretøy, samt personer som får installert alkolås som resultat av promillekjøring berøres av dette systemet. I tillegg vil brukere av andre kjøretøy som er utstyrt med alkolås berøres, men her er det i utgangspunktet ikke aktuelt at data blir behandlet av andre enn bileier.

Figur 6: Bildet viser sjåfør som foretar blåseprøve med alkolås (foto: SINTEF).

Tabell 10: Oppsummering av forhold som berører personvern ved alkolås.

Oppsummering: Alkolås med logging og/eller varsling	
Type personopplysninger	*Tidspunkt for blåseprøve og evt. promille*
Hvor i systemet lagres og behandles personopplysninger?	*Data lagres i en enhet i kjøretøyet, og evt hos arbeidsgiver ved yrkestrafikk.*
Personregistre som kan være involvert	*Systemet involverer personregistre når det benyttes som alternativ til inndragning av førerkort.*
Behandlingsansvarlig Databehandler	*I forbindelse med yrkestrafikk vil arbeidsgiver være behandlingsansvarlig. Som alternativ til inndragning av førerkort for promilledømte, vil myndighetene være behandlingsansvarlig. For alkolås som system vil det sannsynligvis være snakk om et svært begrenset antall ansatte med tilgang til denne type informasjon.*
Hvem blir berørt (brukere)?	*Ansatte hos arbeidsgivere som har installert alkolås på tjenestekjøretøy, personer som får pålagt bruk av alkolås som alternativ til inndratt førerkort ved promillekjøring, samt brukere av andre kjøretøy som er utstyrt med alkolås.*

2.9 Lokasjonsbaserte tjenester

Lokasjonsbaserte tjenester baserer seg på et system som registrerer hvor brukeren befinner seg og tilbyr relevante tjenester for dette området, for eksempel via mobiltelefon. Innenfor transportsystemet brukes dette gjerne for å formidle trafikantinformasjon, men det kan også benyttes til kommersielle tilbud og underholdningstjenester.

I utgangspunktet kan denne type tjenester formidle trafikantinformasjon uten å avsløre brukerens posisjon for andre. Eksempler på slike tjenester kan være sms med varsel om rutetider når man befinner seg på en bussholdeplass, informasjon om nærmeste bensinstasjon eller severdigheter langs kjøreruten, navigasjonstjenester og intelligente fartstilpasningssystem som gir informasjon om fartsgrense på stedet (se avsnitt 2.7). Dersom man tillater at opplysninger om den enkelte trafikant/kjøretøys posisjon og egenskaper formidles til andre brukere, kan man ta i bruk mer dynamiske tjenester som køvarsling, varsling om glatt veibane basert på friksjonssensorer i nærliggende kjøretøy, flåtestyring m.m.

De siste årene har det vært nærmest eksplosiv bruk av sosiale medier som facebook, twitter o.l. Teknologibransjen har spådd at lokasjonsbaserte tjenester vil være den neste store trenden innenfor sosiale medier, slik at man i tillegg til å oppdatere brukerprofil med *hvem* man er og *hva* man gjør, også vil vise omverden *hvor* man befinner seg. På teknologisiden jobbes det for å flytte geolokalisering over fra gps/mobil-system til server-siden, slik at man alltid er lokalisert, uavhengig av operatør o.l. I praksis vil man da gjøre det mulig for sine kontakter å drive kontinuerlig overvåking. Transportselskapet UShip bruker denne løsningen for å tilby sine kunder kontinuerlig sporing av pakker via sjåførens mobiltelefon, isteden for den tradisjonelle sporingstjenesten hvor man registrerer når pakker ankommer eller forlater terminaler (www.nrkbeta.no: ”Hvem, hva ... og nå også hvor”).

Ved bruk av lokasjonsbaserte tjenester har man mulighet til å finne ut hvor en trafikant eller et kjøretøy befinner seg til enhver tid, ved sporing via satellitt eller mobiltelefon. Denne type

tjenester må i de fleste tilfeller være basert på frivillighet for å oppfylle kravene i Personopplysningsloven (Schartum 2001). For de tjenestene som finnes tilgjengelige i dag, er dette ofte løst ved at brukeren tegner et abonnement på den aktuelle tjenesten.

Hva slags personopplysninger behandles?

Lokasjonsbaserte tjenester medfører behandling av posisjoneringsdata (tid og sted) for den enkelte trafikant som benytter tjenesten. Ofte identifiseres brukeren via mobilabonnement.

Hvor i systemet lagres og behandles personopplysninger?

De lokasjonsbaserte tjenestene som er tilgjengelige i dag er gjerne basert på sporing via mobiltelefon, og informasjon behandles hos tjenestetilbyder eller operatør av tjenesten. Utviklingen i samfunnet går i retning av større og mer omfattende bruk av sosiale medier – og det finnes etter hvert programmer som via gps og Smartphone viser for omverdenen hvor man til enhver til oppholder seg.

Personregistre som kan være involvert

For å oppfylle kravene i Personopplysningsloven, er lokasjonsbaserte tjenester gjerne basert på at brukerne tegner et abonnement. Dette gjør at den enkelte aktør opererer med et kunderegister over trafikanter som abonnerer på ulike tjenester.

Behandlingsansvarlig og databehandler

Den som tilbyr tjenesten vil være behandlingsansvarlig med tanke på personopplysninger, mens de som drifter tjenesten er databehandlere. Lokasjonsbaserte tjenester har potensial for å tas i bruk i stor utstrekning og med mange nye aktører, dersom løsningen tilbys markedet uten regulering fra myndighetene.

Hvem blir berørt?

Personer som velger å abonnere på lokasjonsbaserte tjenester berøres av dette systemet.

Tabell 11: Oppsummering av forhold som berører personvern ved lokasjonsbaserte tjenester.

Oppsummering: Lokasjonsbaserte tjenester	
Type personopplysninger	*Identifikasjon av bruker, samt posisjoneringsdata.*
Hvor i systemet lagres og behandles personopplysninger?	*Hos tjenestetilbyder eller operatør av systemet. Lokasjonsbaserte tjenester har potensial til å tas i bruk i stor utstrekning og med mange nye aktører, dersom bruken ikke reguleres.*
Personregistre som kan være involvert	*Kunderegister*
Behandlingsansvarlig	*Tjenestetilbyder/operatør av systemet.*
Databehandler	
Hvem blir berørt (brukere)?	*Personer som abonnerer på tjenesten.*

2.10 Sporing av kjøretøy

Sporing av kjøretøy er etter hvert blitt nokså utbredt i Norge, med bruk av gps og satellittsystem, eller GSM/GPRS-teknologi som gir posisjon ved bruk av mobilnettet. Data som identifiserer kjøretøyet og informasjon om posisjon overføres fra en mobil enhet til f.eks. en pc, hvor informasjonen kan presenteres visuelt på et kart.

Denne type system brukes blant annet til flåtestyring, som er nærmere beskrevet i avsnitt 2.11.

Sporing av kjøretøy brukes av privatpersoner, blant annet for å sikre at de skal finne igjen bilen ved eventuelle tyveri[10]. Det finnes forholdsvis rimelige system på markedet som tilbyr overvåking i sanntid, varslingstjenester dersom kjøretøyet befinner seg i spesielle områder og som også gjør det mulig å stoppe kjøretøyet (kutte bensintilførsel) ved hjelp av mobiltelefon.

Forsikringsselskap som gir kunder rabatt for eller setter krav til at kjøretøy skal ha gjenfinningssystem, krever at gjenfinningssystemet er forsikringsgodkjent (Forsikringsselskapenes godkjenningsnemnd 2010). Etter dette regelverket skal alarmen gå til en alarmsentral med utrykningsapparat, og som har konsesjon for slik virksomhet.

Også politiet benytter teknisk sporing av kjøretøy, gods eller andre gjenstander som alternativ til tradisjonell spaning for å bekjempe kriminalitet (Justis og politidepartementet 2009).

Det kan også være aktører som er interessert i å etablere nye tjenester knyttet til sporingssystem. Et eksempel er forsikringsselskap som tilbyr løsninger hvor forsikringspremien avhenger av sted (type vei eller gate) og tidspunkt for kjøringen.

System som sporer kjøretøy vil utfordre personverninteressene, både fordi det registreres og lagres store mengder data om bevegelsesmønster, og fordi det kan være vanskelig for den som blir berørt å vite at overvåkingen skjer. Ved å installere sporingsenheter i kjøretøy, vil man f.eks. kunne ha full kontroll over hvor familiemedlemmer befinner seg til enhver tid.

[10] Transmittere (jamming) for å forstyrre GPS- og/eller mobilkommunikasjonen i et område benyttes av kriminelle (2010-10-11: http://www.gpsworld.com/defense/security-surveillance/expert-advice-gps-forensics-crime-and-jamming-8986).

Det europeiske satellittnavigasjonssystemet Galileo[11], legger tilrette for tjenester som innebærer kontinuerlig registrering og åpner for navigasjonstjenester som ikke kan leveres over dagens amerikanske GPS-system.

Hva slags personopplysninger behandles?

Ved sporing av kjøretøy, identifiseres det aktuelle kjøretøyet og det registreres detaljert informasjon om hvor kjøretøyet befinner seg til enhver tid.

Hvor i systemet lagres og behandles personopplysninger?

Data vil lagres i en enhet i kjøretøyet, samt i en sentral eller et definert sted som dataene overføres til. Hvem som helst kan anskaffe sporingsutstyr og bestemme hvor informasjon skal sendes, f.eks. til en pc eller mobiltelefon.

Personregistre som kan være involvert

Så lenge sporingsteknologien benyttes til privat bruk, er det ikke involvert personregistre.

Behandlingsansvarlig og databehandler

Til privat bruk, er det ikke aktuelt å definere behandlingsansvarlig og databehandler. Dersom andre aktører (f.eks. forsikringsselskap) får tilgang til denne type informasjon, vil de besitte kunnskap om spesifikke kjøretøys bevegelsesmønster som må håndteres på lik linje med andre personopplysninger. Alarmsentral og operatører som behandler personopplysninger defineres som databehandlere.

Når politiet foretar teknisk sporing, vil påtalemyndighet være behandlingsansvarlig.

Hvem blir berørt?

Den som eier eller bruker et kjøretøy med sporingsutstyr blir berørt av dette systemet. Det kan være vanskelig for den som blir overvåket å vite at dette foregår.

[11] Galileo er et europeisk satellittnavigasjonssystem som planlegges tatt i bruk innen få år.

Tabell 12: Oppsummering av forhold som berører personvern ved sporing av kjøretøy.

Oppsummering: Sporing av kjøretøy	
Type personopplysninger	*Kjøretøyidentifikasjon, informasjon om posisjonering (tid og sted).*
Hvor i systemet lagres og behandles personopplysninger?	*I sporingsenhet, samt i en hvilken som helst datakilde valgt av den som anskaffer sporingsutstyret.*
Personregistre som kan være involvert	*I utgangspunktet involveres ikke personregistre.*
Behandlingsansvarlig	*Ikke aktuelt for privat bruk. Forsikringsselskap eller andre aktører som tilbyr tjenester basert på sporingsdata vil være behandlingsansvarlig. Ved teknisk sporing brukt i politietterforskning vil påtalemyndigheten være behandlingsansvarlig.*
Databehandler	*Ikke aktuelt for privat bruk. Alarmsentral og operatører som drifter system basert på sporingsdata er databehandlere.*
Hvem blir berørt (brukere)?	*Den som eier eller bruker et kjøretøy som er utstyrt med sporingsenhet. Brukeren vil ikke nødvendigvis vite at han overvåkes.*

2.11 Overvåking av yrkesstransport

Godstransporten og ansatte hos transportbedrifter er utsatt for ganske omfattende kontroll og overvåking allerede i dag. Dette gjøres for å avdekke både trafikksikkerhetsforhold og forhold som angår konkurranse i transportnæringen. ITS-løsninger muliggjør en effektivisering av slike kontroller, både ved at selve kontrollvirksomheten gjøres mer kostnadseffektiv for Statens vegvesen og ved at transportnæringen oppnår reduserte køer og ventekostnader (Statens vegvesen 2007).

Kontroll av last for tunge kjøretøy kan forbedres ved bruk av WIM-teknologi (Weighing in motion – automatisk veiing av kjøretøy i fart), RFID eller automatisk kjennemerkeregistrering og elektronisk rapportering til kontrollstasjoner (Statens vegvesen 2007).

AutoPASS-brikkene eller annen RFID-teknologi kan benyttes til å lagre informasjon om farlig gods i tunge kjøretøy. Dette kan være nyttig for å overvåke kjøretøy med farlig last i tunneler eller i områder med restriksjoner på denne type ferdsel. Williams (2008) beskriver to mulige løsninger for framtidig teknologi på dette området:

- Det kan sendes et varsel fra infrastrukturen til fører av farlig gods når han nærmer seg en restriksjonssone.
- Det kan sendes et kontinuerlig signal fra kjøretøyet til omgivelsene om type farlig gods, føreridentifikasjon og lignende.

Det siste punktet innebærer vesentlig større implikasjoner for personvernet. Dersom kjøretøyet beveger seg inn i en restriksjonssone, kan dette utløse en reaksjon på ulike nivå; fra varsling av fører til automatisk stans av kjøretøy eller varsling av politi og nødsentral.

Statens vegvesen beskriver i sin ITS-strategi konkrete tiltak de vil gjennomføre for å forbedre tungbilkontroller (Statens vegvesen 2007). På kort sikt er dette å gjennomføre et prøveprosjekt med WIM og automatisk nummerskiltgjenkjenning med oppslag i registre, samt å teste konsept og etablere system for overvåking av farlig gods i minst en viktig tunnel. På lengre sikt ønsker man å

innføre WIM med automatisk nummerskiltgjenkjenning på de viktigste kontrollstasjonene i landet.

I utgangspunktet medfører ikke disse tiltakene registrering av andre personopplysninger enn det man allerede behandler i dag. Likevel utfordrer bruk av ITS-løsninger personvernet, fordi en del data har fått elektronisk lagringsform, samtidig som det totale omfanget av data har økt. Samtidig kan tiltakene bidra til en enklere arbeidsdag for førerne, ved å redusere unødvendig venting og tidstap.

Den ansatte i en transportbedrift kan være utsatt for ganske omfattende overvåking av sin arbeidsgiver. Satellittovervåking av kjøretøy basert på gps eller Galileo, muliggjør sporing av containere og enkeltkjøretøy, samt registrering av posisjon og fart. Dette kan benyttes til både flåtestyring, transportmiddelkontroll og ettersporing av gods. Det er også en økende bruk av elektroniske feltverktøy som gjør at dokumentasjon, verifisering av kjøreoppdrag, timelister og feltrapporter skjer mer eller mindre automatisk. Dette resulterer i at arbeidsgiver til enhver tid har full kontroll over de enkelte førernes bevegelser og atferd. Ved innføring av denne type system, må den ansattes rett til privatliv veies mot arbeidsgivers styringsrett.

Hva slags personopplysninger behandles?

Ulike løsninger for overvåking av godstransport gir muligheter for omfattende registrering av data. Eksempler på personopplysninger som behandles er kjøretøy-/føreridentifikasjon, posisjoneringsinformasjon, informasjon om lasten som transporteres, samt forhold ved førerens gjennomføring av kjøreoppdrag (kjøre-/hviletid m.m.). Statens vegvesen har i prinsippet tilgang til denne informasjon også i dag når kontrollene gjennomføres manuelt, men ny teknologi muliggjør mer effektive og omfattende kontroller, samt elektronisk lagring av informasjon.

Hvor i systemet lagres og behandles personopplysninger?

Når kontrollvirksomheten av godstransport etter hvert blir mer og mer elektronisk, vil kjøretøyene måtte utstyres med RFID-brikker eller annen teknologi som muliggjør lagring og overføring av informasjon. I tillegg vil dataene lagres elektronisk i Statens vegvesens datasystem, eller hos arbeidsgiver når systemet brukes til flåtestyring, sporing av gods o.l.

Statens vegvesen har et eget kontrollsystem for utekontroller; Vadis (Vehicle and Driver Inspection system).

Personregistre som kan være involvert

Overvåking av godstransport vil kunne involvere flere personregistre. Først og fremst benyttes kjøretøyregisteret for å identifisere kjøretøy, men også andre dataregister kan tas i bruk, avhengig av hva man ønsker å kontrollere.

Behandlingsansvarlig og databehandler

Statens vegvesen vil, på samme måte som når kontrollene foretas manuelt, være behandlingsansvarlig og ha databehandlere til å håndtere personopplysningene som samles inn. Politiet foretar egne kontroller og er selv behandlingsansvarlig for disse.

Når ITS-løsningene brukes til flåtestyring, er arbeidsgiver behandlingsansvarlig. Evt. operatører med tilgang til data om de enkelte kjøretøy og førere er databehandlere.

Hvem blir berørt?

Når overvåking av godstransport skjer elektronisk, er det de ansatte og bedrifter i transportnæringen som berøres. En av utfordringene med bruk av ITS-løsninger er at den enkelte fører kan være uvitende om at registrering og overføring av data foregår, og det kan derfor være vanskelig å ha oversikt over hvilke opplysninger man gir fra seg og hvem som får tilgang til informasjonen.

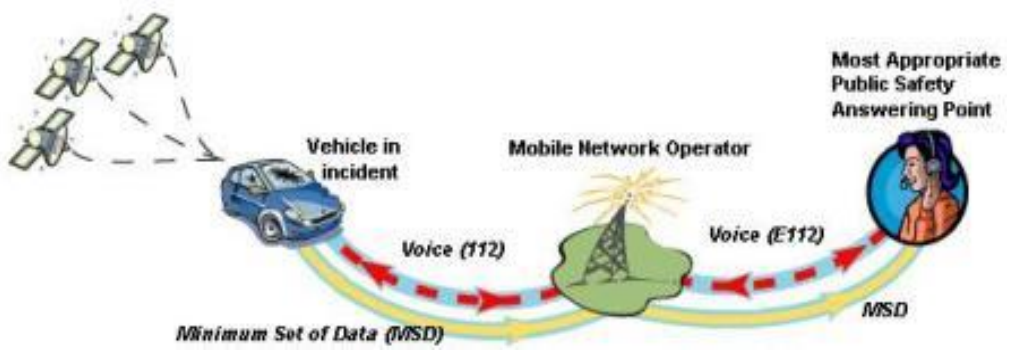
Figur 7: Illustrasjon av flåtestyringssystem (kilde: www.norsknavigasjon.no).

Tabell 13: Oppsummering av forhold som berører personvern ved overvåking av godstransport.

Oppsummering: Overvåking av yrkestransport	
Type personopplysninger	*Identifikasjon av kjøretøy og fører, posisjoneringsdata, data om godset som fraktes, informasjon om kjøreoppdrag og forhold ved førerens gjennomføring av oppdraget, f.eks. overholdelse av kjøre-/hviletid.*
Hvor i systemet lagres og behandles personopplysninger?	*Informasjon lagres elektronisk i kjøretøyet, samt i dataregistre hos kontrollør (Statens vegvesen) eller arbeidsgiver.*
Personregistre som kan være involvert	*Kjøretøyregisteret. Andre register kan også tas i bruk.*
Behandlingsansvarlig	*Statens vegvesen ved tungbilkontroller og arbeidsgiver ved flåtestyring o.l. Politiet er behandlingsansvarlig for egne kontroller.*
Databehandler	*Evt. aktører som håndterer personopplysninger på vegne av Statens vegvesen, politi eller arbeidsgiver.*
Hvem blir berørt (brukere)?	*Ansatte og bedrifter i transportnæringen.*

2.12 eCall

eCall er et europeisk system for automatisk varsling av trafikkulykker, som muliggjør satellittsporing av kjøretøy ved bruk av GPS-enheter innebygd i kjøretøyene. Når et kjøretøy er involvert i en ulykke, sendes det nødmelding fra kjøretøyet til nærmeste nødsentral. Systemet vil både kunne aktiveres manuelt, eller utløses automatisk ved hjelp av sensorer i kjøretøyet. Det foregår da en automatisk dataoverføring av nøkkelinformasjon om kjøretøyet, samt tidspunkt og stedfesting av ulykkespunktet. I tillegg er det beskrevet løsninger hvor man oppnår telefonisk kontakt mellom passasjerene i kjøretøyet og nødsentralen.



Figur 8: eCall-arkitektur (kilde: www.eSafetysupport.org)

eCall-løsningen utvikles innenfor EU-kommisjonen og forventes å bli obligatorisk utstyr i alle nye biler (www.esafety.org). Norge har undertegnet en intensjonsavtale som tar sikte på innføring av eCall her i landet. Per i dag er det ikke planlagt at det sendes automatisk informasjon fra ulykkeskjøretøyet til andre kjøretøy i nærheten, men det foregår forskning på denne type løsninger også.

Datatilsynet er involvert i en arbeidsgruppe som arbeider med hvordan en slik ordning kan implementeres i Norge. Arbeidsgruppen anerkjenner at formålet med systemet er godt, men

påpeker samtidig at systemet reiser flere problemer med hensyn til personopplysningsvern, og foreslår at den enkelte må kunne bestemme om systemet skal være aktivert eller ikke (Fornyings- og administrasjonsdepartementet 2009).

Hva slags personopplysninger behandles?

Når eCall-systemet aktiveres, overføres automatisk informasjon om tidspunkt for ulykken, kjøretøyidentifikasjon, stedfesting av ulykkespunkt og hvilken retning kjøretøyet beveget seg før ulykken inntraff, samt eventuelle data fra bilens sensorer (i det minste om varslingen ble utløst manuelt eller automatisk).

I tillegg jobbes det med å etablere løsninger hvor trafikantene kan abonnere på private tilleggstjenester som gjør at supplerende opplysninger overføres til nødsentralen når en ulykke inntreffer. Dette kan også være sensitive opplysninger, som for eksempel informasjon om førerens helsetilstand, medisinbruk og lignende.

Hvor i systemet lagres og behandles personopplysninger?

Basert på satellittnavigasjonssystemet, vil man til enhver tid kunne foreta en nøyaktig stedfesting av kjøretøyets posisjon, og det vil være behov for å lagre enkelte opplysninger i en enhet i kjøretøyet. I prinsippet kan mye informasjon om kjøretøyets (og førerens) posisjon lagres, men slik eCall-systemet er beskrevet per i dag, vil det kun være nødvendig å lagre bilens siste bevegelser.

Det er opp til hver enkelt om man ønsker å tegne abonnement på eventuelle tilleggstjenester. Slik mulighetene beskrives i forskningsprosjektet, kan det bli aktuelt at en eller flere private aktører tilbyr seg å lagre informasjon om helsetilstand, medisinbruk og andre opplysninger, slik at man ved en ulykkessituasjon gjør dette tilgjengelig for nødmeldingsentralen.

Nødmeldingsentralen vil kun motta personopplysninger når en ulykke inntreffer. Da vil dataene sannsynligvis lagres på samme måte som andre meldinger til nødmeldingsentralen.

Personregistre som kan være involvert

Ved nødsentralen vil det være behov for å bruke kjøretøyregisteret eller andre register som identifiserer kjøretøyet. Ved etablering av tilleggstjenester, vil private aktører operere med register over personopplysninger som den enkelte ønsker skal gjøres kjent for hjelpepersonell ved ulykker.

Behandlingsansvarlig og databehandler

Nødsentralen og ambulansetjenesten vil allerede i dag være behandlingsansvarlig for personopplysninger i forbindelse med nødmeldinger som ringes inn. Dersom eCall-systemet medfører nye aktører og organisasjoner, vil også disse være behandlingsansvarlig.

Utrykningspersonell og medisinsk personell som behandler trafikantene, vil være databehandlere. Nødsentralen og hjelpepersonell behandler personopplysninger også i dag. De største forskjellene i hvem som får tilgang til personopplysninger, ligger i mulighetene for etablering av nye organisasjoner og private aktører i tilknytning til eCall-systemet. Systemet vil imidlertid gi tilgang

på mer data enn man har hatt tidligere, gjennom rutiner for automatisk overføring av data og identifisering av kjøretøy.

Hvem er berørt?

På sikt vil alle trafikanter omfattes av eCall-systemet, ved at det blir standardutstyr på alle nye biler. Man kan tenke seg en ordning basert på frivillighet, som gjør at man kan velge å deaktivere systemet.

Systemet har størst implikasjoner for personvernet til de trafikantene som er involvert i ulykker eller som velger å registrere sensitive opplysninger hos private aktører som tilbyr tilleggstjenester.

Tabell 14: Oppsummering av forhold som berører personvern ved systemet eCall.

Oppsummering: eCall	
Type personopplysninger	*Kjøretøyidentifikasjon, stedfesting av ulykkespunkt, tidspunkt for ulykke, evt. data fra bilens sensorer (minimum: om varslingen ble utløst manuelt eller automatisk).* *I tillegg kan det etter hvert være mulig å abonnere på private tilleggstjenester som innebærer lagring og behandling av sensitive personopplysninger.*
Hvor i systemet lagres og behandles personopplysninger?	*I kjøretøyet og evt. hos private aktører som tilbyr tilleggstjenester. Ved ulykker vil data overføres og behandles hos en nødsentral.*
Personregistre som kan være involvert	*Kjøretøyregisteret eller andre register som identifiserer kjøretøyene. Evt. private register over opplysninger som hver enkelt ønsker skal gjøres kjent ved en ulykkessituasjon.*
Behandlingsansvarlig	*Nødsentral og ambulansetjeneste er behandlingsansvarlig, og eventuelle private aktører som håndterer personopplysninger.*
Databehandler	*Operatører, utrykningspersonell og medisinsk personell som behandler trafikanter som er involvert i trafikkulykker.*
Hvem blir berørt (brukere)?	*Systemet vil i størst grad påvirke de som er involvert i trafikkulykker, men i utgangspunkter er alle trafikanter (i bil) berørt, ved at eCall-systemet lagrer kjøretøyets siste bevegelser i atferdsregistratoren. De som velger å benytte tilleggstjenester kan få mulighet til å registrere sensitive personopplysninger hos private aktører.*

2.13 Lagring av data i bilen

De fleste av bilens funksjoner styres i dag elektronisk, og informasjon om disse funksjonene lagres i bilens databrikker. ISA med lagring av data, som nevnt i avsnitt 2.7, er ett eksempel, mens flere eksempler på bruksområder og data for dagens anvendelser og framtidige løsninger er gitt i ETSI (2010). Siden 1996 er alle nye biler utstyrt med OBD-II-system (On-board Diagnostics System). Hensikten med dette systemet er blant annet å lette arbeidet for verkstedene som skal utføre service og reparasjoner på kjøretøyet, ved at de automatisk kan hente ut feilmeldinger og informasjon fra den elektroniske kontrollenheten (www.obdii.com).

De færreste bilførere er klar over at kjøretøyet lagrer informasjon om atferd og forhold ved kjøretøyet. En artikkel i Samferdsel (2008) diskuterer personvernaspekter knyttet til lagring av data på denne måten. Noen av dataene lagres i hele bilens levetid, mens andre data lagres i perioder, gjerne over flere år. I utgangspunktet er det bilens eier som også bestemmer over dataene og hvem som skal få tilgang, men bileierne har sjelden oversikt over hvilke opplysninger som finnes. Verkstedene har tilgang til de dataene de trenger for å utføre nødvendig vedlikehold, og politiet og Havarikommisjonen kan hente ut data fra bilens datasystem ved etterforskning av ulykker.

I prinsippet kan hvem som helst gå til innkjøp av utstyr som gjør det mulig å hente ut opplysninger som er lagret i bilens datasystem.

Hva slags personopplysninger behandles?

Kjøretøyet lagrer informasjon om hastighet, motorturtall, utslipp av forurensing, bruk av bremser og antiskrenssystem, innstilling av speil og sete, vindusstilling, bruk av lys, data fra kollisjonsputesensorer, GPS-informasjon (posisjon, tidspunkt, fart), informasjon om bilens eier m.m.

Hvor i systemet lagres og behandles personopplysninger?

Opplysninger lagres i bilens datasystem, men også bilnøkkelen er utstyrt med en databrikke hvor informasjon om bilens eier ligger lagret.

Bilverkstedene henter ut informasjon for å utføre sitt arbeid på best mulig måte, og denne informasjonen lagres sannsynligvis i verkstedets egne datasystem.

Personregistre som kan være involvert

I utgangspunktet involveres ikke personregistre, men informasjon kan muligens knyttes til kunderegister hos bilverkstedene.

Behandlingsansvarlig og databehandler

Bileieren er i utgangspunktet selv behandlingsansvarlig og bestemmer over dataene og hvem som skal få tilgang, men som regel har bileier liten oversikt over hva som lagres av informasjon i kjøretøyet.

I utgangspunktet er det ansatte hos verkstedene som behandler data fra kjøretøyet. Bilverkstedene og eventuelle andre eksterne aktører er behandlingsansvarlige og bør definere hvordan personopplysninger skal håndteres i bedriften.

I spesielle tilfeller kan ansatte hos politi og Havarikommisjon være behandlingsansvarlige.

Hvem blir berørt?

Alle bileiere (med biler fra 1996 eller senere), eller eventuelt også brukere av disse kjøretøyene, berøres av systemet.

Tabell 15: Oppsummering av forhold som berører personvern ved lagring av data i bilen.

Oppsummering: Lagring av data i bilen	
Type personopplysninger	*Kjøretøyidentifikasjon og informasjon om atferd og forhold ved kjøretøyet.*
Hvor i systemet lagres og behandles personopplysninger?	*Informasjon lagres i bilens datasystem. Hvem som helst kan anskaffe utstyr som gjør det mulig å hente ut opplysninger, men i utgangspunktet bruker verkstedene dette for å utføre service og nødvendige reparasjoner. Politiet og Havarikommisjon kan bruke bilens datasystem ved etterforskning av ulykker.*
Personregistre som kan være involvert	*Personregistre er i utgangspunktet ikke involvert.*
Behandlingsansvarlig	*Bileier bør i utgangspunktet være behandlingsansvarlig for egne data, men har ofte liten oversikt over hva som lagres av informasjon. Verksteder og andre eksterne aktører er behandlingsansvarlige og regulerer hvordan data som benyttes i deres arbeid skal håndteres. Havarikommisjon og politi i spesielle tilfeller.*
Databehandler	
Hvem blir berørt (brukere)?	*Bileier eller eventuelle brukere av et kjøretøy.*

2.14 Oppsummering

Intelligente transportsystem (ITS) har i løpet av de siste årene blitt et viktig begrep i veisektoren. Den teknologiske utviklingen har gitt oss nye og effektive løsninger innenfor områder som trafikantinformasjon, trafikk- og flåtestyring, førerstøttesystem og navigasjon, overvåking og kontroll, drift av infrastruktur og betalingssystem. Felles for ITS-løsningene er at de baserer seg på elektronisk innsamling og bruk av data. Begrunnelsen for å utvikle og ta i bruk ITS-løsninger er at det anses å ha et enormt potensial for å oppnå sikrere og mer effektive transportsystem. Samtidig er det sterke drivkrefter som bidrar til denne utviklingen, gjennom myndigheter, fagmiljø og markedskrefter.

Ut ifra personvernhensyn kan de nye teknologiske mulighetene representere store utfordringer. Økt bruk av elektronisk registrering og lagring av data gjør at det samles inn svært store mengder data i forbindelse med transport, og det kan være mange grunner til å bruke data til andre formål enn det som opprinnelig var tenkt. Systemene utgjør en infrastruktur som kan tas i bruk på flere måter med tilgang til nye aktører. Dette er ikke forenelig med målene i Personopplysningsloven.

Samtidig er det et paradoks at det nettopp er bruk av samvirkende system og kobling av ulike registre som gir størst potensiell effekt for oppnåelse av transportpolitiske mål. ITS bidrar også til å gi trafikanter store fordeler med hensyn til komfort, effektivitet og sikkerhet, og løsningene vil i mange tilfeller tas godt imot av brukerne.

I ***Tabell 16*** oppsummerer vi noen momenter knyttet til behandling av personopplysninger for de ITS-løsningene som er beskrevet foran.

Tabell 16: Oppsummering av vesentlige forhold ved personvern for utvalgte ITS-løsninger.

ITS-applikasjoner	Omfang og type personopplysninger	Lagring og behandling	Behandlingsansvarlig, antall aktører	Hvem blir berørt
Kamera-overvåking	Ikke-sensitive, men omfattende: Person, sted, tid og atferd. Kan berøre privatlivets fred.	Videoopptak lagres og behandles hos aktør eller tredjepart som drifter systemet. Ikke personregistre.	Offentlige og private, flere aktører: Statens vegvesen, kollektivterminaler, private selskap. .	Alle personer i det aktuelle området.
Automatisk nummerskilt-gjenkjenning	Ikke sensitive: Kjøretøy, eier, passeringssted og tid. Kan berøre privatlivets fred.	Lagres i veikantutstyr og aktørens sentralsystem. Behandling avhenger av formålet. Kobles med kjøretøyregistre, folkeregisteret, oversikt over stjålne kjøretøy.	Offentlige og private, flere aktører: Kan være myndigheter og private aktører avhengig av formålet.	Alle bileiere og bilførere.
Automatisk trafikkontroll	Sensitive: Kjøretøy og bilfører, passeringssted og tid, evt. trafikkforseelser.	Lokalt i veikantutstyr, hos Statens vegvesen og Politiet. Kobles med kjøretøyregister og prikkbelastningsregister.	Offentlige, kun bestemte aktører: Statens vegvesen og Politiet	Potensielt alle bilførere, ved trafikkforseelser (fartsgrense og signalanlegg).
Elektronisk billettering	Ikke sensitive: Person, tid, rute og holdeplass eller sone for på-/avstigning. Berører personlig økonomi.	Reiseopplysninger lagres på elektronisk billett og i sentral database hos selskapene. Personopplysninger lagres i kunderegister (kollektivselskap, administrasjonsselskap), ønskes koblet mot folkeregisteret.	Private og evt. offentlige, flere aktører: Kollektivselskap og evt. administrasjonsselskap.	Kollektivtrafikanter som velger elektronisk billettering.
Elektronisk betaling av bompenger	Ikke sensitive: Kjøretøy, eier, passeringssted og tid. Berører personlig økonomi.	I AutoPASS-brikken (kun brikkeid), lokalt i veikantutstyr og i driftsselskapenes sentralsystem (betalingsform avgjør lagringstid). Kobles med kunderegister. Ved passering av kjøretøy uten AutoPASS-brikke gjelder automatisk nummergjengkjenning.	Offentlige og private, flere aktører: Statens vegvesen, bompengeselskap, driftsoperatører og forhandlere.	Alle bileiere med AutoPASS avtale.

Tabell 16 forts.: Oppsummering av vesentlige forhold ved personvern for utvalgte ITS-løsninger.

ITS-applikasjoner	Omfang og type personopplysninger	Lagring og behandling	Behandlingsansvarlig, antall aktører	Hvem blir berørt
Utvidet bruk av AutoPASS	Sensitive og omfattende: Kjøretøy, eier, passeringssted og tid, logging og kjørelengde. Evt. betalt årsavgift, EU-kontroll, forsikringsforhold, heftelser, prøvekjennetegn, kjøretøyklassifisering og last. Berører personlig økonomi.	I AutoPASS-brikken (kun brikkeid), veikantsystemet og sentralsystemet hos de ulike operatørene. Kobles med kunderegister og kjøretøyregisteret. Statens vegvesen ønsker sentralt kunderegister.	Offentlige og private, mange aktører: Statens vegvesen og bomselskap, flere aktører ved nye anvendelsesområder for AutoPASS.	Alle bileiere og bilførere.
Intelligente fartstilpasnings-system med atferdsregistrator	Sensitive: Hastighet, fartsgrense og kjørestil, evt. stedfesting. Berører mistanke om straffbare forhold.	Lagres i atferdsregistrator i bil. Mange mulige system, bruksområder og aktører. Vil komme ønsker om å koble registre.	Private, flere aktører: Flere løsninger, formål, behandlingsansvarlig og databehandlere.	Bilførere; arbeidstakere og private.
Alkolås med logging eller varsling	Sensitive: Tidspunkt for blåseprøve og evt. promille. Berører mistanke om straffbare forhold.	Data lagres i en enhet i kjøretøyet og evt. hos arbeidsgiver eller kontrollør. Involverer ikke personregistre.	Private og evt. offentlige aktører, flere: Arbeidsgiver, forsikring, myndigheter.	Ansatte, personer med pålagt bruk av alkolås, alle bilførere.
Lokasjonsbaserte tjenester	Ikke-sensitive: Bruker, posisjonering (sted og tid). Kan berøre privatlivets fred.	Hos tjenestetilbyder eller operatør av systemet, mange aktuelle aktører.	Private, mange aktører: Tjenestetilbyder og operatør av systemet.	Alle brukere.
Sporing av kjøretøy	Ikke sensitive: Kjøretøy, posisjonering (tid og sted). Kan berøre privatlivets fred.	I sporingsenhet, samt datakilde valgt av den som anskaffer sporingsutstyret. Involverer ikke personregistre.	Private og evt. offentlige, flere aktører: Private aktører. Ved teknisk sporing i politietterforskning, vil påtalemyndigheten være behandlingsansvarlig.	Ansatte, bilfører i kjøretøy med sporingsenhet (evt. uten å vite det).
Overvåking av yrkestransport	Sensitivt og omfattende: Kjøretøy, bilfører, posisjonering, data om varer, kjøreoppdrag og gjennomføring, f.eks. overholdelse av kjøre-/hviletid. Kan berøre mistanke om straffbare forhold.	Lagres elektronisk i kjøretøyet, samt i dataregistre hos kontrollør (Statens vegvesen, Politiet) eller arbeidsgiver. Kobles med kjøretøyregistre og evt. andre registre.	Offentlige og private, flere aktører: Statens vegvesen (tungbilkontroller), politiet (kontroller) og arbeidsgiver ved flåtestyring o.l.	Ansatte og bedrifter i transportnæringen.
eCall	Ikke sensitive, evt. sensitive personopplysninger ved frivillige private tilleggstjenester: Kjøretøy (eier), sted og tid.	Posisjonsdata (siste posisjon) lagres i bilen. Behandles ved nødsentral og evt. private aktører (tilleggstjenester). Kobles med kjøretøyregistre og evt. private registre (tilleggstjenester).	Offentlige og evt. private, flere aktører: Nødsentral, ambulansetjeneste, evt. private aktører (tilleggstjenester).	Alle bileiere
Lagring av data i bilen	Ikke sensitive: Kjøretøy, forhold ved kjøretøyet, informasjon om atferd. Kan berøre privatlivets fred.	Lagres i bilens datasystem. Behandles av verksted, evt. politiet og Havarikommisjonen. Alle kan anskaffe utstyr for å hente ut opplysninger. Involverer ikke personregistre.	Private aktører, evt. offentlige, potensielt mange aktører: Verksted, evt. politiet og Havarikommisjonen.	Alle bileiere.

Bruk av personopplysninger kan utgjøre en risiko for personvernet, når det gjelder forhold knyttet til liv og helse, økonomi, anseelse og integritet for enkeltmennesker. I veitransport er sensitive personopplysninger i liten grad involvert, men helseopplysninger og mistanke om straffbare forhold kan være aktuelt for noen anvendelser (eksempelvis eCall, alkolås, automatisk trafikkontroll og intelligente fartstilpassere). Taushetsplikt i forbindelse med sensitive eller intime data kan være motivasjon for å innføre personvernfremmende teknologier.

Personopplysninger kan få konsekvenser for den enkeltes økonomi. Andre opplysninger kan i seg selv være relativt uskyldige, men omfanget av personopplysninger kan oppleves som truende for den enkeltes privatliv og integritet. Når det gjelder data om posisjon (sted og tid) registrerer noen ITS-løsninger kjøretøyet (og evt. bilfører) i bestemte passeringssnitt (som f.eks. trafikkovervåking, automatisk nummerskiltgjenkjenning og elektronisk betaling i bomstasjoner), mens andre løsninger registrerer tid og sted kontinuerlig (lokasjonsbaserte tjenester og sporing av kjøretøy). Noen løsninger kan oppleves som omfattende fordi de også registrerer atferd (kameraovervåking, registrering av data i bilen, intelligente fartstilpassere) og fordi man ikke nødvendigvis er klar over at man blir registrert.

De fleste løsningene kan i teorien berøre alle trafikanter eller bileiere og bilførere, selv om noen løsninger begrenser seg til ansatte i bestemte bedrifter. I et samfunn hvor data registreres i stadig større grad, kan det være vanskelig for den enkelte å skaffe seg oversikt over omfanget av persondata som behandles. Spørsmålet blir da om brukerne er klar over risiko og konsekvenser knyttet til omfanget av personopplysninger andre får tilgang til.

For de fleste løsningene kan behandlingsansvarlig være offentlige eller private aktører, avhengig av anvendelsesområdet. Ofte formidles også data mellom ulike aktører. Automatisk trafikkontroll skiller seg ut ved et begrenset antall offentlige behandlingsansvarlige. Utvidet bruk av AutoPASS, lokasjonsbaserte tjenester og delvis også datalagring i bil er system som kan innebærer mange behandlingsansvarlige, og for datalagring i bil er det tildels uklare ansvarsforhold.

Denne gjennomgangen viser at det ikke er lett å klassifisere eller gruppere de ulike ITS-løsningene i veisektoren ut fra forhold ved registrering, lagring og behandling av personopplysninger. Videre i rapporten belyser vi risiko ved behandling av personopplysninger i intelligente transportsystem. Vi har valgt ITS-løsninger som omfatter personvernimplikasjoner av forskjellig karakter som case i risikoanalysen: Automatisk nummerskiltgjenkjenning, sporing av kjøretøy, lokasjonsbaserte tjenester og intelligente fartstilpasningssystem med lagring av data.

Teknisk sett finnes det uante muligheter for dataregistrering og sporing, men personvernhensyn må legge føringer og begrensninger for anvendelse av teknologi. Dette er i stor grad politiske valg som bør bygge på en samlet vurdering av ulike samfunnseffekter.

3 Risiko ved behandling av personopplysninger i intelligente transportsystem

I det foregående kapitlet har vi beskrevet et utvalg intelligente transportsystem som benyttes i veisektoren, der dette kan ha implikasjoner for personvernet. Vi har valgt å se videre på noen system som på forskjellige måter, etter vår vurdering, kan ha store konsekvenser for personvernet.

Før det besluttes å gjennomføre et tiltak skal den behandlingsansvarlige vurdere personvernkonsekvensene, se kap. 3.1. Kan formålet oppnås med en utforming av tiltaket der man unngår å registrere personopplysninger eller som innebærer mindre grad av registrering? Dersom slik registrering innføres skal behandlingsansvarlig sørge for en forsvarlig behandling av personopplysningene. En risikovurdering tar utgangspunkt i de *opplysningene* som blir behandlet, *sannsynligheten* for uønskede hendelser og *konsekvensene* hvis disse hendelsene skjer. I dette kapitlet presenterer vi metodikk for risikovurdering knyttet til informasjonssystem, før vi ser nærmere på risikoen ved behandling av personopplysninger for

- automatisk nummerskiltgjenkjenning (kapittel 3.3)
- sporing av kjøretøy (kapittel 3.4)
- lokasjonsbaserte tjenester (kapittel 3.5)
- intelligent fartstilpasningssystem med lagring av data (kapittel 3.6)

eCall inngår i vurderingene for sporing av kjøretøy, som et mulig bruksområde. Av de systemene som er omtalt, skiller eCall seg ut ved at personopplysningene kan ha direkte betydning for liv og helse. Av den grunn kan hensynet til datatilgjengelighet komme foran hensynet til konfidensialitet (hindre utlevering) og integritet (sikre korrekte data). Det er foreløpig uklart hvordan eCall som system blir implementert. eCall behandler ikke sensitive persondata i seg selv, men eventuelle tilleggstjenester kan gjøre det.

3.1 Vurdering av personvernkonsekvenser ved utforming av tiltaket

Regjeringen fastslår at det skal legges vekt på hvordan IKT-system i transportsektoren utformes, slik at mulighetene for misbruk av personinformasjon reduseres eller elimineres (Samf.dep. 2009, kap. 14.1). Personvernhensyn skal trekkes inn som et sentralt hensyn fra starten av planlegging og videreutvikling av IKT-system.

Før et tiltak innføres, skal den behandlingsansvarlige vurdere personvernkonsekvensene av tiltaket. Registrering av personopplysninger utgjør en mulig trussel ved at opplysninger kan komme på avveie, misbrukes eller inngå i overvåkning. Dataminimalisme er et sentralt prinsipp i personopplysningslovgivningen; å registrerer så få opplysninger som mulig, bare det som er nødvendig, og bare så lenge som nødvendig. Det skal vurderes om formålet kan oppnås med andre tiltak som unngår registrering av personopplysninger eller som i mindre grad involverer personopplysninger. Vurderingen skal inkludere om tiltaket har grunnlag i lov eller bygger på informert samtykke fra den registrerte, om den registrerte har tilstrekkelig informasjon, og om det vil ha konsekvenser for den registrerte å nekte å oppgi opplysninger osv. (Fornyings- og administrasjonsdepartementet 2008). Videre må det vurderes om personverninteressene veier tyngre enn formålet med tiltaket.

3.2 Risikovurdering av informasjonssystem

Personvernrisiko er kombinasjonen av konsekvensen en hendelse har for den enkeltes personvern og sannsynligheten for at hendelsen inntreffer. Vurdering av personvernrisiko er dermed en samlet vurdering av sannsynlighet og mulig konsekvens av hendelser.

Risikovurderingen er en vurdering av datasikkerheten og tar ikke stilling til formålet med registrering av personopplysninger eller om tiltaket bør gjennomføres. En risikovurdering tar utgangspunkt i de *opplysningene* som blir behandlet, sannsynligheten for uønskede hendelser og konsekvensene hvis disse hendelsene skjer.

For vurdering av risiko ved behandling av personopplysninger, legger vi til grunn metoden for risikovurdering av informasjonssystem beskrevet av Datatilsynet (2002). Risikovurdering har som formål å identifisere *hendelser* som kan få betydning for sikring av personvernet, dvs. hendelser knyttet til konfidensialitet, integritet og tilgjengelighet av personopplysninger. Videre beskrives *konsekvenser* for personvernet; forhold knyttet til liv og helse, personens økonomi, eller anseelse og integritet for enkeltmennesket, *Sannsynligheten* for at en hendelse skal inntreffe, kan vurderes i forhold til hvor mye som skal til av tilfeldigheter eller menneskelig aktivitet basert på kvalifisert kunnskap og grad av besluttsomhet. Vil uaktsomhet, forsett eller overlegg være tilstrekkelig? I tillegg vurderes akseptabelt risikonivå og nødvendige tiltak for å opprettholde et akseptabelt risikonivå.

Metoden slik den beskrives, er ment for virksomheter for å vurdere risikoen i konkrete system med konkrete formål med behandlingen av personopplysninger. Det er ofte hensiktsmessig å drøfte hendelsene i en workshop eller tilsvarende arbeidsform, der aktører som kjenner systemet fra ulike sider (interesser, roller) sammen kan drøfte mulige konsekvenser og sannsynlighet. En og samme hendelse kan medføre konsekvenser av ulik alvorlighetsgrad. Vurdering av resulterende risikonivå kan derfor være en avveining av sannsynligheten for ekstreme konsekvenser (for noen få) og sannsynligheten for mindre alvorlige konsekvenser som kanskje rammer flere. For en konkret vurdering vil det være aktuelt å stille opp:

- Beskrivelse av akseptabelt risikonivå
- Identifisering av uønskede hendelser
- Konsekvensvurderinger av hver av de uønskede hendelsene
- Vurdering av sannsynlighet for hver av de uønskede hendelsene
- Resulterende risikonivå og nødvendige tiltak for å opprettholde akseptabelt risikonivå

Gjennomgangen her blir generell da vi ikke har bestemte bedrifter, registre eller fysiske omgivelser i tankene. Vi kan ikke fastsette et akseptabelt risikonivå, men drøfte noen konsekvenser av ulike nivå. Likeledes gis en mer samlet framstilling av hendelser, konsekvenser og sannsynlighet for å unngå unødvendige gjentakelser.

3.2.1 Akseptabelt risikonivå er en vurdering virksomheten må gjøre

Iht. Personopplysningsloven § 2-4 Risikovurdering, skal virksomheter føre oversikt over hvilke personopplysninger som behandles. Virksomheten skal selv fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger. For å kunne si noe om kriteriene for akseptabel risiko er det nødvendig å kartlegge:

- *Verdiene*; dvs. personopplysninger som virksomheten skal sikre konfidensialitet, integritet eller tilgjengelighet for. Gjelder personopplysningene sensitive data, intime data, omfattende informasjon om personen osv.
- *Miljøet* som disse verdiene befinner seg i, dvs. informasjonssystemet, fysiske installasjoner og organisasjonen.
- Mulige *hendelser* som kan ha konsekvens for personvernet, konsekvensene hvis de skjer, og sannsynligheten for at de inntreffer.

Vår vurdering er at virksomheter innenfor transport som et minimum bør sette akseptabelt risikonivå slik at hendelser som medfører uopprettelige konsekvenser for liv, helse og (kundens og tredjeparts) økonomi unngås. Dette kan gjerne gjøres gjennom en policy for informasjonssikkerhet som gjøres lett tilgjengelig for brukerne av systemet.

3.2.2 Beskrivelse av den registrerte, verdiene og hendelser

Den registrerte

Den registrerte omtaler vi som trafikanten; dette kan være bileier, bilfører eller andre trafikanter som registreres i systemet. I mange tilfeller omtales den registrerte som kunde, dvs. når trafikanten har inngått et kundeforhold til databehandler eller behandlingsansvarlig. Et kundeforhold innebærer en frivillig avtale og, som regel, økonomiske forpliktelser for begge parter.

Verdiene – når disse er lokasjonsdata

I de etterfølgende avsnittene presenterer vi risikovurderinger for automatisk nummerskiltgjenkjenning, sporing av kjøretøy, lokasjonsbaserte tjenester og intelligent fartstilpasningssystem med lagring av data. Felles for disse ITS-anvendelsene er at personopplysningene i liten grad gir sensitiv eller intim informasjon[12]. Derimot ser vi at noen av anvendelsene kan oppleves som omfattende overvåking, fordi de kan gi informasjon om hvor en person befinner seg, i noen tilfeller nesten til enhver tid. Denne informasjonen kan i noen tilfeller oppleves krenkende for den registrerte.

- Lokasjonsopplysninger (tid og sted) kan knyttes til helse, religion, partipolitikk, regelbrudd og kriminell aktivitet osv. Informasjon om hvor man har vært kan brukes til å trekke slutninger om hvilke helsetjenester man har oppsøkt, deltakelse i religiøse eller politiske aktiviteter, demonstrasjoner osv., eller at man ikke har befunnet seg der man oppgir å ha vært. Eksempelvis kan lokasjon av en mobiltelefon i noen tilfeller bestemmes ned til 1 m nøyaktighet (Gruteser & Grunwald 2005). For noen bruksområder kan informasjon evt. også benyttes for å trekke slutninger om regelbrudd, som f.eks. fartsoverskridelser.
- For personer som opplever trusler og forfølgelse vil det være spesielt alvorlig dersom utenforstående kan få tak i informasjon om hvor de er, hvor de har vært og hvor de pleier å ferdes. Dette gjelder et fåtall personer, men ser ut til å være et økende problem. Forfølgelse av

[12] Sensitiv informasjon er i Personopplysningsloven definert som opplysninger om rase, etnisk bakgrunn, helse, seksuelle forhold, politisk, filosofisk eller religiøs oppfatning, medlemskap i fagforeninger, og mistanke om eller dom for straffbar handling. Intim informasjon defineres i (Raguse m.fl. 2008a) som opplysninger gitt i fortrolighet, personlig korrespondanse og forhold knyttet til kroppslig nærhet.

kjente personer er et økende problem i flere land. Også antall personer som har behov for beskyttelse, voldsalarm og skjult identitet øker. I disse tilfellene vil også "forfølgerne" ha en sterk motivasjon for å få tak i opplysningene.

Identifisering av uønskede hendelser – brudd på konfidensialitet, integritet og tilgjengelighet

Informasjonssikkerhet omfatter konfidensialitet, integritet og tilgjengelighet. *Konfidensialitet* innebærer at informasjonen ikke skal være tilgjengelig for uvedkommende. *Integritet* innebærer at personopplysningene skal beskyttes mot uønskede og ikke-autoriserte endringer. *Tilgjengelighet* innebærer at personopplysningene skal være relevante, tilstrekkelige og tilgjengelig for autorisert behandling. Uønskede hendelser kan grovt deles inn i ureglementert utlevering (brudd på konfidensialitet), endring (brudd på integritet) og utilgjengelighet av data.

3.2.3 Hvilke konsekvenser kan en hendelse få?

Konsekvensvurdering er en vurdering av hvilke følger de ulike hendelsene kan få, med utgangspunkt i målet med sikring av personopplysninger: Beskyttelse av liv og helse, personlig integritet, makt og beslutninger, omdømme og økonomi for enkeltmennesket. Personvernkonsekvensene av en hendelse er i første rekke knyttet til verdiene, dvs. personopplysningenes art, og beskrives kvalitativt og kvantitativt ved å besvare spørsmål av typen: Hvis hendelsen skjer, hva kan dette medføre?

I tillegg vil konsekvens avhenge av hvor mange personer som berøres, hvem informasjonen spres til (nærhet til den det gjelder), geografisk og tidsmessig omfang. Forholdet til liv og helse og om konsekvensene er reversible står sentralt. Datatilsynet angir en gradering med fire kategorier av personvernkonsekvenser:

K = 4: Hendelsen kan føre til tap av liv eller vedvarende helsetap, eller betydelig og uopprettelig økonomisk tap, eller alvorlig tap av anseelse eller integritet som påvirker liv, helse eller økonomi.

K = 3: Hendelsen kan føre til tap av helse, uopprettelig økonomisk tap eller alvorlig tap av anseelse og integritet.

K = 2: Hendelsen kan medføre betydelig, men gjenopprettelig økonomisk tap eller tap av anseelse eller integritet (knyttet til opplysninger den registrerte oppfatter som krenkende eller som andre kan gjøre seg nytte av).

K = 1 Hendelsen kan medføre økonomisk, men gjenopprettelig tap eller tap av anseelse eller integritet (knyttet til opplysninger den registrerte oppfatter som følsomme).

Hendelsene har betydning for de personene som rammes, for virksomheten, og for tilliten til sektoren og samfunnsaktører for øvrig. I tillegg til å vurdere personvernkonsekvensene, kan det være aktuelt for en virksomhet å vurdere hva det vil koste dem av tiltak å rette opp igjen skade og tillit, når en hendelse skjer.

3.2.4 Hvor sannsynlig er det at hendelsen skjer?

Datatilsynet (2002) angir tre innfallsvinkler til vurdering av sannsynligheten for at en hendelse skal skje: Hvor ofte har det skjedd før (historiske data)? Hva skal til eller hvor lite skal til for at

det skjer (mulighet)? Hvorfor vil noen at det skal skje (motivasjon)? For å beskrive mulighet og motivasjon, kan personer som utgjør en trussel for personvernet deles i fire grupper:

- Dyktige utenforstående; faglig dyktige med nødvendig ”verktøy” som utnytter kjente svakheter i systemet.
- Kunnskapsrike utenforstående som har teori, praksis og ”verktøy” spesielt utviklet for å angripe IT-system.
- Organisasjoner med økonomisk støtte; grupper av utenforstående som har tilgang på eksperter, økonomisk støtte og siste nytt innenfor ”verktøy”.
- Insidere som har tilgang til følsom informasjon, prosesser og moduler som kan utnyttes/misbrukes av disse personene eller utenforstående.

Med utgangspunkt i begrepene uaktsomhet, forsett og overlegg, kan sannsynlighet beskrives på en 4-delt skala:

S = 4: Svært høy sannsynlighet for at hendelsen inntreffer:

Sikkerhetsbrudd kan skje ved uaktsomhet, ubevisst eller uten forsett, av egne medarbeidere eller utenforstående. Det er ikke nødvendig med spesielle kunnskaper om interne forhold.

S = 3: Høy sannsynlighet for at hendelsen inntreffer:

Sikkerhetsbrudd kan skje ved uaktsomhet av egne medarbeidere. Utenforstående må ha noe kompetanse, og forsettelig (bevisst eller aktivt) gå inn for å bryte sikkerhetstiltakene.

S = 2: Moderat sannsynlighet for at hendelsen inntreffer:

Sikkerhetsbrudd kan skje ved at egne medarbeidere opptrer med forsett og har en viss kompetanse. Utenforstående må opptre med overlegg og noe kunnskap om interne forhold (med hensikt og plan, eksempelvis ved at flere tiltak brytes i riktig rekkefølge) for å omgå/bryte sikkerhetstiltakene.

S = 1: Lav sannsynlighet for at hendelsen inntreffer:

Sikkerhetsbrudd kan kun skje ved at egne medarbeidere opptrer med overlegg og har spesiell kompetanse eller kunnskap. Utenforstående må ha spisskompetanse og samarbeid med personer i virksomheten.

3.3 Risikovurdering ved automatisk nummerskiltgjenkjenning

Automatisk nummerskiltgjenkjenning benyttes blant annet for betaling eller adgangskontroll i parkeringsanlegg, bomstasjoner, miljøsoner og anleggsområder (se kap.2.2). Kontrollen gjennomføres effektivt ved å sjekke bildet av registreringsnummeret mot en database. Metoden kan også benyttes for å spore opp stjålne kjøretøy og evt. annen kriminalitet knyttet til bilbruk. Vi har identifisert følgende ulike bruksområder for automatisk nummerskiltgjenkjenning:

- Betaling i betalingssystem (bompengesystem, parkering, ferge osv.).
- Kontroll / håndtering av manglende betaling i betalingssystem (dette utløser lagring av bilde).
- Adgangskontroll (til parkering, anlegg osv.) der registreringsnummeret blir sjekket mot en hviteliste (white list).

- Trafikkontroller som i noen tilfeller utløser lagring av bilde (fartsgrense, betalte avgifter, gjennomført EU-kontroll, ettersøkte kjøretøy der registreringsnummeret blir sjekket mot en svarteliste (black list) osv).
- Trafikkanalyser, dvs. kartlegging av dagens trafikkmønster (fra/til reisemønster, OD-matrise).

For hvert bruksområde er det en behandlingsansvarlig som bestemmer hvilke data som skal registreres og hvordan de skal behandles, og en eller flere databehandlere.

3.3.1 Nummerskiltgjenkjenning: Hvilke verdier skal sikres

I kapittel 1 presenterte vi hvordan personopplysningsloven definerer personopplysninger, sensitive opplysninger, registrering og behandling. Der nevner vi også kort ulike verdispørsmål og hensyn som ligger til grunn for å beskytte personopplysninger.

Ved automatisk nummerskiltgjenkjenning identifiseres kjøretøy og bileier, og i noen tilfeller sted og tid ved passering (posisjon). I tillegg kan disse dataene i noen tilfeller knyttes mot bilder eller informasjon i andre registre. Dette vil ytterst sjelden gjelde intime personopplysninger (opplysninger gitt i fortrolighet, innerste tanker, kroppslig nærhet osv.) og opplysningene er bare sensitive i den grad de kan knyttes til kriminell aktivitet. Opplysningene skal også beskyttes i forhold til om de har konsekvenser for personens økonomi, identitet og omdømme eller makt og beslutninger som gjelder enkeltindividet.

System for automatisk nummerskiltgjenkjenning inneholder verdier som skal sikres i forhold til konfidensialitet, integritet og tilgjengelighet. Dette gjelder eksempelvis utstyr, programvare og informasjon. Flere registre kan være aktuelle; kjøretøyregisteret, kunderegistre, oversikt over stjålne kjøretøy osv. Systemet består av følgende hoveddeler:

- Dynamiske data om passeringer (nummerskilt, tid og sted) som registreres i veikantutstyr.
- Når nummerskiltet ikke identifiseres entydig, eller har betydning som bevis, oversendes foto av kjøretøyet for manuell behandling i sentralsystemet.
- De dynamiske dataene sjekkes mot ulike registre (statiske data) for ulike bruksområder: Kunderegistre, adgangsregistre, kjøretøyregisteret, registre over stjålne kjøretøy eller kjøretøy involvert i kriminalitet osv.
- Evt. hvitelister og svartelister oppdateres og sendes fra sentralsystemet til veikantutstyret, der det lagres lokalt.
- For andre registre sendes det en forespørsel til det aktuelle registeret, og opplysningene behandles i sentralsystemet.

3.3.2 Nummerskiltgjenkjenning: Miljøet verdiene befinner seg i

Hvordan opplysningene lagres og behandles avhenger av formålet med nummerskiltgjenkjenningen. Ofte vil data lagres både i veikantutstyret og i sentralsystemet hos databehandler.

Normalt vil *sentralsystemene* være i beskyttede miljø både fysisk og logisk, der operatørene har opplæring i informasjonssikkerhet og har undertegnet taushetserklæringer. Bruken av systemet registreres slik at avvik kan detekteres og følges opp (dette er i seg selv personopplysninger

knyttet til de ansatte, og må følges opp deretter). Systemene er beskyttet i forhold til vann, brann og eksterne inntrengere.

Veikantutstyret er mindre beskyttet i forhold til vær og klima og ytre påvirkninger. Tilgang til informasjonen kan beskyttes med brukernavn og passord, men informasjonsmediet kan fjernes fysisk.

Som nevnt sendes informasjon mellom ulike registre og sentralsystem og mellom sentralsystem og veikantutstyr. En behandlingsansvarlig skal bare sende fra seg informasjon dersom man har trygghet for at den som tar imot informasjonen har en forsvarlig sikkerhet. Utenforstående kan forsøke å få tilgang til *informasjon som sendes*. Denne informasjonen bør derfor sikres ved hjelp av kryptering etc., der mottaker kvitterer for at informasjonen er mottatt i intakt tilstand.

3.3.3 Nummerskiltgjenkjenning: Identifisering av uønskede hendelser

Ved gjennomgangen av mulige uønskede hendelser har vi sett på ulike mulige anvendelsesområder for automatisk nummerskiltgjenkjenning samlet. *Alle hendelser og konsekvenser vil ikke være aktuelle for alle bruksområder, hvis man ser på hvert bruksområde isolert.* Mange av hendelsene som er beskrevet gjelder betalingssystem. Som nevnt er det en behandlingsansvarlig for hvert bruksområde som bestemmer hvilke data som skal registreres og hvordan de skal behandles, og en eller flere databehandlere.

Behovet for konfidensialitet, integritet og tilgjengelighet:

Verdiene (personopplysningene) skal sikres i forhold til konfidensialitet, integritet og tilgjengelighet. Utgangspunktet er å unngå hendelser som kan bidra til ikke-reversible konsekvenser for liv, helse og (kundens eller utenforståendes) økonomi. I skalaen for konsekvens går det et skille ved K= 2 (se kapittel 3.2.3), der høyere vurdering innebærer ikke-reversible konsekvenser.

- For registreringer som grunnlag for betaling (parkering, bompasseringer, fergetur etc.), er det viktig at informasjonen som registreres er korrekt og ikke kan endres uten saklig grunn (integritet). I enkelte tilfeller eller hvis omfanget blir omfattende, vil passeringsdata fortelle mye om et menneske, og bør derfor holdes konfidensielt. Slik informasjon kan bare gjøres tilgjengelig for autoriserte personer, og det bør registreres hvem som foretar evt. endringer og når de er foretatt.
- Kundeopplysninger som gir grunnlag for faktura bør sikres konfidensialitet, slik at uvedkommende ikke kan få tak i dem. Slik informasjon kan bare gjøres tilgjengelig for autoriserte personer, og det bør registreres hvem som foretar evt. endringer og når de er foretatt.
- For registrering som grunnlag for betaling synes tilgjengeligheten av dataene å være mindre viktig enn konfidensialitet og integritet. Dette vil først og fremst ramme manglende oppgjør for enkeltpasseringer og vil som regel ikke utgjøre vesentlige ulemper.
- Ved autorisasjon (adgangskontroll) og for å identifisere kriminalitet, vil manglende tilgjengelighet kunne ha større konsekvens. Slike registre må sikres mot tilgang for uvedkommende (konfidensialitet) og underlegges strenge krav til beskyttelse og tilgang.

Nedenfor er en oversikt over de identifiserte hendelsene, og vurdert konsekvens og sannsynlighet for hendelsene, se ***Tabell 17***. Vi beskriver de identifiserte hendelsene i forhold til *utlevering* (brudd på konfidensialitet), *endring* (brudd på integritet) og *utilgjengelighet* av data. Hver enkelt hendelse, evt. årsaker og utløsende faktorer, og vurdering av konsekvens, sannsynlighet og resulterende risikonivå, beskrives i **vedlegg**.

Tabell 17: Oversikt over identifiserte hendelser, vurdert konsekvens og sannsynlighet

	Hendelse	Vurdert konsekvens	Vurdert sannsynlighet	Resulterende risikonivå
	Skala:	K (1 – 4)	S (1 – 4)	R = K x S
Utlevering				
1	Informasjon utlevert til uvedkommende	2	2	**4**
2	Informasjon ikke slettet så snart som mulig	3	3	**9**
3	Det innhentes flere opplysninger enn nødvendig	3	1	**3**
4	Informasjon formidles til andre aktører	2	2	**4**
5	Informasjon benyttes til andre formål	2	2	**4**
Endring				
6	Registrerte opplysninger blir endret	3	1	**3**
Utilgjengelighet				
7	Data er ikke tilgjengelig for behandling ved passering	3	2	**6**
8	Data er ikke tilgjengelig for behandling ved avregning	2	1	**2**
9	Data er ikke tilgjengelig for kontroll for kunden	2	2	**4**
10	Trafikanten kjenner ikke hvilke data som er registrert	2	2	**4**

Av tabellen over ser vi at det spesielt er hendelsene 2 og 7 som har høy risiko, dersom vurderingene er fornuftige.

Hendelse 2 innebærer at data om passeringer (evt. beskrivelse av et reisemønster) ikke blir slettet så snart formålet med databehandlingen er oppnådd. Dette vurderes som krenkende (uopprettelig tap) for trafikanten (K = 3). Samtidig varierer bevisstheten rundt sletting av data mellom virksomheter og anvendelsesområder, og hendelsen er vurdert til å ha høy sannsynlighet (S = 3).

Hendelse 7 er knyttet til utilgjengelighet av data. Konsekvensen kan i enkelte tilfeller være alvorlig, mens sannsynligheten er vurdert til å være moderat.

Dersom man aksepterer et risikonivå tilsvarende 4 i tabellen, er det først og fremst tiltak for å redusere konsekvens og sannsynlighet for hendelsene 2 og 7 som må gjennomføres i virksomheten. Dersom man gjør en vurdering som tilsier at akseptabelt risikonivå bør være lavere, ser vi at det vil være mange hendelser som gir grunnlag for tiltaksplaner.

3.4 Risikovurdering ved sporing av kjøretøy

Ved sporing av kjøretøy brukes GPS/GPRS-teknologi og satellittsystem. Data som identifiserer kjøretøyet og informasjon om posisjonen overføres fra en mobil enhet til f.eks. en mobiltelefon, et sentralsystem eller en pc der informasjonen kan presenteres visuelt på et kart.

Sporing av kjøretøy brukes bl.a. til flåtestyring for næringstransport, av private for å finne igjen bilen ved evt. tyveri og av politiet for kriminalitetsbekjempelse. En form for sporing av kjøretøy inngår også i eCall-teknologien.

3.4.1 Sporing: Hvilke verdier skal sikres

System for sporing av kjøretøy inneholder verdier som skal sikres i forhold til konfidensialitet, integritet og tilgjengelighet. Ved sporing av kjøretøy identifiseres kjøretøy og detaljert informasjon om hvor kjøretøyet befinner seg (posisjon) til en hver tid. Data som identifiserer kjøretøyet og informasjon om posisjonen lagres i en mobil enhet, og overføres (jevnlig) fra den mobile enheten til en mottakerenhet, f.eks. en pc, mobiltelefon eller sentralsystem. Systemet består av følgende hoveddeler:

- Dynamiske data om posisjon (kjøretøy-id, tid og sted) registreres fortløpende i mobil enhet.
- De dynamiske dataene om posisjon (kjøretøy-id, tid og sted) overføres fra mobil enhet til mottakerenhet (pc/mobiltelefon/sentralsystem).
- Registre (statiske data) som de dynamiske dataene sjekkes mot. Flere registre kan være aktuelle; kjøretøyregisteret, registre over ansatte/vaktlister, oversikt over stjålne kjøretøy eller kjøretøy involvert i kriminalitet osv. Disse registrene er lagret hos de ulike aktørenes sentralsystem.
- Mottakerenheten gjennomfører evt. spørring i aktuelle registre og sjekk av dynamiske data mot evt. registre skjer i mottakerenheten.

I mange tilfeller kan kjøretøyets eier identifiseres ved hjelp av kjøretøyidentiteten. Disse opplysningene er bare sensitive i den grad de kan knyttes til regelbrudd og kriminell aktivitet. Men fordi de registrerer hvor kjøretøyet oppholder seg til enhver tid, kan registreringen oppleves som omfattende. Det er også et moment at den som blir registrert ikke nødvendigvis er klar over overvåkingen.

eCall avviker fra andre sporingssystem ved at dataene bare lagres i mobil enhet i kjøretøyet. Disse dataene overskrives jevnlig, slik at bare data om de siste posisjonene er lagret. Kun ved utløsing av airbag i bilen blir data om kjøretøyets identitet og posisjon overført til sentral enhet, i dette tilfellet en alarmsentral. Det kan være aktuelt å koble disse dataene med helsedata som kjøretøyeier frivillig har oppgitt for formålet.

3.4.2 Sporing: Miljøet verdiene befinner seg i

Den mobile enheten er festet til bilen og utsatt for de samme påvirkninger som denne. Det fysiske miljøet er sjelden et problem, med unntak av alvorlige hendelser som brann etc. Dersom noen ønsker det, vil det sannsynligvis være mulig å fjerne enheten. Mulighetene for å tappe enheten for data vil avhenge av hvilket produkt som anvendes som mobil enhet.

Ved *privat bruk* vil dataene gjerne sendes til en mobiltelefon eller en pc. Det vil i enkelte tilfeller være lett for andre å få tilgang til disse dataene.

Ved *flåtestyring* og ved oppfølging fra f.eks. *alarmsentral eller politi,* vil dataene være overført til et sentralsystem eller en pc. Normalt vil kontorplass og sentralsystem være i beskyttede miljø både fysisk og logisk, der databehandler har opplæring i informasjonssikkerhet og har undertegnet taushetserklæringer. Bruken av systemet registreres slik at avvik kan detekteres og følges opp. Systemene er beskyttet i forhold til vann, brann og eksterne inntrengere.

Dataene kan være mest ubeskyttet ved *overføring*. Man får relativt lite informasjon ved å snappe opp enkeltoverføringer, men problemet er større dersom man kan fange opp overførte data over tid. Ved å kryptere dataene som overføres kan de sikres mot at uvedkommende oppfatter eller endrer dataene. Ved bruk av en meldingsautentiseringskode (MAC) eller digital signatur kan mottakeren forsikre seg om at dataene som mottas er de samme som de som ble sendt (hele meldingen er mottatt uendret); digital signatur kan også anvendes for å kvittere for mottak.

3.4.3 Sporing: Identifisering av uønskede hendelser

Vi presenterer en oversikt over identifiserte hendelser (utlevering, endring og utilgjengelighet av data) for sporing av kjøretøy i ***Tabell 18***. *Alle hendelser er ikke like aktuelle for alle anvendelsesområder.* Et utgangspunkt er å unngå hendelser som kan bidra til ikke-reversible konsekvenser (K > 2, se kapittel 3.2.3) for andres liv, helse og økonomi. Dette gir følgende behov for konfidensialitet, integritet og tilgjengelighet:

- Sporing av kjøretøy gir kontinuerlig informasjon om hvor kjøretøyet befinner seg. Overvåkingen av bilfører kan derfor oppleves som vesentlig. Dataene bør derfor holdes konfidensielt. Slik informasjon kan bare gjøres tilgjengelig for autoriserte personer, og det bør registreres hvem som har innsyn og for hvilke tidsperioder. Dette er spesielt viktig dersom observasjonene gir grunnlag for å undersøke regelbrudd og kriminell virksomhet.
- Lagring av slike data kan oppleves som massiv overvåking. Hvis slike data skal lagres, må de sikres mot endring og innsyn.
- Manglende data (utilgjengelighet) kan ha økonomiske konsekvenser for enkeltpersoner og virksomheter (redusert effektivitet).
- Manglende data kan ha større konsekvenser for registre som har som formål å identifisere kriminalitet. Slike registre må sikres mot tilgang for uvedkommende (konfidensialitet) og underlegges strenge krav til beskyttelse og tilgang.
- For eCall kan manglende data ha betydning for liv og helse. Kravene til tilgjengelige korrekte data (kjøretøy-id og posisjon) kan ha prioritet foran konfidensialitet. En tilsvarende vurdering kan evt. også gjøres i forhold til innhenting av frivillige private helseopplysninger, og hvor vesentlige disse er i forhold til det helsevesenet på stedet vil ha oversikt over.

Den enkelte hendelse, årsaker og utløsende personer, og vurdering av konsekvens og sannsynlighet for hver hendelse, er presentert i **vedlegg**.

Tabell 18: Oversikt over identifiserte hendelser, vurdert konsekvens og sannsynlighet

	Hendelse	Vurdert konsekvens	Vurdert sannsynlighet	Resulterende risikonivå
	Skala:	K (1 – 4)	S (1 – 4)	R = K x S
Utlevering				
1	Informasjon utlevert til uvedkommende	2	3	**6**
2	Informasjon ikke slettet så snart som mulig	2	3	**6**
3	Det innhentes flere opplysninger enn nødvendig	3	3	**9**
4	Informasjon formidles til andre aktører	2	2	**4**
5	Informasjon benyttes til andre formål	2	2	**4**
Endring				
6	Registrerte opplysninger blir endret	3	1	**3**
Utilgjengelighet				
7	Data er ikke tilgjengelig (andre konsekvenser)	2	2	**4**
8	Data er ikke tilgjengelig (konsekvenser for 3.part)	2	1	**2**
9	Data er ikke tilgjengelig (økonomiske konsekvenser for trafikant)	2	2	**4**
10	Trafikanten kjenner ikke hvilke data som er registrert	2	2	**4**

Av tabellen over ser vi at ifølge de vurderingene som er gjort, så er det spesielt hendelsene 1-3 som har høy risiko, og som krever gjennomføring av tiltak i virksomheten.

Hendelse 1 gjelder utlevering av opplysninger til uvedkommende. Dette oppleves som krenkende for trafikanten. Konsekvensen er vurdert til å være moderat til høy, mens sannsynligheten er vurdert som høy, blant annet basert på muligheten for uaktsomhet blant egne ansatte.

Hendelse 2 gjelder manglende sletting av data når formålet er oppnådd. Dette kan oppleves som krenkende for trafikanten og konsekvensen er vurdert til å være moderat til høy. Sannsynligheten er vurdert som høy, blant annet fordi det er varierende oppmerksomhet rundt sletting av data.

Hendelse 3 gjelder innhenting av personopplysninger som ikke er nødvendige for formålet. Dette er vurdert å være svært krenkende (K= 3). Sannsynligheten er vurdert å være høy (S=3), blant annet basert på muligheten for uaktsomhet og mulighet for kobling av registre hos egne ansatte.

For å hindre disse hendelsene synes det viktig å legge vekt på å utvikle gode sletterutiner, loggføring av databehandling, og å innføre tiltak som sikrer at ulike registre holdes atskilt.

3.5 Risikovurdering ved lokasjonsbaserte tjenester

Lokasjonsbaserte tjenester tilbyr tjenester som er relevante der brukeren befinner seg, som for eksempel navigasjonstjenester, intelligente fartstilpasningssystem i bil, informasjon om kollektivtransport, service og severdigheter langs reiseruta osv., i de fleste tilfeller ved frivillig abonnement på tjenestene. Ved bruk av lokasjonsbaserte tjenester har man mulighet til å finne ut hvor en trafikant eller et kjøretøy befinner seg til enhver tid, ved sporing via satellitt eller

mobiltelefon. Ofte identifiseres brukeren via mobilabonnement. Man kan også formidle hvor man er via sosiale medier.

Dersom man tillater at opplysninger om den enkeltes posisjon og egenskaper formidles til andre brukere, kan man ta i bruk dynamiske tjenester som køvarsling, varsling av glatt veibane basert på friksjonssensorer i kjøretøyene, sporing av pakker via førerens mobiltelefon osv.

3.5.1 Lokasjonsbaserte tjenester: Hvilke verdier skal sikres

System for lokasjonsbaserte tjenester inneholder verdier, dvs. informasjon om hvor individ og/eller kjøretøy til enhver tid befinner seg, som skal sikres i forhold til konfidensialitet, integritet og tilgjengelighet. Dette gjelder eksempelvis utstyr, programvare og informasjon.

Tjenestetilbyder eller operatør oppretter kunderegistre og behandler detaljerte data om posisjon (tid og sted). Systemet består av følgende hoveddeler:

- Kunderegister
- Dynamiske data om posisjon (person- eller kjøretøy-ID, tid og sted) registreres fortløpende
- Evt. registre (statiske eller dynamiske data) som de dynamiske dataene sjekkes mot (informasjon om kollektivtrafikk, fartsgrenser, tilgjengelige tjenester, informasjon fra andre kjøretøy, posisjon til venner og bekjente osv.). Mottakerenheten gjennomfører evt. spørring i aktuelle registre og sjekk av dynamiske data mot evt. registre skjer i mottakerenheten.

Disse opplysningene er sensitive i den grad de kan knyttes til helse, religion, partipolitikk, regelbrudd og kriminell aktivitet osv. Men fordi de registrerer hvor personen og kjøretøyet oppholder seg til enhver tid, kan registreringen oppleves som omfattende. Den som registreres vil vanligvis være klar over at man blir registrert, men har ikke nødvendigvis innsikt mht. hvem og hvor mange som får informasjonen, eller hvor lenge den er tilgjengelig.

3.5.2 Lokasjonsbaserte tjenester: Miljøet som verdiene befinner seg i

Den mobile enheten er gjerne mobiltelefon, håndholdt eller bærbar pc eller gps-utstyr i bil. Lokasjonsdata (id, tid og sted) overføres fortløpende til tjenesteyter eller operatør, og informasjon om de lokasjonsbaserte tjenestene mottas på mobil enhet.

Det fysiske miljøet er sjelden et problem med unntak av alvorlige hendelser som brann etc. Den *mobile enheten* er utsatt for tyveri etc. og det kan være lett for andre å få tilgang til informasjonen på denne. Hos tjenesteyter vil *sentralsystem* eller pc vanligvis være i beskyttede miljø både fysisk og logisk, der databehandler har opplæring i informasjonssikkerhet og har undertegnet taushetserklæringer. Bruken av systemet kan registreres slik at avvik kan detekteres og følges opp. Systemene er beskyttet i forhold til vann, brann og eksterne inntrengere.

Kobling mot andre dynamiske data kan skje via *veikantutstyr*. Veikantutstyr vil være utsatt for vær, vind, fysiske krefter og for tapping av informasjon.

3.5.3 Lokasjonsbaserte tjenester: Identifisering av uønskede hendelser

Nedenfor er en oversikt over de identifiserte uønskede hendelsene, og vurdert konsekvens og sannsynlighet for hendelsene (detaljert beskrivelse av hver hendelse i **vedlegg**). *Alle hendelser og*

konsekvenser er ikke aktuelle for alle anvendelser av lokasjonsbaserte tjenester. I skalaen for konsekvens går det et skille ved K= 2, der høyere vurdering innebærer ikke-reversible konsekvenser for liv, helse og økonomi. Dette gir følgende behov for konfidensialitet, integritet og tilgjengelighet:

- Lokasjonsbaserte tjenester gir kontinuerlig informasjon om hvor person eller kjøretøy befinner seg. Overvåkingen av trafikanten kan oppleves som vesentlig, men er normalt noe kunden aksepterer for å motta verdsatte tjenester. Av hensyn til tilliten fra kunden bør dataene holdes konfidensielt. Slik informasjon bør bare gjøres tilgjengelig for autoriserte personer, og det bør registreres hvem som har innsyn og for hvilke tidsperioder. Dette er spesielt viktig dersom observasjonene gir grunnlag for å undersøke regelbrudd og kriminell virksomhet.
- Lagring av slike data kan oppleves som massiv overvåking. Hvis slike data skal lagres, må de sikres mot endring.
- Manglende data (utilgjengelighet) kan ha økonomiske konsekvenser for virksomheten (redusert effektivitet).
- Manglende data kan ha konsekvenser for å identifisere kriminalitet. Slike registre må sikres mot tilgang for uvedkommende (konfidensialitet) og underlegges strenge krav til beskyttelse og tilgang.
- Når lokasjonsbaserte tjenester benyttes for å overvåke personer eller gi trafikkopplysninger og navigasjonstjenester til sårbare trafikanter (synshemmede, barn, demente, psykisk utviklingshemmede osv.), så kan manglende data ha betydning for liv og helse. Kravene til tilgjengelige korrekte data (id og posisjon) kan ha prioritet foran konfidensialitet.

Av tabellen neste side ser vi at det ifølge de vurderingene som er gjort, spesielt er hendelsene 1 og 3 som har høy risiko og som krever gjennomføring av tiltak i virksomheten.

Hendelse 1 gjelder utlevering av data til uvedkommende. Dette oppleves som krenkende for trafikanten og et tillitsbrudd i forhold til tjenesteyter. Høy sannsynlighet er knyttet til mulig uaktsomhet hos egne ansatte, eller forsett.

Hendelse 3 er knyttet til at det innhentes flere personopplysninger enn nødvendig, noe trafikanten opplever som tap av integritet. Høy sannsynlighet er knyttet til blant annet muligheten for å koble ulike registre.

Tabell 19: Oversikt over identifiserte hendelser, vurdert konsekvens og sannsynlighet

	Hendelse	Vurdert konsekvens	Vurdert sannsynlighet	Resulterende risikonivå
	Skala:	K (1 – 4)	S (1 – 4)	R = K x S
Utlevering				
1	Informasjon utlevert til uvedkommende	2	3	**6**
2	Informasjon ikke slettet så snart som mulig	2	2	**4**
3	Det innhentes flere opplysninger enn nødvendig	3	3	**9**
4	Informasjon formidles til andre aktører	2	2	**4**
5	Informasjon benyttes til andre formål	2	2	**4**
Endring				
6	Registrerte opplysninger blir endret	2	1	**2**
Utilgjengelighet				
7	Data er ikke tilgjengelig for kunden (fare for helse etc.)	2	2	**4**
8	Data er ikke tilgjengelig for kunden (økonomiske konsekvenser)	2	2	**4**
9	Data er ikke tilgjengelig for tjenestetilbydere	2	2	**4**
10	Trafikanten kjenner ikke hvilke data som er registrert	2	2	**4**

3.6 Risikovurdering for intelligente fartstilpasningssystem (ISA) med lagring av data

Intelligente fartstilpasningssystem (ISA) er satellittbaserte system som kobler koordinatfestet fartsgrenseinformasjons med kjøretøyets posisjon, og som varsler føreren når fartsgrensa overskrides. Dynamiske system varsler også om endret fartsgrense pga. hendelser, været eller føreforhold. ISA har et betydelig trafikksikkerhetspotensial.

ISA som kun varsler føreren har i utgangspunktet ikke personvernimplikasjoner. Det som omtales videre her er bruk av *ISA med lagring av data*. Atferdsregistratoren i bilen logger kontinuerlig bilens posisjon, hastighet og kjørestil, dvs. akselerasjon, retardasjon og hastighet i kurver. Kommunikasjonsløsninger og programvare gjør at informasjonen kan sendes fra bilen til en mottakerenhet. Dette gjør det mulig å overvåke blant annet posisjon og fart i sanntid.

Muligheten for logging og overføring av data stiller spørsmål om hvilke myndigheter og andre aktører som skal kunne ha tilgang til dataene, og hvilke beslutninger disse dataene skal kunne være grunnlag for.

3.6.1 ISA: Hvilke verdier skal sikres

Intelligente fartstilpasningssystem med atferdsregistrator og mottakerenhet inneholder verdier, dvs. informasjon om kjøretøy-id, posisjon, hastighet, fartsgrense og kjørestil (f.eks. fartsvalg i kurver). Noen løsninger lagrer ikke data om posisjon. Systemet består av følgende hoveddeler:

- Kjøretøyets posisjon, akselerasjon, retardasjon og fartsnivå logges i mobil enhet i kjøretøyet, sammen med fartsgrense (og horisontalkurvatur) på stedet.

- Mobil enhet henter koordinatfestet fartsgrenseinformasjon fra statiske registre og dynamiske registre.
- Informasjon om kjøretøy-id, posisjon, fartsnivå, fartsgrense og kjørestil sendes fra mobil enhet i kjøretøyet til mottakerenhet.

Lokasjonsopplysninger er sensitive i den grad opplysninger om hvor man er kan knyttes til helse, religion, partipolitikk, regelbrudd og kriminell aktivitet osv. Det som skiller ISA fra de andre anvendelsene er først og fremst opplysninger om evt. fartsoverskridelser. Fordi det registrerer hvor kjøretøyet oppholder seg til enhver tid og data om førerens kjørestil, kan registreringen oppleves som omfattende. Den som registreres trenger ikke nødvendigvis være klar over at man blir registrert, og har heller ikke nødvendigvis innsikt mht. hvem og hvor mange som får informasjonen, eller hvor lenge den er tilgjengelig.

3.6.2 ISA: Miljøet verdiene befinner seg i

Den mobile enheten (ISA og atferdsregistrator) er utstyr i bil. Data overføres via satellitt til mottakerenhet. Avhengig av formål og anvendelse kan mottakerenhet være en privat mobiltelefon eller pc, eller en pc eller sentralsystem hos en tjenesteyter.

Private mobiler og pc'er kan være utsatt for tyveri og for innsyn i data. Hos tjenesteyter vil *sentralsystem* eller pc vanligvis være i beskyttede miljø både fysisk og logisk, der databehandler har opplæring i informasjonssikkerhet og har undertegnet taushetserklæringer. Bruken av systemet kan registreres slik at avvik kan detekteres og følges opp. Systemene er beskyttet i forhold til vann, brann og eksterne inntrengere.

3.6.3 ISA: Identifisering av uønskede hendelser

I tabellen nedenfor er en oversikt over de identifiserte uønskede hendelsene, og vurdert konsekvens og sannsynlighet for hendelsene. *Alle hendelser og konsekvenser er ikke aktuelle for alle anvendelser av lokasjonsbaserte tjenester.* I skalaen for konsekvens går det et skille ved K= 2 (se kapittel 3.2.3), der høyere vurdering innebærer ikke-reversible konsekvenser. Dette gir følgende behov for konfidensialitet, integritet og tilgjengelighet:

- ISA-tjenester gir kontinuerlig informasjon om hvor kjøretøyet befinner seg og førerens kjørestil, fartsnivå og overholdelse av fartsgrenser. Slik informasjon bør bare gjøres tilgjengelig for autoriserte personer, og det bør registreres hvem som har innsyn og for hvilke tidsperioder. Dette er spesielt viktig dersom observasjonene gir grunnlag for å undersøke regelbrudd og kriminell virksomhet.
- Lagring av slike data kan oppleves som massiv overvåking. Hvis slike data skal lagres, må de sikres mot endring.
- Manglende data (utilgjengelighet) kan ha konsekvenser for å identifisere regelbrudd eller kriminalitet. Slike registre må sikres mot tilgang for uvedkommende (konfidensialitet) og underlegges strenge krav til beskyttelse og tilgang.
- Utilgjengelige data kan evt. medføre at en trafikant holder for høy eller for lav hastighet i forhold til forholdene og andre trafikanter.

Beskrivelse av hendelser, årsaker, medvirkende personer, konsekvens og sannsynlighet er vist i **vedlegg**.

Tabell 20: Oversikt over identifiserte hendelser, vurdert konsekvens og sannsynlighet

	Hendelse	Vurdert konsekvens	Vurdert sannsynlighet	Resulterende risikonivå
	Skala:	K (1 – 4)	S (1 – 4)	R = K x S
Utlevering				
1	Informasjon utlevert til uvedkommende	3	3	**9**
2	Informasjon ikke slettet så snart som mulig	3	3	**9**
3	Det innhentes flere opplysninger enn nødvendig	3	3	**9**
4	Informasjon formidles til andre aktører	3	3	**9**
5	Informasjon benyttes til andre formål	2	2	**4**
Endring				
6	Registrerte opplysninger blir endret	3	1	**3**
Utilgjengelighet				
7	Data (tjeneste) er ikke tilgjengelig for kunden	3	1	**3**
8	Data er ikke tilgjengelig for behandling	2	2	**4**
9	Data er ikke tilgjengelig for kontroll	3	2	**6**
10	Trafikanten kjenner ikke hvilke data som er registrert	2	2	**4**

Av tabellen over ser vi at ifølge de vurderingene som er gjort, så er det spesielt hendelsene 1-4 og 9 som har høy risiko, og som krever gjennomføring av tiltak i virksomheten.

Risikoen er knyttet til manglende forståelse for behovet for skjerming av data, og at dette er attraktive data som mange kan ønske å få tak i (f.eks. publisere) og evt. lagre og bearbeide for etablering av førerprofiler.

3.7 Kort oppsummering om risikovurdering

Vi har presentert vurderinger knyttet til hendelser, konsekvenser og sannsynlighet for ITS-anvendelser der registrering av personopplysninger kan ha konsekvenser for personvernet; automatisk nummerskiltgjenkjenning, sporing av kjøretøy, lokasjonsbaserte tjenester og intelligente fartstilpasningssystem med lagring av data.

Typisk for de tre første ITS-anvendelsene er at de i liten grad er direkte knyttet til sensitiv eller intim personinformasjon, men forteller hvor et kjøretøy eller en person er eller har vært. Mens *automatisk nummerskiltgjenkjenning* bare kan gi informasjon om passeringer av bestemte punkt, så kan *sporing av kjøretøyet* følge kjøretøyets bevegelser. Flere anvendelser av sporing av kjøretøy er først og fremst aktuelt for utførelsen av oppdrag i arbeidstiden. *Lokasjonsbaserte tjenester* baserer seg på å følge personens (mobiltelefonens) eller bilens bevegelser og kan benyttes hele døgnet. Basert på mobiltelefonens posisjon kan en person i teorien følges ganske tett både inne og ute. Disse tjenestene er som regel basert på en frivillig avtale. Hvis sporing av

kjøretøy avgrenses til oppdrag i arbeidstiden, synes lokasjonsbaserte tjenester å bidra til den mest omfattende registreringen av personer.

Mulige uønskede hendelser ved behandling av personopplysningene og vurdering av årsaker, sannsynlighet og konsekvenser er beskrevet i vedlegg. Sannsynligheten er vurdert på en skala fra svært lav (1) til svært høy (4), med utgangspunkt i motivasjon og mulighet for at hendelsen skal skje. Konsekvensene av hendelsene er vurdert på en skala fra 1 - 4 etter alvorlighetsgrad, der nivå 1 representerer tap som kan gjenopprettes og nivå 4 representerer tap av liv, vedvarende helsetap, betydelige og uopprettelige økonomiske tap, eller alvorlig tap av anseelse eller integritet som påvirker liv, helse eller økonomi. Ved vurdering av risiko har vi lagt vekt på at anvendelsene ikke skal medføre uopprettelig tap for enkeltindividet, virksomheten eller samfunnet. Tabellen nedenfor gir en oppsummering av vurderingene i form av tallverdier.

Ut fra disse vurderingene synes hendelsene 1 - 3 og 9 å være de mest problematiske; dvs. risiko for at informasjonen leveres til uvedkommende, at det innhentes mer informasjon om personen enn nødvendig, manglende rutiner for sletting av persondata, og at data ikke er tilgjengelige for behandling for tjenestetilbyder.

Andre ITS-applikasjoner kan lagre både posisjon og opplysninger som kan knyttes til den registrertes atferd. Eksemplet som er tatt med her, er fartstilpasningssystem knyttet til en enhet som lagrer data. Også for denne anvendelsen er hendelsene 1-3 og 9, men også 4, problematiske og er til dels vurdert til å ha høyere resulterende risikonivå.

Tabell 21: Oppsummering av vurderinger av hendelser, konsekvens K, sannsynlighet S og resulterende risikonivå R

		Automatisk nummer-gjenkjenning			Sporing av kjøretøy			Lokasjons-baserte tjenester			Intelligent fartstilpasser		
Hendelse		K	S	**R**	K	S	**R**	K	S	**R**	K	S	**R**
Utlevering													
1	Informasjon utlevert til uvedkommende	2	3	**6**	2	3	**6**	2	3	**6**	3	3	**9**
2	Informasjon ikke slettet så snart som mulig	2	2	**4**	3	3	**9**	2	2	**4**	3	3	**9**
3	Flere opplysninger enn nødvendig innhentes	3	3	**9**	3	3	**9**	3	3	**9**	3	3	**9**
4	Informasjon formidles til andre aktører	2	2	**4**	2	2	**4**	2	2	**4**	3	3	**9**
5	Informasjon benyttes til andre formål	2	2	**4**	2	2	**4**	2	2	**4**	2	2	**4**
Endring													
6	Registrerte opplysninger blir endret	2	1	**2**	3	1	**3**	2	1	**2**	3	1	**3**
Utilgjengelighet													
7	Registre er ikke tilgjengelig for oppslag/kontroll	2	2	**4**	2	2	**4**	2	2	**4**	3	1	**3**
8	Data er ikke tilgjengelig for behandling	2	2	**4**	2	1	**2**	2	2	**4**	2	2	**4**
9	Data er ikke tilgjengelig for kundens kontroll	3	2	**6**	2	2	**4**	3	2	**6**	3	2	**6**
10	Trafikanten kjenner ikke hvilke data som er registrert	2	2	**4**	2	2	**4**	2	2	**4**	2	2	**4**

Gjennomgangen av hendelser, konsekvens og sannsynlighet viser at intelligente transportsystem (ITS) medfører utfordringer for personvernet. Andre bruksområder av systemene og andre ITS-løsninger enn de som er beskrevet her, kan ha andre risikoprofiler. For å opprettholde et akseptabelt risikonivå, er det behov for å gjennomføre tiltak på grunnlag av gjentatte

risikovurderinger (ved jevne mellomrom og ved vesentlige endringer i forutsetninger) for ulike anvendelser og virksomheter

4 Bruk av personvernfremmende teknologier i transport

Personvernfremmende teknologier (privacy enhancing tehnologies, PET) er et samspill mellom tekniske og organisatoriske tiltak for å sikre personopplysninger. Begrepet brukes både om tekniske og organisatoriske tiltak som tar sikte på å begrense andres mulighet til å identifisere den enkelte, med utgangspunkt i prinsippet om dataminimalitet. Viktige prinsipp for *dataminimalitet* er å sørge for å unngå å lagre data som man ikke strengt tatt trenger, å begrense antall lagringssteder og tilgangen til dataene, og å sørge for gode tekniske og organisatoriske rutiner for å slette opplysninger når det ikke lenger er behov for dem.

Vi kan skille mellom *personvernfremmende* og *personvernstøttende* teknologi. I dette kapitlet presenterer vi noen sentrale personvernfremmende teknologier[13] og anvendelsesområder, mens personvernstøttende teknologi blir kort omtalt i kap. 4.1.

Et typisk anvendelsesområde er når flere aktører deler noen data, mens andre data må holdes separat (f.eks. ved elektronisk billettering som inkluderer mer enn ett transportselskap). Eksempler er teknologier for anonymisering, pseudonymisering og identitetsforvaltning. Andre eksempler på bruksområder er:

- Pseudonyme løsninger som alternativ til full anonymitet og full identifikasjon.
- Pseudonyme sertifikat i løsninger for digital signatur, der dette er tilstrekkelig.
- Anonyme betalingskort som alternativ til bankkort/kredittkort som er knyttet til identitet.

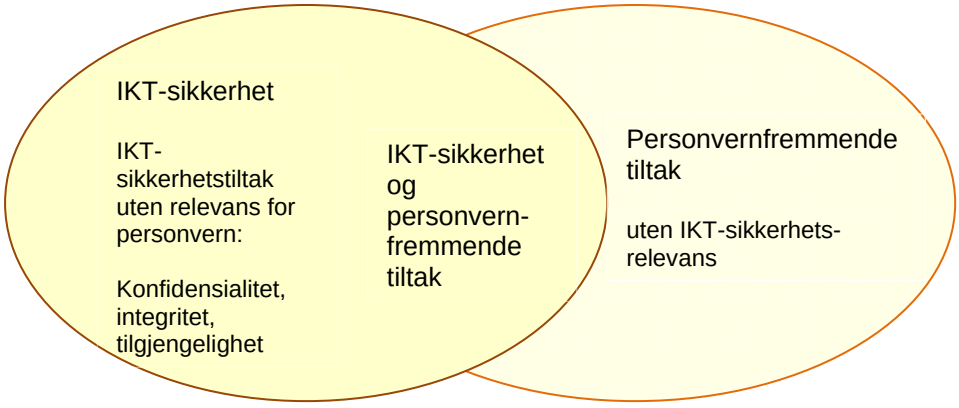
Teknologiene kan i seg selv være relativt nøytrale. Man må kjenne både fordeler og mulige ulemper, eller uheldige konsekvenser for personvernet, og benytte teknologiene på en fornuftig og gjennomtenkt måte. Det utvikles en rekke ulike løsninger, ofte som skreddersøm eller som tilleggsapplikasjoner for å forbedre system som ikke fungerer tilfredsstillende. Dette gir lite standardisering og mulighet for å sette sammen ulike ferdige løsninger (Ministry of Science Technology and Innovation 2005).

I det første kapitlet så vi at det er sterke drivkrefter for ITS-løsninger; både produsenter, tjenesteytere, myndigheter og trafikanter etterspør effektive og sikre løsninger. Vi finner ikke de samme sterke markedskreftene for personvernfremmende teknologier. Flertallet opplever de positive sidene ved tiltaket og vil ikke være sterke pådrivere for personvernfremmende teknologier, mens trafikanter som opplever konsekvensene av tillitsbrudd vil være i mindretall. Det er to mulige innfallsvinkler til økt bruk av personvernfremmende teknologier i transportsektoren:

- Ansvarlige aktører presenterer ”sikre” løsninger, blant annet for å oppnå tillit hos kunder og myndigheter.
- Den enkelte bruker sikrer seg ved å kjøpe tjenester via tiltrodd tredjepart.

[13] Innholdet i dette kapitlet bygger i hovedsak på Fornyings- og administrasjonsdep. (2009), Raguse m.fl. 2008a, Raguse m.fl. 2008b, Ministry of Science Technology and Innovation (2005) og Teknologirådet 2005. Ministry of Science Technology amd Innovation (2005), og også Olsen (2010), gir i tillegg informasjon om konkrete produkter og tjenester.

Det er delvis overlappende områder mellom IKT-sikkerhet og personvernfremmende teknologier.



Figur 9: Overlapping mellom personvernfremmende teknologier og generell IKT-sikkerhet (etter Raguse m.fl. 2008b)

IKT-sikkerhet gjelder tiltak for å sikre informasjonens konfidensialitet, integritet og tilgjengelighet, og omfatter fysisk sikring av miljøet, sikring av informasjonssystemet (brannmur, virusbeskyttelse osv.) og organisatoriske tiltak (informasjon, opplæring, rutiner, tilgangskontroll, logging av databehandling osv). Tiltakene kan gjelde både personopplysninger og andre opplysninger. Tiltakene må vurderes i forhold til konsekvensene av sikkerhetsbrudd. Personvernfremmende tiltak beskytter konfidensialitet, integritet og tilgjengelighet (IKT-sikkerhet) av personopplysninger. Andre personvernfremmende tiltak er ulike løsninger for å registrere og lagre færre opplysninger knyttet til personer, og for å holde ulike datasett om personer atskilt fra hverandre.

4.1 Personvernstøttende teknologi

Personvernstøttende teknologier (privacy management) er teknologi som støtter oss i arbeidet med å administrere personvernregler. Eksempler er:

- Informasjonsverktøy som støtter virksomheter i å beskrive virksomhetens personvernpolicy på nettsidene, og å sjekke at de samme nettsidene overholder den policyen de beskriver.
- Informasjonsverktøy som støtter den enkelte bruker i å gjøre valg i tråd med egen personvernpolicy, for eksempel ved å varsle om nettlasting av nettsider som ikke samsvarer med de reglene brukeren selv har definert (virksomhetens personvernpolicy som beskrevet over er omgjort til maskinlesbar kode slik at man kan varsles automatisk).

Spamfiltre, blokkere og programvare for å hindre virus og spionprogramvare som vi har nevnt under anonymisering, kan også regnes som personvernstøttende teknologi.

4.2 Personvernfremmende teknologier

Vi har mange måter å framstille oss på, og den digitale identiteten vår er en samling identifiserende personopplysninger i elektronisk form. Dette kan være alt fra formelle ”signaturer” til kontekstuelle modeller basert på hva man gjør (personprofiler) ved sammenstilling av data fra nettet. Vesentlig for personvernet er hvor lett det er å koble opplysningene til en bestemt person, fordi det er vanskelig å ha kontroll over tilgang til og spredning av elektroniske data.

Personvernfremmende teknologier er tekniske og organisatoriske tiltak som begrenser andres mulighet til å identifisere den enkelte, og som reduserer muligheten for å sammenstille mye data om en person. Prosjektet PRISE (Raguse m.fl. 2008a) presenterer følgende definisjon:

> Personvernfremmende teknologier (privacy enhancing technologies, PET) er et enhetlig system for informasjons- og kommunikasjonsteknologi som beskytter personvernet gjennom å *unngå eller minimalisere* persondata og å *kontrollere tilgangen* til persondata i henhold til regler og rutiner, uten å ødelegge funksjonaliteten i systemet.

Teknologiene tar utgangspunkt i tre prinsipp:

- *Anonymitet*; informasjonen kan ikke knyttes til en bestemt person.
- *Ikke-observerbar*; privat informasjon er ikke synlig eller tilgjengelig for andre
- *Unngå sammenkobling*; unngå at andre kan sette sammen informasjon fra ulike kilder, graden avhenger av innsatsen som er nødvendig for å sammenkoble informasjonen. Innen samme organisasjon må dataene holdes atskilt (separering) og mellom organisasjoner må det benyttes ulike pseudonym (identifiseringsnøkler) for ulike databaser og formål.

Teknologiene kan grupperes i noen hovedgrupper: Anonymisering, pseudonomisering, kryptering som en del av anonymisering og pseudonomisering, identitetsforvaltning og tilgangsforvaltning.

4.2.1 Anonymisering

Anonymisering er én gruppe personvernfremmende teknologier, der hensikten er at informasjonen ikke kan knyttes til en bestemt person. Dermed kan informasjonen heller ikke settes sammen med annen informasjon om personen (anonymitet, unngå sammenkobling av data). Graden av anonymisering avhenger av innsatsen som kreves for å linke person og data. Det finnes tjenester som muliggjør anonym elektronisk kommunikasjon for vanlige brukere. Slik teknologi skjuler forbindelsen mellom brukeren og sporene han eller hun etterlater seg, og kan derfor hindre uønsket identifisering. Datamaskinens ip-adresse[14] kan skjules ved at informasjonen sendes gjennom en kjede av samarbeidende tiltrodde aktører, beskyttet med kryptering slik at anonymiteten beholdes selv om en av nøklene fra en av de tiltrodde tredjepartene kompromitteres. Gruteser & Grunwald (2005) beskriver ulike metoder for å hindre at andre kan registrere lokasjonen (sted og tid) for mobiltelefoner, bærbare og håndholdte pc'er.

Automatiske sletterutiner er sentralt for å sikre at lagrede data fjernes eller anonymiseres for statistikkformål etc., når behovet for å knytte opplysningene til en person ikke lenger er tilstede.

Ulike metoder for sletting av elektroniske spor og aktiviteter kan også inngå som anonymiseringsteknologier (støtter både anonymitet, uobserverbarhet og å unngå kobling av data). Disse tilbys både for nettverk og brukerutstyr, for eksempel verktøy for sletting av surfehistorikk, og metoder for reell sletting av data på harddisk (ved innlevering for reparasjon, resirkulering osv.)

[14] En IP-adresse er en unik nettverksadresse som tildeles en enhet, f.eks. en skriver eller en PC, i et nettverk. Internetworking Protocol (IP) er den grunnleggende kommunikasjonsprotokollen i internett. Den beskriver hvordan data pakkes i pakker som påføres en mottaker-adresse og en avsender-adresse. Routerne i nettet bruker adressene til å sende pakkene videre til de kommer fram til mottaker-adressen.

Spamfiltre, blokkere og beskyttelse mot virus og spionvare støtter også indirekte anonymitet ved å unngå at den enkelte oppgir opplysninger om seg selv, blant annet ved å svare på henvendelser som gjelder svindelforsøk (phishing[15]).

Eksempler på anonymisering i transportsektoren

Å tilby et tilsvarende anonymt alternativ, er en forutsetning for å sikre reell informert samtykke ved inngåelse av kundeavtaler.

Kontant betaling er et eksempel på anonym løsning i betalingssystem. Det er få eksempler på tekniske løsninger for reell anonymitet i transportsektoren, men eksempler kan være løsninger for anonym elektronisk betaling (e-cash) og elektronisk billett for enkeltreise (dette er delvis et spørsmål om grad av anonymitet, se også eksempler på pseudonymisering).

Det presenteres også løsninger når RFID-sendere benyttes for å spore godset fra leverandør til butikk, der forbrukeren kan slå RFID-senderen over på stillemodus (beskyttes mot tilgang og identifisering) når de forlater butikken (Granau 2008).

4.2.2 Pseudonymisering

Ved å ta i bruk en pseudonymisert identifikator kan identiteten til den registrerte helt eller delvis holdes skjult, uten at vesentlig funksjonalitet går tapt med hensyn til å følge datasubjekter (personer) over tid. Graden av pseudonymitet avhenger av innsatsen som kreves for å knytte informasjonen til en identitet, ved for eksempel;

- Offentlige pseudonym, som telefonnumre i offentlige registre
- Opprinnelig ikke-offentlige pseudonym, som valgte brukernavn og passord kjent av en avgrenset krets personer
- Opprinnelig ikke-linkbar pseudonym, eksempelvis elektroniske billetter i kollektivtrafikken som ikke knyttes til en bestemt trafikant ved kjøp[16].

Uregistrerte (anonyme) kontantkort og e-postadresser gir pseudonymitet der bruken ikke kan knyttes direkte til en bestemt person, men der det kan være mulig å lagre data om bruken over tid som gir en brukerprofil (Teknologirådet 2005).

Pseudonymiseringsverktøy muliggjør f.eks. elektronisk betaling (e-transaksjoner) uten å kreve privat informasjon, og kan separere sensitive private data fra transaksjonsdata:

- Ved å erstatte kundens navn med en nøytral transaksjons-id eller flere tilfeldige numre (det kan lages en profil over kunden, men kunden forblir anonym).
- Ved å tilby verktøy som remodellerer eksisterende databaser med ulike nøkler for å linke ulike tabeller, istedenfor ett sett unike identiteter (unngå utilsiktet kobling av data).

Kjernen i systemet er en *koblingssentral* hvor personidentifiserende identifikatorer (som for eksempel fødselsnummer) blir gjort om til pseudonymer som ikke direkte kan knyttes til en identifiserbar person. Slike koblingssentraler mellom identifiserbare identifikatorer og

[15] Phishing er et begrep for metoder for ulovlig innhenting av (fiske etter) sensitiv digital informasjon, som passord eller kredittkortnummer.

[16] Raguse m.fl. (2008a) bruker biometriske data som ikke er lagret i registre som eksempel på opprinnelig ikke-linkbar pseudonym, selv om de fleste oppfatter biometriske data som sterkt knyttet til den enkelte person.

pseudonymer kan plasseres i ulike deler av informasjonssystemet eller være under brukerens kontroll, og koblinger kan skje automatisk etter nærmere bestemte regler forvaltet av en uavhengig og tiltrodd *pseudonymforvalter*.

Tiltrodd tredjepart tildeler sertifikat og nøkler i en Public Key Infrastructure (PKI). *Surrogatnøkler* er beregnede nøkler som erstatter nøkkelfelt i datasettet. Disse er utviklet for å redusere behovet for datakraft for å sjekke transaksjoner mot eksisterende databaser, men fungerer også som beskyttelse ved å hindre sammenstilling av data i ulike registre.

Eksempler på pseudonymisering i transportsektoren

Elektroniske billetter og flerreisekort i kollektivtrafikken er eksempel på pseudonyme løsninger. For å være sikker på at reisekortet ikke kan knyttes til en bestemt person, kan det kjøpes kontant eller gjennom anonyme betalingsløsninger. Hvis det elektroniske reisekortet kan brukes på flere reiser kan det opprettes en reiseprofil, men denne kan i utgangspunktet ikke knyttes mot en bestemt person.

Statens vegvesens håndbok for billettering angir bruk av flere personvernfremmende teknologier, blant annet under kapittel 6 om krav til sikkerhet. Ved *elektronisk billettering* i kollektivtrafikken (buss, trikk, bane, båt og ferge), blir ikke kundens identitet registrert i forbindelse med reiseopplysninger eller avregning av tjenester. For avregning av tjenester vil en transaksjons-id følge datasettet. For reiseopplysinger kan man enten lagre anonym reisestatistikk, eller registrere et reisekort-id slik at man kan bygge opp (pseudonyme) reiseprofiler.

De fleste løsninger for elektronisk billettering gir kunden tilbud om å følge status med hensyn til billetter og reiser på ”min side”, med tilgang via brukernavn og passord. Dette gir ikke i seg selv tilstrekkelig sikkerhet for pseudonym identitet, men krever forvaltning av brukernavn og passord slik at man unngår å benytte f.eks. e-postadresser som beskriver hvem man er.

Også ved bompasseringer blir kjøretøyidentiteten skilt fra transaksjonsdataene ved hjelp av en transaksjons-id som følger transaksjonsdataene for avregning.

Tilsvarende kan AutoPASS-brikken fungere som pseudonymt *betalingsmiddel i automatiserte bompengeanlegg*. Foss og Hjelkrem (2010) beskriver forutsetninger for å opprette anonyme avtaler ved bruk av AutoPASS-brikken[17]. Brukerens mulighet for å sjekke avregning er knyttet til en kode som benyttes ved første gangs pålogging på ”min side”.

At elektronisk betaling i kollektivtrafikken og i bompengeanlegg beskrives som pseudonyme og ikke anonyme, er knyttet til muligheten for å registrere bruk av samme kort/brikke over tid, noe som gir grunnlag for å bygge opp trafikantprofiler og evt. linke annen informasjon.

4.2.3 Identitetsforvaltning og tilgangsforvaltning

Identitetsforvaltning er en gruppe personvernfremmende teknologier som tar utgangspunkt i hvordan identifisering og autentisering kan tilpasses de ulike rollene enkeltindividet har, f.eks. som ansatt, student eller kunde. For å gjøre det vanskeligere å koble sammen ulik data, reises spørsmålet om tildeling av hensiktsmessig identifikator (f.eks. brukernavn som ikke avslører identiteten din) og autentiseringsmekanisme (f.eks. passord) til ulike formål. Forskningen

[17] Med kundeavtale fungerer AutoPASS-brikken som betalingsmiddel tilsvarende et bank- eller kredittkort. Statens vegvesen er eier av AutoPASS-brikkene og teknisk utstyr på innkrevingspunkt.

innenfor identitetsforvaltning setter spørsmål ved hva (f.eks. hvilken rolle) som skal identifiseres, og hvordan dette gjøres på en tilstrekkelig sikker måte (autentisering).

Autentisering er å verifisere at du er den du oppgir å være. Dette kan være for å beskytte adgangen til informasjon, tjenester og ressurser og for å holde den enkelte ansvarlig for sine handlinger. En vanlig metode for å begrense adgang til nettbaserte tjenester og ressurser er autentisering ved hjelp av brukernavn og passord. Sikkerheten er ikke spesielt god (kan gjettes, oppgis til falsk nettside osv.), men man kan være anonym. For personvernet er det bekymringsfullt at de fleste autentiseringsløsninger benytter personopplysninger i prosessen:

- *autentisering av et individ* (alle elektroniske spor på den aktuelle tjenesten kan knyttes til reell person)
- *autentisering av en identitet*, f.eks. virtuell identitet (som kan eller ikke kan knyttes til et individ); at man er rettmessig bruker av et pseudonym er tilstrekkelig for en kunderelasjon, men ikke for kredittvurdering.
- *autentisering av et attributt*; at individet har en bestemt egenskap, f.eks. alder.

Teknologier for autentisering kan anvendes på måter som styrker eller svekker personvernet, og er basert på:

- Noe man vet (passord, PIN-kode)
- Noe man har (legitimasjon, smartkort etc.)
- Noe man er (fysiske karakteristika – biometri)

Noen ganger trenger den aktuelle tjenesten kun å bekrefte en bestemt egenskap, som for eksempel alder eller kredittgrense. Ved å autentisere relevante egenskaper, f.eks. medlemskap, alder eller kjønn, vil det være mulig å tilby en lang rekke tjenester uten å knytte dette til noen identitet. I slike tilfeller kan en identitetsutsteder (f.eks. banken din, en teleleverandør eller arbeidsgiver) opptre som en pålitelig tredjepart og garantere for denne egenskapen, uten å avsløre din identitet.

Det er utarbeidet tekniske standarder for identitetsforvaltning for å imøtekomme regulatoriske krav til informasjonssikkerhet og effektivisere tilgangsstyringen til virksomheters ulike ressurser og tjenester. Identitetsforvaltningssystem støtter personer i å holde rede på sine ulike brukernavn.

For å sikre persondata (i forhold til konfidensialitet, integritet/endring og tilgjengelighet) benyttes prinsipper for IKT-sikkerhet, med kryptering av forsendelser og lagring av data, digitale signaturer, rolleforvaltning og dokumentasjon (logging) av tilgang, databehandling, endring og forsendelse. Loggføring av databehandlingen er i seg selv behandling av personopplysninger (om de ansatte) som har krav på samme type sikkerhet som andre persondata. Et eksempel på rutine er at loggen slettes etter hver sikkerhetsrevisjon.

Sticky policies er krypterte beskjeder som er knyttet til og følger hvert dataelement gjennom hele levetiden, om hvordan de enkelte delene av dataene kan behandles gjennom systemet (kobles mot f.eks. autorisasjon). For at dette skal fungere, så må alle som behandler dataene (gjennom hele kjeden av databehandling) bruke samme *sticky system*.

Tilsvarende er *sticky data tracks* krypterte beskjeder knyttete til hvert dataelement gjennom hele levetiden, som beskriver hvordan de enkelte delene av datasettet er behandlet (loggføring av hvem som har hatt tilgang, gjennomført endringer osv.)

Eksempler på identitetsforvaltning og adgangskontroll i transportsektoren

Eksempler på identitetsforvaltning og adgangskontroll finner vi innenfor ulike deler av transportsektoren. I Statens vegvesens håndbok for elektronisk billettering angis regler for adgangskontroll, pålogging og beskyttelse av passord. Alle aktører i systemet skal ha en unik identitet og utveksling av informasjon skal bare skje etter gjensidig autentisering. Vi finner eksempler både innenfor parkering, drosje, kollektivtrafikk og bompengeselskap på prinsippet om at ansatte har begrenset adgang til virksomhetens registre. Regnskapsavdelingen har for eksempel ikke tilgang til de samme datasettene (registrene) som de som administrerer bestilling av turer. Adgangen begrenser seg til tilgang til de personlige opplysningene som den (kategori) ansatte har behov for i sin utførelse i jobben, og bare for de behandlinger som de har bruk for. Mens et fåtall har tilgang til å endre eller slette data, kan flere ha tilgang til å lese dataene.

Vi har ikke kjennskap til hvordan ulike virksomheter behandler informasjonen som logging av databehandling gir. Det er varierende praksis med hensyn til (automatisk) sletting av data det ikke lenger er bruk for.

I forslag til anonyme AutoPASS-avtaler, legges det opp til at kunden skal benytte en kode (dvs. noe kunden vet knyttet til utdeling av AutoPASS-brikken) som autentisering for å få tilgang til oversikt over innbetalinger og passeringer på ”min side”.

4.2.4 Kryptering som ledd i anonymisering og pseudonymisering

Kryptering går ut på å forvrenge meldingsinnholdet for å gjøre meldingen ulesbar for andre. Fordi elektronisk kommunikasjon er utsatt for avlytting eller manipulering, er det i mange tilfeller avgjørende at kommunikasjonen finner sted på krypterte linjer, eller at innholdet krypteres før overføring. Innholdskryptering er et viktig informasjonssikkerhetstiltak for å sikre opplysninger som kommuniseres eller lagres (e-poster, dokumenter og transaksjoner) mot uautorisert innsyn (konfidensialitet) eller endring (integritet). Krypteringsverktøy benyttes spesielt for sensitive data og når miljøet ikke kan sikres.

Kryptografi som ledd i en anonymiserings- eller pseudonymiseringsprosess er en personvernfremmende teknologi. Effektive system for automatisk kryptering av alt som lagres er tilgjengelig for vanlig utstyr som for eksempel mobiltelefoner og minnepinner. Men det mangler bevissthet og kunnskap hos brukerne og en fungerende infrastruktur for utveksling og autentisering av offentlige kryptografiske nøkler (public key infrastrukture PKI) (NOU 2009:1).

Kryptering er spesielt viktig ved sending av data og beskytter e-poster, dokumenter og transaksjoner fra å bli lest av utenforstående. Krypteringen kan være med bruk av samme nøkkel begge veier (symmetriske nøkler) eller forskjellige nøkler (asymmetriske nøkler). Krypterte e-poster hindrer innsyn i meldingen (*uobservert*), men skjuler ikke hvem som sender til hvem når. *TCP/IP transportlag sikkerhet* (TLS/SSL) som innebærer kryptering av alle transaksjons-meldinger (*uobservert*) benyttes for sensitive opplysninger som finanstransaksjoner. Sammen med den krypterte meldingen kan det sendes en meldingsintegritetskode som gjør at man kan sjekke at meldingen er mottatt intakt (data er *uendret*), og/eller en signatur som tilsier at meldingen kommer fra en bestemt krypteringsnøkkelinnehaver. Dette kan betraktes som en form for pseudonym *autentisering* av aktørene, ettersom det i utgangspunktet ikke trenger å være en kobling mellom krypteringsnøkkelen og andre personopplysninger.

Krav til bruk av kryptografi kan være avtalebasert. Kryptografi benyttes for å oppfylle regler som krever eller forutsetter sikring av datakonfidensialitet og –integritet, eksempelvis i forbindelse med taushetspliktsbestemmelser. Det er rettslige krav til bruk av kryptografi av en viss styrke på

bestemte områder, for eksempel ved elektronisk formidling av taushetsbelagte opplysninger til forvaltningsorganer (jf. forskrift om elektronisk kommunikasjon med og i forvaltningen 28. juni 2002 nr. 656, §§ 20–23), ekstern data-overføring av sensitive personopplysninger (personopplysningsloven § 13), og ved behandling av sikkerhetsgradert informasjon (sikkerhetsloven § 11).

Eksempler på kryptering av personopplysninger

Statens vegvesens håndbok for elektronisk billettering angir også regler for kryptering eller sikring på tilsvarende måte, for alle personopplysninger som overføres elektronisk ved hjelp av overføringsmedium utenfor behandlingsansvarliges fysiske kontroll. Alle aktører i systemet skal ha en unik identitet, og utveksling av informasjon skal bare skje etter gjensidig autentisering. Mottaker skal sjekke at den mottatte informasjonen er den samme som den som ble sendt (meldingsintegritet).

Uten å kunne dokumentere status, så har vi en oppfatning av at oppmerksomheten rundt dette varierer med type data og ulike system. Data som har betydning for avregning av tjenester, blir gjerne sikret godt. Vi har ikke kjennskap til om regnskapsdata for offentlig betalte transporter sikres like godt ved formidling mellom ulike offentlige etater.

4.3 Anvendelse av personvernfremmende teknologier innenfor transport på vei

Personvernfremmende teknologier for ulike deler av databehandlingen

ETSI (2010, s. 19) gir eksempel på hvordan bileier eller bilfører kan administrere bruken av personlige opplysningene som registreres i bilen; hvilke typer opplysninger tillates formidlet, under hvilke omstendigheter og til hvilke aktører.

Igjen viser vi til Statens vegvesens *håndbok for elektronisk billettering* som et eksempel på hvordan man må benytte ulike IKT-sikkerhetstiltak og personvernfremmende teknologier for å sikre forsvarlig databehandling. Håndboka angir at kundens identitet ikke skal registreres sammen med reiseopplysninger eller ved avregning av tjenester. Det angis regler for adgangskontroll, pålogging og beskyttelse av passord. Alle aktører i systemet skal ha en unik identitet, og utveksling av informasjon skal bare skje etter gjensidig autentisering. Mottaker skal sjekke at den mottatte informasjonen er den samme som den som ble sendt (meldingsintegritet) og alle personopplysninger som overføres elektronisk ved hjelp av overføringsmedium utenfor behandlingsansvarliges fysiske kontroll, skal krypteres eller sikres på tilsvarende måte.

Bruk av håndbøker og standarder, men også aktiv bruk av sikkerhetsrevisjon, angir hvilke krav som må tilfredsstilles. Ut fra dette vurderes hvilke løsninger som er aktuelle, deriblant personvernfremmende teknologier. PRISE-prosjektet viser følgende sammenheng mellom ulike sikkerhetsteknologier[18], databehandling og personvernfremmende teknologier (Raguse m.fl. 2008a):

[18] Rapporten *Oversikt over sikkerhetsteknologier* (Teknologirådet 2007) presenterer ulike personvernutfordringer knyttet til ulike (basis-) sikkerhetsteknologier.

Tabell 22: Valg av personvernfremmende teknologi på grunnlag av basisteknologi og databehandling.

Basisteknologi	*Databehandling*	*Personvernfremmende teknologier (PETs)*
Sensorer	Datainnsamling	Teknologier for dataminimalisme og transparens
Kommunikasjonsteknologi	Publisering	Transparens, sikring av persondata (applikasjon, protokoll, fysisk system)
Lagring	Lagring	Anonymitet, pseudonymitet, tilgangskontroll, sikring av persondata, metoder der regler for behandling følger dataene (sticky policies) og der protokollen over behandlingen følger dataene (sticky data tracks)
Analyse og beslutningsverktøy	Sammenstilling av data fra ulike kilder	Anonymitet, pseudonymitet, dataminimalisme, transparens, sticky policies, sticky data tracks, privacy enhancing data mining (algoritmer, klassifisering, kryptering)

Veien videre

Som nevnt er det mange markedskrefter for økt bruk av intelligente transportsystem (ITS), men få for økt bruk av personvernfremmende teknologier. Det er to innfallsvinkler til økt bruk av personvernfremmende teknologi:

- Transportnæringen presenterer ”sikre” løsninger som et ledd i kvalitetssikringen av sine tilbud og opprettholdes av tillit fra kunder og myndigheter
- Den enkelte trafikant sikrer seg ved å kjøpe tjenester via tiltrodd tredjepart-tjenester.

Personvern som gode kan både knyttes til person, virksomhet og samfunn (demokrati). Når ingen av innfallsvinklene over gir sterke drivkrefter, kan det indikere at styrket personvern er et fellesgode som alle vil ha, men der markedskreftene ikke gir god nok regulering. Borking (2008) gir noen grunner til hvorfor det er slik. En grunn er at det er knyttet konkrete kostnader til innføring av personvernfremmende teknologier, mens det er vanskeligere å kvantifisere nytteverdien. Det kan også være slik at ”alle” har nytte av at ”alle andre” innfører tiltakene. Personvernfremmende teknologier er relativt ny teknologi (begrepet er brukt siden 1995) som fremdeles er under utvikling (innovasjon). Han peker på at for at bruken av en ny teknologi (PETs) skal spre seg til nye sektorer og anvendelsesområder, må en viss andel brukere (”critical mass”) overbevise flertallet om effektiviteten av teknologiene. For å få gjennomslag i den enkelte virksomhet, må en av de sentrale aktørene ha tiltro til teknologien (oppfatningen er viktigere enn faktisk effektivitet osv.). Borking (2008) påpeker videre at virksomheten og teknologien må passe til hverandre, der innovasjon og innføring av ny teknologi er knyttet til et høyt modningsnivå[19]. Typisk for virksomheter som innfører nye personvernfremmende teknologier først, er at de enten er avhengig av stor grad av tillit eller er virksomheter som systematisk forbedrer sine rutiner og tjenester basert på kvantitative målinger, tester og innovasjon. Han viser til ulike stadier der generelle personvernfremmende teknologier innføres først (rollebasert autorisasjon, kryptering etc.), og der de neste stegene er teknologi for segregering av data, personvernadministrasjon og anonymisering (Borking 2008, s. 59).

[19] Laveste nivå er knyttet til kaos og ad hoc løsninger, nivå 2 til planlegging av prosesser og de som fungerer gjentas, nivå 3 til implementering av standarder og definerte resultat av prosesser, på nivå 4 blir utførelse og kvalitet kontrollert kvantitativt. Det høyeste nivået kjennetegnes av innovasjon og forbedringer på grunnlag av tester og målbare resultat. Forbedringsprosessene er kontinuerlige, trinnvise og knyttet til virksomhetens mål (Borking 2008, s.55-56).

Det er den enkelte virksomhet som må gjennomføre vurdering av konsekvenser for personvernet ved innføring av nye tiltak, risikovurdering av behandling av personopplysninger og sikkerhetsrevisjoner. To forhold kan tale for en tydeligere myndighetsrolle:

- Personvern kan sees som et fellesgode som markedskreftene ikke regulerer godt nok, men med betydning både på individnivå, virksomhetsnivå og for samfunnet (demokrati).
- Det er behov for felles retningslinjer og krav (bransjestandard) og å se de ulike delene av sektoren i sammenheng, slik at kravene står i forhold til hverandre.

Schiefloe (2010) hevder at kravene til personvern innenfor helse på noen områder hindrer innovasjon og nyskaping, på andre områder hindrer effektiv funksjon (noe som definisjonen av PETs stadfester at disse ikke skal gjøre), mens andre områder ikke er tilstrekkelig regulert. Også innenfor transportsektoren kan det se ut som om noen virksomheter og anvendelsesområder blir fulgt med stor oppmerksomhet og strenge krav, mens andre i liten grad reguleres (Øvstedal 2009). I noen virksomheter bar tiltakene klart preg av å være tilbakeskuende, basert på hendelser som allerede hadde inntruffet, mens andre virksomheter i større grad var pro-aktive.

En rapport fra Danmark (Ministry of Science Technology and Innovation 2005) foreslår følgende skritt for å øke oppmerksomheten om og å bedre personvernet:

1) Etablere personvernstøttende informasjonsverktøy på offentlige nettsider, som gjør det enklere for egen etat å etablere og overholde egen personvernpolicy, og som kan bidra til å øke publikums oppmerksomhet om personvern
2) Etablere felles regler for identitetsforvaltning med personvernregler
3) Etablere verktøy for å administrere personvernregler

5 Avsluttende kommentarer

Innledningsvis har vi sett at den teknologiske utviklingen gir oss nye og effektive løsninger innenfor områder som trafikantinformasjon, trafikk- og flåtestyring, førerstøttesystem og navigasjon, overvåking og kontroll, drift av infrastruktur og betalingssystem. Det forventes at disse intelligente transportsystemene (ITS) vil bidra vesentlig til sikrere og mer effektive transportsystem, og sterke drivkrefter bidrar til utviklingen gjennom myndigheter, fagmiljø og markedskrefter. Økt bruk av elektronisk registrering og lagring av data, gjør at det samles inn svært store mengder data i forbindelse med transport. Dette etablerer en infrastruktur som åpner for å benytte teknologien for registrering av flere opplysninger, nye formål eller andre aktører. Nye teknologiske løsninger gjør det også mulig å overføre data uten at den som registreres merker det. Ut fra personvernhensyn kan de nye teknologiske mulighetene representere store utfordringer. Og det er et paradoks at det nettopp er bruk av samvirkende system og kobling av ulike registre som gir størst potensiell effekt for oppnåelse av transportpolitiske mål (se eksempelvis Avinor m.fl. 2006).

Hvorfor skal vi ta hensyn til personvernet

Personvernet er nært knyttet til enkeltindividets behov og muligheter for privatliv, selvbestemmelse og selvutfoldelse. Personvern handler om selv å kontrollere når, hvordan og hvor mye informasjon om egen person som spres til andre, og om retten til å ha en egen privat sfære der en kan være alene. Type personopplysninger (intime, sensitive, stigmatiserende), omfang og hvordan opplysningene formidles uvedkommende har betydning for konsekvensene av manglende personvern.

Det er ikke nødvendigvis de opplysningene loven definerer som sensitive, som folk flest er opptatt av å beskytte. Generelt er aksepten for registrering større når man er på et offentlig sted som i kollektivtransporten, enn når man er på privat område. Mange opplever personbilen som sin private arena. Undersøkelser viser at flertallet aksepterer mange registreringsformer, men personvernet skal beskytte også de som har andre grenser for hva de ønsker å fortelle om seg selv. Personopplysningene kan utgjøre en trussel for personer som av forskjellige grunner er utsatt for diskriminering, uønsket oppmerksomhet, forfølgelse eller vold. Vi ser også at sårbare grupper i samfunnet er mer skeptisk til registreringer samtidig som de kan være mer utsatt for registrering, behandling og påfølgende beslutninger som på grunnlag av personopplysninger.

I et samfunn hvor data registreres i stadig større grad, kan det være vanskelig for den enkelte å skaffe seg oversikt over omfanget av persondata som behandles. Den viktigste loven om personvern er Personopplysningsloven av 14. april 2000. Formålet er å beskytte mot krenkelser av personvernet ved manuell og elektronisk behandling av personopplysninger. En vesentlig utfordring for lovverket er å holde tritt med den teknologiske utviklingen.

Registreringene i transportsystemet er omfattende, men få opplysninger er sensitive

Vi beskriver ulike ITS-løsninger i veisektoren som kan ha følger for personvernet. Mange av disse har flere bruksområder og behandlingsansvarlige kan være ulike aktører, både offentlige og private. Noen løsninger berører alle bileiere og bilførere eller alle trafikanter, andre berører først og fremst ansatte i jobbsammenheng. De fleste opplysningene som behandles er ikke sensitive eller intime, men kan oppleves som omfattende ved at det registreres og lagres informasjon om hvor man er og hvordan man reiser. Noen ITS-løsninger berører sensitive opplysninger ved

mistanke om regelbrudd, som automatisk trafikkontroll, intelligent fartstilpasningssystem og alkolås. Dette kan også gjelde overvåking av yrkestransport, utvidet bruk av AutoPASS og automatisk nummerskiltgjenkjenning.

Yrkestransporten står i en særstilling med omfattende overvåking på ulike områder, som ikke er basert på et frivillig samtykke på samme måte som i et kundeforhold. Samtidig kan det være vanskelig å beskytte seg mot avgjørelser tatt på grunnlag av feilaktige registreringer.

Risikovurderingene som er presentert i kapittel 3, bekrefter at behandling av personlige opplysninger innebærer risiko for personvernet. Dette krever bevissthet ved valg og design av løsninger. Personvernet skal veies mot andre formål i hver enkelt sak og situasjon. Det er også behov for å gjennomføre risikovurderinger for de ulike anvendelsesområdene og virksomhetene, og å gjennomføre tiltak som står i samsvar med utfordringene. Dette krever blant annet årvåkenhet ved omorganiseringer og ved tildeling av nye oppgaver, slik at databehandlere har den kunnskapen og de ressursene som er nødvendig for å ivareta oppgavene, samtidig som ansvaret som behandlingsansvarlig er tydelig plassert. En trend som gir økte utfordringer er arbeidsdeling og utsetting av oppgaver både i det offentlige og i det private, som medfører at flere aktører er involvert i tekniske leveranser og deling av data (se eksempelvis Meland m.fl. 2007).

En utfordring er funksjonsutglidning – at innsamlede data kan benyttes til nye formål

Flere forhold kan bidra til funksjonsutglidning, det vil si at registreringene benyttes til andre formål enn det opprinnelige. Rettssikkerhet kan være en pådriver for å utnytte data som allerede er samlet inn. Det kan argumenteres for å utnytte eksisterende løsninger for å oppnå enda bedre effekter, eller at nye tjenester kan bidra til å dekke kostnadene ved etablering av tjenesten. I andre sammenhenger har man ikke nok kunnskap om hvilke registreringsmuligheter den valgte tjenesten faktisk gir. Samtidig medfører rimelige løsninger for økt datalagringskapasitet at det blir mindre fokus på å utvikle gode sletterutiner.

Myndighetene kan legge til rette med regelverk, veiledning og tilsyn

Samferdselsdepartementet fastslår at de har ansvaret for overordnede politiske mål, å fastlegge rammebetingelser, følge opp behovet for kontroll og bidra til kompetanseoppbygging (Samferdselsdep. 2010). Myndighetene bør legge til rette for at man kan se transportsektoren som helhet, slik at kravene til ulike områder og anvendelser står i forhold til hverandre. Dette kan ivaretas ved et klart og tydelig regelverk, veiledning som ivaretar transportbransjens praktiske utfordringer og tilstrekkelig tilsyn. Implementering av ITS-løsninger krever god planlegging, og oversikt over involverte virksomheter, roller, funksjoner og informasjonsflyt. Slik vi ser det er det innført klare regler og rutiner på områder som har fått medias og datatilsynets oppmerksomhet, mens andre virksomheter fortsatt baserer seg på å lære av hendelser som skjer. Som aktørene selv påpeker kan uønskede hendelser hos en aktør få store ringvirkninger for andre i samme bransje (Øvstedal 2009). Det er ikke gitt at publikum og media skiller mellom de ulike aktørene, og regler, rutiner og arbeidsmåter kan måtte legges om for et stort nettverk av aktører. Dette gjør at bransjen selv kan være motivert for felles regelverk, retningslinjer og kompetansetiltak.

Det kan også legges føringer ved konsesjon for persontransport og i funksjonskontrakter, med tydelig informasjon og klare regler. Det er behov for klare regler for eiendomsrett over personopplysninger, for å opplyse trafikantene om registreringene (for eksempel at informasjon om registreringsenheter følger bilens manual) og for bruk av data. Det er også behov for å avklare

regler om registrering og lagring av personopplysninger i forhold til andre lover som Bokføringsloven og Arbeidsmiljøloven. I dag velges det forskjellige tekniske løsninger og tolkninger av regleverk som gir svært forskjellige føringer for personvernet, selv på områder som elektronisk billettering der det har vært informasjonsutveksling mellom aktørene. For trafikantene blir dette uoversiktlig.

Myndighetene kan bidra med tiltak som gir økt fokus på trafikantenes personvern, ved å legge til rette informasjon og veiledere, og ved selv å framstå som eksempel til etterfølgelse. Dette arbeidet må preges av langsiktighet, med føringer utover medias søkelys i øyeblikket. Tema som bør vektlegges, er formålet med registreringen, gyldig behandlingsgrunnlag og reelle valgmuligheter som basis for frivillighet og frivillig samtykke. Et skritt på veien bør være at behandlingsansvarlige utarbeider en sikkerhetspolicy der personvernet inngår som en viktig del av policyen. Eksempelvis bør Statens vegvesen, som et viktig ledd i sitt arbeid med å definere og implementere ulike ITS-løsninger og tiltak, basere tiltakene på en sikkerhetspolicy som gjøres tilgjengelig for alle trafikanter. EasyGo (samordnet elektronisk bompengebetaling for nordiske bompengesystem) har utarbeidet en slik sikkerhetspolicy som kan være et eksempel for andre.

Å øke kunnskapen om og interessen for personvernfremmende teknologier i transportsektoren, kan bidra til å redusere omfanget av personopplysninger og muligheten for innsyn i dem. I kapittel 4 så vi at innsikt i problemstillingen og gode rutiner i virksomheten, er en forutsetning både for innføring av personvernfremmende teknologier og for å at de skal gi ønsket effekt.

Transportsektoren vil stå ved mange veivalg og verdivalg

Den teknologiske utviklingen medfører at det blir stadig rimeligere og enklere å lagre store mengder data og å analysere dem. Det presenteres stadig nye muligheter og produkter som kan gjøre hverdagen enklere, sikrere og mer behagelig, og gi større valgfrihet samtidig som transportene effektiviseres. ITS bidrar til å gi trafikanter store fordeler med hensyn til komfort, effektivitet og sikkerhet, og løsningene blir i mange tilfeller godt mottatt av brukerne. Markedskreftene er sterke, og både myndigheter og fagmiljø ønsker å utnytte mulighetene. Mange system kan tas i bruk uten å lagre personopplysninger, eller med løsninger som sikrer at omfanget blir begrenset. Potensialet vil imidlertid være enda større uten slike begrensinger. Systemene utgjør også en infrastruktur som kan tas i bruk på flere måter med tilgang til nye aktører. Teknisk sett finnes det uante muligheter for dataregistrering og sporing, men personvernhensyn må legge føringer og begrensninger for anvendelse av teknologi.

Å vurdere de ulike mulighetene og formålene mot nytten av å ivareta personvernet, og å ivareta enkeltindividets rett til å velge selv, vil derfor være viktige verdivalg som vil ha konsekvenser. Utfordringene ligger i å ivareta vernet om personopplysninger uten å lage så rigide system at vi ikke kan ta ut de positive effektene av intelligente transportløsninger. Dette gjelder både miljøeffekter, effektive og behagelige private reiser, og effektivisering av næringstransport. Å ferdes i trafikken er, for de fleste av oss, noe av det farligste vi gjør. Derfor er det viktig at vi også på dette området utytter mulighetene for sikrere transport. Dette er i stor grad politiske valg, som bør bygge på en samlet vurdering av ulike samfunnseffekter.

Referanser

Arbeids- og administrasjonsdepartementet (2002): *FOR 2002-06-28 nr.656 Forskrift om elektronisk kommunikasjon med og i forvaltningen 28. juni 2002*. Lovdata.

Avinor, Jernbaneverket, Kystverket, Statens vegvesen, ITS Norge (2006*): ITS – Intelligente transport systemer. Overblikk, visjoner og mulighetsområder.* Arbeidsdokument. Oslo: Statens vegvesen.

Bang, B. og R. Wahl (2007): *ITS – IKT i transportsektoren. Klargjøring og avgrensning.* Rapport A07010. Trondheim: SINTEF Teknologi og samfunn.

Berg, C., Bayer, S.B. & G. Thesen (2008): *Ungtrafikk. Resultater fra et ISA-forsøk med unge* førere i Karmøy. Stavanger: IRIS

Borking, J. (2008): Organiszational adoption of Privacy Enhancing Technologies (PET). In Cas, J. (ed) (2009): *D7.3 PRISE Concluding Conference Proceedings*, "Towards privacy enhancing security technologies – the next steps" Vienna, April 28th and 29th 2008. PRISE consortium. www.prise.oeav.ac.at

Bjørnskau, T; Gripsrud, M; Grunnan, T. og T. Leite (2007): *Security i transport og personvernets grenser.* Rapport 914/2007. Oslo: Transportøkonomisk institutt.

Carstens, O.M.J. og Tate F.N. (2005): Intelligent speed adaption: accident savings and cost-benefit analysis. *Accident Analysis & Prevention* 37 (3) pp. 407-416.

Carstens, O., Fowkes M., Lai,f., Chorlton, K., Jameson, S., Tate F. & B. Simpkin (2008): *ISA-UK Intelligent Speed Adaption.* Final report. London: UK Department of Transport.

Datatilsynet (2002): *Risikovurdering av informasjonssystem*. Oppdatert 15.02.02, opptrykk 06.03.09. www.datatilsynet.no

Datatilsynet (2007): *Elektronisk billettering.* 04.07.2007, Sverre Engelsciøn. www.datatilsynet.no

Datatilsynet (2010): *Bruk av sporingsteknologi i virksomheters kjøretøy. Veiledning fra Datatilsynet, juli 2010.* (17.10.2010) www.datatilsynet.no

Datatilsynet (2010): Fakta om eCall. 13.08.2010, Atle Årnes og Gunnel Helmers. www.datatilsynet.no

Den europeiske menneskerettskonvensjonen, vedlegg i Justis- og Politidepartementet (1999): LOV 1999-05-21 nr 30: Lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven).

ETSI (2010): *Human Factors (HF); Intelligent Transport Systems (ITS); ICT in cars. Technical report ETSI TR 102 762 v1.1.1 (2010-04).* France: European Telecommunications Standards Institute.

Europakommisjonen (1995): *Personverndirektivet EU-direktiv 95/46/EF*. Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og fri utveksling av slike opplysninger.

Fornyings- og administrasjonsdepartementet (2009): *Individ og integritet*. Oslo: Norges offisielle utredninger (NOU):1.

Fornyings- og administrasjonsdepartementet (2000): *FOR 2000-12-15 nr 1265: Forskrift om behandling av personopplysninger (personopplysningsforskriften).* Oslo: Datatilsynet, Statsforvaltningsavdelingen.

Fornyings- og administrasjonsdepartementet (2008): *Vurdering av personvernkonsekvenser. Veileder til utredningsinstruksen.* Oslo.

Forsikringsselskapenes godkjenningsnemnd (2010): *Krav til søke- og gjenfinningssystemer for kjøretøy, anleggsmaskiner og båt med mer.* 3. utgave. Finansnæringens hovedorganisasjon.

Forsvarsdepartementet (1998): *Sikkerhetsloven*. Sist endret ved LOV-2005-06-17-81 fra 2006-01-01. Lovdata.

Foss, T. og O. Hjelkrem (2010): *Mulighetsstudie av anonym betaling i automatiske AutoPASS anlegg.* Rapport 15371. Trondheim: SINTEF Teknologi og samfunn.

Granau, F. (2008): The RFID chip development to meet known privacy and security issues. In Cas, J. (ed) (2009): *D7.3 PRISE Concluding Conference Proceedings*, "Towards privacy enhancing security technologies – the next steps" Vienna, April 28th and 29th 2008. PRISE consortium. www.prise.oeav.ac.at

Gruteser, M. & D. Grunwald (2005): Enhancing Location Privacy in Wireless LAN Through Disposable Interface Identifiers: A Quantitative Analysis. *MONET* 10, 3: 315-325. www.informatik.uni-trier.de/~ley/db/journals/monet/monet10.html#GruteserG05

Hide project (2009): *D3.4a Ethical Brief on PETs*. www.hideproject.org

ITS Norge (2009): *ITS Action Plan og forslag til direktiv fra EU. Rammeverk for utnyttelse av ITS på vegtransportområdet og for grenseflater med andre transportområder.* Notat fra Christiansen, februar 2009.

ITS Norge (2005): *Security og biometri i transportsektoren. Kartlegging av behov for Person-ID.* Oslo: ITS Norway multimodal

Justis- og politidepartementet (2009): *Skjult informasjon – åpen kontroll. Metodekontrollutvalget evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker.* Oslo: Norges offisielle utredninger (NOU 2009:15).

Justis- og politidepartementet (2000): *Lov 2000-04-14 nr 31: Lov om behandling av personopplysninger*. Lovdata.

Meland, S., Samstad, H., Wahl, R. & M. Killi (2007): *Utfordringer innenfor personvern, ansvar og roller ved ITS-anvendelser i transportsektoren.* SINTEF / TØI.

Ministry of Science Technology and Innovation (2005): Privacy enhancing Technologies. META group report v1.1. http://www.itst.dk/sikkerhed/privacy/filer/privacy-og-privacy-forum/Privacy%20Enhancing%20Technologies.pdf

Olsen, T. (2010): *Personvernøkende identitetsforvaltning*. Doktoravhandling. Oslo: Universitetet i Oslo, Juridisk fakultet.

Vegdirektoratet, Politidirektoratet, Helsedirektoratet, Utdanningsdirektoratet og Trygg Trafikk *Nasjonal tiltaksplan for trafikksikkerhet på veg 2010-2013*. Oslo.

Raguse, M.; Langfeldt, O. & M. Hansen (2008): *PRISE Project Deliverable 3.3. Proposal report. Privacy enhancing shaping security research and technology – A participatry apporach to develop acceptable and accepted principles for European Security Industries and Policies.* Kiel, Germany: PRICE consortium. http://www.prise.oeaw.ac.at/docs/PRISE_D3.3_Proposal_Report.pdf

Raguse, M.; Meints, M.; Langfeldt, O. & W. Peissl (2008): *PRISE Project D6.2. Criteria for privacy enhancing security technologies. Privacy enhancing shaping security research and technology – A participatry apporach to develop acceptable and accepted principles for*

European Security Industries and Policies. Kiel, Germany: PRICE consortium. http://www.prise.oeaw.ac.at/docs/PRISE_D_6.2_Criteria_for_privacy_enhancing_security_technologies.pdf

Ravlum, I. A. (2004): *Personvern og forbrukerrettigheter i transport. Nordisk seminar.* Rapport 745/2004.Oslo: Transportøkonomisk institutt.

Samferdselsdepartementet (2010): *Strategi. Intelligente transportsystemer.* Oslo: Samferdselsdepartementet.

Samferdselsdepartementet (2009): *St.m.16 (2008-2009): Nasjonal transportplan 2010-2019.* Oslo.

Scartum, D.W. (2001): *Personvern og lokasjonsbaserte tjenester*. Publisert på www.jus.uio.no

Schiefloe, P. M. (2010): Sikringsparadokser. Kronikk i Adresseavisen 28. mai. 2010. http://www.apertura.ntnu.no/folk/permsdok/Sikringsparadokser.pdf

Statens vegvesen (2009): *Strategi for AutoPASS (foreløpig rapport, versjon 0.89, 11. juni 2009).* Oslo: Statens vegvesen, Veg og trafikkavdelingen.

Statens vegvesen (2010): *Handlingsplan 2010 – 2013 (2019).* Oslo: Vegdirektoratet.

Statens vegvesen (2004): *Håndbok 206 – 1 Elektronisk billettering. Veiledning*. Oslo: Vegdirektoratet.

Statens vegvesen (2007): *ITS-Strategi for Statens vegvesen. Målrettet, troverdig og effektiv bruk av ITS – på veg mot et bedre samfunn.* Rapport nr 7/2007. Oslo: Vegdirektoratet, Veg- og trafikkavdelingen.

Teknologirådet (2005): *Elektroniske spor og personvern*. Rapport 1- 2005. Oslo: Teknologirådet.

Teknologirådet (2007): *Sikkerhet og personvern. Oversikt over sikkerhetsteknologier. PRISE Privacy enhancing shaping security research and technology – A participatry apporach to develop acceptable and accepted principles for European Security Industries and Policies.* Oslo: Teknologirådet.

Wahl, Ragnhild; Skjetne, Eirik; Bang, Børge; Tveit, Ørjan (2007): *Fremtidig ITS-anvendelse i transportsektoren.* Rapport A07005. Trondheim: SINTEF Teknologi og samfunn.

Williams, Bob (2008): *Intelligent Transport Systems Standards*. Boston: Artech House.

Øvstedal, Liv (2009): *Kan man reise anonymt i Norge? Personopplysningsloven i transportsektoren.* Rapport A10918. Trondheim: SINTEF Teknologi og samfunn.

Nettadresser:

www.autopass.no
www.datatilsynet.no
www.esafety.org
www.esafetysupport.org
www.jus.io.no
www.mhf.se
www.norsknavigasjon.no
www.nrkbeta.no
www.obdii.com
www.ruter.no
www.tkort.no
www.sintef.no/Teknologi-og-samfunn/Sikkerhet/SjekkIT

Vedlegg 1: Risikovurdering ved automatisk nummerskiltgjenkjenning

I dette vedlegget presenterer vi vurderingen av konsekvens og sannsynlighet for hver av de identifiserte uønskede hendelsene for behandling av personopplysninger for automatisk nummerskiltgjenkjenning (se kap. 3.2). Automatisk nummerskiltgjenkjenning kan ha ulike bruksområder og ikke alle vurderinger gjelder for alle bruksområdene.

Skalaen for konsekvens (1-4) og for sannsynlighet (1-4) er presentert i kapittel 3. Vi viser først en oppsummerende tabell og deretter vurderingen av årsaker og evt. medvirkende personer, konsekvens, sannsynlighet og resulterende risikonivå for hver hendelse.

Tabell v1: Automatisk nummerskiltgjenkjenning:
Oversikt over identifiserte hendelser, vurdert konsekvens og sannsynlighet

	Hendelse	Vurdert konsekvens	Vurdert sannsynlighet	Resulterende risikonivå
Utlevering				
1	Informasjon utlevert til uvedkommende	2	2	**4**
2	Informasjon ikke slettet så snart som mulig	3	3	**9**
3	Det innhentes flere opplysninger enn nødvendig	3	1	**3**
4	Informasjon formidles til andre aktører	2	2	**4**
5	Informasjon benyttes til andre formål	2	2	**4**
Endring				
6	Registrerte opplysninger blir endret	3	1	**3**
Utilgjengelighet				
7	Data er ikke tilgjengelig for behandling ved passering	3	2	**6**
8	Data er ikke tilgjengelig for behandling ved avregning	2	1	**2**
9	Data er ikke tilgjengelig for kontroll for kunden	2	2	**4**
10	Trafikanten kjenner ikke hvilke data som er registrert	2	2	**4**

Utlevering av personopplysninger – brudd på konfidensialitet

Konfidensialitet innebærer at informasjonen ikke skal være tilgjengelig for uvedkommende.

Hendelse 1 (utlevering) *Risikonivå: 2 x 2 = 4*	Informasjon om en eller flere passeringer (evt. beskrivelse av et reisemønster) til en identifiserbar trafikant (bileier, bilfører, medpassasjerer) blir utlevert til noen som ikke skal ha tilgang til slik informasjon. Trafikantens integritet kan eller vil svekkes.
Årsak og evt. utløsende person(er)	[1] En utenforstående skaffer seg tilgang til databehandlerens sentralsystem pga for dårlige sikkerhetsrutiner og adgangskontroll (kopiering på stedet, hacking), kopierer data og bringer disse videre eller bruker de selv. [2] En ansatt får tilgang til data vedkommende ikke burde ha tilgang til, pga dårlige sikkerhetsrutiner og adgangskontroll, og bringer disse videre eller bruker de selv. [3] En ansatt som har tilgang til informasjon knyttet til en trafikant, bryter taushetserklæringen og bringer data videre eller bruker de selv. [4] Data om reiser/passeringer blir utlevert/sendt til feil trafikant pga feil i sentralsystemet eller databehandlerfeil. [5] En utenforstående får tilgang til registrerte passeringer og kan sjekke eier av bilen i kjøretøyregisteret.
Konsekvensvurdering K = 2	Hendelsen er trolig en av de hendelsene som en trafikant opplever som mest krenkende for personvernet. Selv om man kan observeres på en biltur, så er lagring og evt. misbruk av lagrede data om reisevirksomheten et følsomt tema for trafikanten. Omfattende data om enkeltpersoner kan oppleves svært krenkende. K = 3: Dersom hendelsen gjelder svært mange trafikanter, kan den evt. kategoriseres som en hendelse med konsekvens K = 3. Det kan imidlertid være mer alvorlig med omfattende data om enkeltpersoner enn enkeltdata om mange personer.
Sannsynlighetsvurdering S = 2	Sannsynlighetsnivå S = 2 er knyttet til at egne medarbeidere med forsett og noe kompetanse kan søke informasjon om bestemte personer etc. Sannsynligheten for at en utenforstående henter ut data ansees som liten (S = 1) både fordi det finnes enklere måter å skaffe tilsvarende data på og fordi det krever spesiell kompetanse og tilgang til sikkerhetsnøkkel og/eller samarbeid med personer innenfor systemet. Sannsynligheten for at en utenforstående prøver å få utlevert opplysninger ved å utgi seg som kunde er relativt stor, men for å lykkes må det enten være svikt i eller mangelfulle rutiner.

Hendelse 2 (utlevering) *Risikonivå: 3 x 3 = 9*	Data om passeringer (evt. beskrivelse av et reisemønster) blir ikke slettet så snart systemet har foretatt behandling av passeringsdata og avregning av transaksjoner og trafikanten har hatt rimelig tid til å kontrollere behandling av data.
Årsak og evt. utløsende person(er)	[1] Programtekniske feil i betalingssystemet [2] Svikt i rutiner og/eller dårlige rutiner
Konsekvensvurdering K = 3	Hendelsen er trolig en av de hendelsene som en trafikant opplever som mest krenkende for personvernet. Selv om man kan observeres på en biltur, så er lagring og evt. misbruk av lagrede data om reisevirksomheten et følsomt tema for trafikanten. For adgangskontroll kan innhentede og lagrede data, hvis de kommer uvedkommende tilhende, gi innsyn i rutiner og andre forhold som man ikke ønsker å informere om.
Sannsynlighetsvurdering S = 3	Bevisstheten om sletting av data varierer mellom virksomheter og anvendelsesområder. For noen virksomheter er bevisstheten høy og sannsynligheten på nivå 1. For andre anvendelsesområder og virksomheter er begrunnelsene for sletting kanskje ikke like åpenbare. Dermed er det mer avhengig av at virksomheten har ansatte med god kompetanse på datasikkerhet. Sannsynlighetsnivå 3 er knyttet til evt. manglende eller dårlige rutiner i egen virksomhet. Av samme grunn som for hendelse 1 er det relativt liten sannsynlighet for at utenforstående endrer lagringstid for dataene.

Hendelse 3 (utlevering) *Risikonivå: 3 x 1 = 3*	Databehandler innhenter personopplysninger som ikke er nødvendig for adgangskontroll, trafikkontroll, trafikkanalyse eller korrekt gjennomføring av betaling, eller for å oppfylle forpliktelser iht. implisitte og eksplisitte avtaler med kunden.
Årsak og evt. utløsende person(er)	[1] Databehandler (eksempelvis eier eller operatør av et bompengesystem) bygger opp kunderegistre med data som gjør det mulig å danne typiske kundeprofiler, reisemønstre og avanserte statistikker for bruk i planlegging av nye produkter. [2] Databehandler har manglende bevissthet i forhold til data som innhentes fra kunden.
Konsekvensvurdering K = 3	Hendelsen kan oppleves som tap av integritet ved at trafikanten oppgir opplysninger om seg selv som vedkommende ellers ikke ville gitt fra seg, eller som vedkommende ikke forstår hensikten med å gi fra seg. For adgangskontroll kan innhentede og lagrede data, hvis de kommer uvedkommende tilhende, gi innsyn i rutiner og andre forhold som man ikke ønsker å informere om.
Sannsynlighetsvurdering S = 2	Sannsynligheten for denne hendelsen er vurdert som moderat. Motivasjonen er liten, fordi virksomhetene er bevisste på at registrering og behandling av data koster tid og penger. Det er også en del oppmerksomhet rundt problemstillingen.

Hendelse 4 (utlevering) *Risikonivå: 2 x 2 = 4*	Databehandler formidler eller selger innhentede personopplysninger til parter utenfor nummerskiltgjenkjenningssystemet, som ønsker å benytte slike opplysninger til produktutvikling eller markedsføring av egen produkter eller tjenester, for eksempel reklame.
Årsak og evt. utløsende person(er)	[1] Databehandler selger deler av eller hele kunderegisteret til firma som tilbyr ulike tjenester. [2] Svikt i rutiner mht utlevering av personopplysninger til myndigheter. [3] Svikt i rutiner mht utlevering av personopplysninger til kunde.
Konsekvensvurdering K = 2	Hendelsen kan oppleves som krenkende og et brudd på tilliten mellom trafikant og databehandler. Dersom hendelsen omfatter mange kunder og bruken oppfattes som meget krenkende kan konsekvensen kategoriseres som K = 3.
Sannsynlighetsvurdering S = 2	Sannsynligheten for denne hendelsen er vurdert som moderat. Motivasjonen for å få tilgang til informasjonen kan være stor hos utenforstående aktører. Samtidig vil hendelsen ha vesentlig betydning for omdømme til den databehandler som er årsak til hendelsen.

Hendelse 5 (utlevering) *Risikonivå: 2 x 2 = 4*	Databehandler bruker innhentede personopplysninger til annen databehandling enn det som framgår av formål, avtaler og databehandlers sikkerhetspolicy.
Årsak og evt. utløsende person(er)	[1] Databehandler utarbeider typiske kundeprofiler og reisemønstre for bruk i planlegging av nye produkter og tjenester og utarbeidelse av avanserte statistikker. [2] Databehandler har manglende bevissthet i forhold til data som innhentes fra trafikanten, avtaler inngått med kunder og egen sikkerhetspolicy.
Konsekvensvurdering K = 2	Hendelsen oppleves som krenkende og et brudd på tilliten mellom trafikant og databehandler. Dersom hendelsen omfatter mange kunder og bruken oppfattes som meget krenkende kan konsekvensen kategoriseres som K = 3.
Sannsynlighetsvurdering S = 2	Sannsynligheten for denne hendelsen er vurdert som moderat. Motivasjonen for å få mest mulig ut av tilgjengelige data kan være stor. Samtidig kan hendelsen ha betydning for omdømmet til databehandler.

Endring av personopplysninger – brudd på integritet

Integritet innebærer at personopplysningene skal beskyttes mot uønskede og ikke-autoriserte endringer.

Hendelse 6 (endring) *Risikonivå: 3 x 1 = 3*	Informasjon om passeringer, betalingshistorikk eller kundens avtale blir endret slik at kunden kan lide tap av anseelse og økonomisk tap.
Årsak og evt. utløsende person(er)	[1] Programtekniske feil i betalingssystemet [2] Feil utført av kundebehandler ved evt. manuell databehandling. [3] En utenforstående skaffer seg tilgang til produkteiers sentralsystem pga for dårlige sikkerhetsrutiner og adgangskontroll (hacking) og endrer data, eksempelvis endrer avtalestatus eller passeringshistorikk for en eller flere kunder.
Konsekvensvurdering K = 3	For de fleste anvendelser er konsekvensene moderate (K = 2). For adgangskontroll til viktige anlegg osv. kan konsekvensene i noen tilfeller være alvorlige. Det kan evt. også oppleves dramatisk feilaktig å bli mistenkt for handlinger man ikke har begått eller for ikke ha betalt avgifter, dvs. feil i registre som passeringsdata sjekkes mot.
Sannsynlighetsvurdering S = 1	Slike endringer krever normalt spisskompetanse og gode muligheter. Evt. programtekniske feil og feil ved manuell databehandling avsløres raskt og vil neppe ha konsekvenser for mange passeringer.

Personopplysningene er utilgjengelige for behandling

Tilgjengelighet innebærer at personopplysningene skal være relevante, tilstrekkelige og tilgjengelige for autorisert behandling.

Hendelse 7 (utilgjengelighet) *Risikonivå: 3 x 2 = 6*	Data om trafikantens avtaleforhold er ikke er tilgjengelig. Trafikanten blir stengt ute (adgangskontroll) eller belastet økonomisk som om vedkommende ikke er kunde fordi data om kundens avtaleforhold ikke er tilgjengelig og kan behandles på korrekt måte.
Årsak og evt. utløsende person(er)	[1] Teknisk feil eller manglende oppdatering av registre på grunn av dårlige rutiner eller svikt i rutiner.
Konsekvensvurdering K = 3	For de fleste anvendelser er konsekvensene moderate (K = 2). For adgangskontroll til viktige anlegg osv. kan konsekvensene i noen tilfeller være alvorlige.
Sannsynlighetsvurdering S = 2	Sannsynligheten for tekniske feil eller mangelfulle rutiner regnes som moderat.

Hendelse 8 (utilgjengelighet) *Risikonivå: 2 x 1 = 1*	En trafikant blir utsatt for økonomisk tap fordi data om avtaleforhold og passeringer ikke er tilgjengelig når produktet/tjenesten skal avregnes. Eksempelvis blir trafikanten trukket for separate passeringer også i de tilfellene disse inngår i samme sone og tidsperiode og skal avregnes som én passering.
Årsak og evt. utløsende person(er)	[1] Teknisk feil eller manglende oppdatering av sentralsystemet på grunn av dårlige rutiner eller svikt i rutiner.
Konsekvensvurdering *K = 2*	Hendelsen kan medføre økonomisk tap, men dette vil være gjenopprettelig.
Sannsynlighetsvurdering *S = 1*	Sannsynligheten for tekniske feil eller mangelfulle rutiner regnes som moderat, og det er sannsynlig at de vil oppdages og rettes innen rimelig tid.

Hendelse 9 (utilgjengelighet) *Risikonivå: 2 x 2 = 4*	En trafikant blir utsatt for økonomisk tap fordi data om passeringer og betaling ikke er tilgjengelig slik at trafikanten kan kontrollere behandlingen av data.
Årsak og evt. utløsende person(er)	[1] Manglende oppdatering i sentralsystemet pga. svikt i rutiner, dårlige rutiner eller teknisk feil. [2] Terskelen for bruk av slik kontrollmulighet er for høy, eksempelvis for eldre personer som ikke har tilgang til internett. [3] Kunden er ikke kjent med muligheten.
Konsekvensvurdering *K = 2*	Hendelsen kan medføre økonomiske tap dersom det oppstår systematiske feil over tid, som trafikanten ikke har mulighet til å kontrollere og avdekke.
Sannsynlighetsvurdering *S = 2*	Sannsynligheten vurderes som moderat ved at noen trafikanter ikke kjenner til mulighetene, mens brukerterskelen (f.eks. tilgang til internett) kan være for høy for andre.

Hendelse 10 (utilgjengelighet) *Risikonivå: 2 x 2 = 4*	En trafikant får ikke vite hvilke personrelaterte data som er lagret i nummerskiltgjenkjenningssystemet.
Årsak og evt. utløsende person(er)	[1] Trafikanten kjenner ikke sine egne rettigheter [2] Databehandler kjenner ikke kundens rettigheter [3] Data er ikke tilgjengelig på en slik form at de er egnet for utlevering til trafikanten [4] Dataene trafikanten etterspør kan ikke knyttes til identifiserbar trafikant (anonyme data).
Konsekvensvurdering *K = 2*	Hendelsen kan oppleves som krenkende i og med at dette er en rettighet vi har iht. Personopplysningsloven.
Sannsynlighetsvurdering *S = 2*	Bevisstheten rundt den registrertes rettigheter vil variere mye mellom ulike virksomheter og anvendelsesområder. Sannsynligheten vurderes som moderat ut fra 1) at trafikanten ikke kjenner sine rettigheter, 2) at databehandler ikke kjenner den registrertes rettigheter eller at dataene ikke er på en slik form at de egner seg for utlevering. Dataene som etterspørres kan også være anonyme; dvs. at de ikke kan knyttes til identifiserbar person.

Vedlegg 2: Risikovurdering ved sporing av kjøretøy

I dette vedlegget presenterer vi vurderingen av konsekvens og sannsynlighet for hver av de identifiserte uønskede hendelsene for behandling av personopplysninger for sporing av kjøretøy (se kap. 3.3). Sporing av kjøretøy kan ha ulike bruksområder og ikke alle vurderinger gjelder for alle bruksområdene.

Skalaen for konsekvens (1-4) og for sannsynlighet (1-4) er presentert i kapittel 3. Vi viser først en oppsummerende tabell og deretter vurderingen av årsaker og evt. medvirkende personer, konsekvens, sannsynlighet og resulterende risikonivå for hver hendelse.

Tabell v2: Sporing av kjøretøy: Oversikt over identifiserte hendelser, vurdert konsekvens og sannsynlighet

	Hendelse	Vurdert konsekvens	Vurdert sannsynlighet	Resulterende risikonivå
Utlevering				
1	Informasjon utlevert til uvedkommende	2	3	**6**
2	Informasjon ikke slettet så snart som mulig	3	3	**9**
3	Det innhentes flere opplysninger enn nødvendig	3	3	**9**
4	Informasjon formidles til andre aktører	2	2	**4**
5	Informasjon benyttes til andre formål	2	2	**4**
Endring				
6	Registrerte opplysninger blir endret	3	1	**3**
Utilgjengelighet				
7	Data er ikke tilgjengelig (andre konsekvenser)	2	2	**4**
8	Data er ikke tilgjengelig (konsekvenser for 3.part)	2	1	**2**
9	Data er ikke tilgjengelig (økonomiske konsekvenser for trafikant)	2	2	**4**
10	Trafikanten kjenner ikke hvilke data som er registrert	2	2	**4**

Utlevering av personopplysninger – brudd på konfidensialitet

Konfidensialitet innebærer at informasjonen ikke skal være tilgjengelig for uvedkommende.

Hendelse 1 (utlevering) *Risikonivå: 2 x 3 = 6*	Informasjon om posisjon (evt. beskrivelse av et reisemønster) til en identifiserbar trafikant (bileier, bilfører) blir utlevert til noen som ikke skal ha tilgang til slik informasjon. Trafikantens integritet kan eller vil svekkes.
Årsak og evt. utløsende person(er)	[1] En utenforstående skaffer seg tilgang til databehandlers pc, mobiltelefon eller sentralsystem pga for dårlige sikkerhetsrutiner og adgangskontroll (hacking, evt. fysisk tilgang), kopierer data og bringer disse videre eller bruker de selv. [2] En ansatt får tilgang til data vedkommende ikke burde ha tilgang til, pga dårlige sikkerhetsrutiner og adgangskontroll, og bringer disse videre eller bruker de selv. [3] En ansatt som har tilgang til informasjon knyttet til en trafikant (bilfører, bileier), bryter taushetserklæringen og bringer data videre eller bruker de selv. [4] Data om reiser (posisjon og tid) blir utlevert/sendt til en utenforstående pga feil i sentralsystemet eller databehandlerfeil. [5] En utenforstående får tilgang til registrerte posisjoner og kan sjekke eier av bilen i kjøretøyregisteret.
Konsekvensvurdering *K = 2*	For flåtestyring gjelder kjøring på arbeidsoppdrag og man er klar over overvåkingen. Dette vil derfor ofte være lite følsomme data for bilfører, men det kan være unntak (eksempelvis ærend av mer privat karakter som må gjennomføres i arbeidstiden). For privatpersoner som blir overvåket uten å være klar over det, kan dette oppleves som svært følsomt. K = 3: Dersom hendelsen gjelder svært mange trafikanter, kan den evt. kategoriseres som en hendelse med konsekvens K = 3.
Sannsynlighetsvurdering *S = 3*	Det kan være forskjellig bevissthet rundt behovet for å skjerme slike data. Sannsynlighetsnivå S = 3 er knyttet til sikkerhetsbrudd ved uaktsomhet hos egne medarbeidere eller at utenforstående aktivt går inn for å bryte sikkerhetstiltak.

Hendelse 2 (utlevering) *Risikonivå: 2 x 3 = 6*	Data om posisjon og tid (evt. beskrivelse av et reisemønster) blir ikke slettet så snart som mulig. For flåtestyring kan dataene gi grunnlag for (anonymisert) statistikk. Det kan evt. være grunnlag for å beholde data lenge som bevis ved etterforskning (politisaker). For eCall synes det ikke aktuelt å lagre personidentifiserbare data etter at hendelsen er tatt hånd om, men det kan være aktuelt med anonymisert statistikk.
Årsak og evt. utløsende person(er)	[1] Programtekniske feil i sporingsprogrammet [2] Svikt i rutiner og/eller dårlige rutiner [3] Databehandler har manglende bevissthet i forhold til lagring av data, evt. lagring med forsett.
Konsekvensvurdering *K = 2*	For flåtestyring gjelder kjøring på arbeidsoppdrag og man er klar over overvåkingen. Dette vil derfor ofte være lite følsomme data for bilfører, men det kan være unntak (eksempelvis ærend av mer privat karakter som må gjennomføres i arbeidstiden). For privatpersoner som blir overvåket uten å være klar over det, kan dette oppleves som svært følsomt. K = 3: Dersom hendelsen gjelder svært mange trafikanter, kan den evt. kategoriseres som en hendelse med konsekvens k = 3.
Sannsynlighetsvurdering *S = 3*	Bevisstheten om sletting av data varierer mellom virksomheter og anvendelsesområder. For noen virksomheter er bevisstheten høy og sannsynligheten på nivå 1. For andre anvendelsesområder og virksomheter er begrunnelsene for sletting kanskje ikke like åpenbare. Dermed er det mer avhengig av at virksomheten har ansatte med god kompetanse på datasikkerhet.

Hendelse 3 (utlevering) *Risikonivå: 3 x 3 = 9*	Databehandler innhenter personopplysninger som ikke er nødvendige for sporingssystemet (flåtestyring eller andre anvendelser).
Årsak og evt. utløsende person(er)	[1] Databehandler bygger opp registre med data som gjør det mulig å danne typiske bilførerprofiler, reisemønstre og avanserte statistikker for bruk i planlegging. [2] Databehandler har manglende bevissthet i forhold til data som innhentes fra bilfører/bileier.
Konsekvensvurdering *K = 3*	Hendelsen kan oppleves som tap av integritet ved at kunden oppgir opplysninger om seg selv som vedkommende ellers ikke ville gitt fra seg eller som vedkommende ikke forstår hensikten med å gi fra seg. For sporing av kjøretøy kan innhentede og lagrede data, hvis de kommer uvedkommende tilhende, gi innsyn i enkeltpersoner bevegelser, aktiviteter og rutiner og i rutiner og forhold ved bedriften som man ikke ønsker å informere om.
Sannsynlighetsvurdering *S = 3*	Sannsynligheten for denne hendelsen er vurdert som høy, begrunnet med at sikkerhetsbrudd kan skje ved uaktsomhet hos egne ansatte. Kobling av ulike registre kan skje ved uaktsomhet, som for eksempel vaktlister, telefonlister, bursdagslister og oversikt over kjøretøy, mens bevisstheten som regel er høy for andre typer informasjon om ansatte.

Hendelse 4 (utlevering) *Risikonivå: 2 x 2 = 4*	Databehandler formidler eller selger innhentede personopplysninger til parter utenfor sporingssystemet, som ønsker å benytte slike opplysninger til produktutvikling eller markedsføring av egen produkter eller tjenester, for eksempel reklame.
Årsak og evt. utløsende person(er)	[1] Databehandler selger deler av eller hele sporingsregisteret til firma som tilbyr ulike tjenester. [2] Svikt i rutiner mht utlevering av personopplysninger til myndigheter. [3] Svikt i rutiner mht utlevering av personopplysninger til kunde.
Konsekvensvurdering *K = 2*	Hendelsen kan oppleves som krenkende og et brudd på tilliten mellom trafikant og databehandler. Dersom hendelsen omfatter mange trafikanter (bilførere) og bruken oppfattes som meget krenkende kan konsekvensen kategoriseres som K = 3.
Sannsynlighetsvurdering *S = 2*	Sannsynligheten for denne hendelsen er vurdert som moderat. Motivasjonen for å få tilgang til informasjonen kan være stor hos utenforstående aktører. Samtidig vil hendelsen ha vesentlig betydning for omdømme til den applikasjons-/produkteier som er årsak til hendelsen.

Hendelse 5 (utlevering) *Risikonivå: 2 x 2 = 4*	Databehandler bruker innhentede personopplysninger til annen databehandling enn det som framgår av formål, avtaler og databehandlers sikkerhetspolicy.
Årsak og evt. utløsende person(er)	[1] Databehandler utarbeider typiske bilførerprofiler, reisemønstre og avanserte statistikker for bruk i planlegging. [2] Databehandler har manglende bevissthet i forhold til data som innhentes fra bilfører/bileier.
Konsekvensvurdering *K = 2*	Hendelsen kan oppleves som krenkende og et brudd på tilliten mellom trafikant og databehandler. Dersom hendelsen omfatter mange trafikanter og bruken oppfattes som meget krenkende kan konsekvensen kategoriseres som K = 3.
Sannsynlighetsvurdering *S = 2*	Sannsynligheten for denne hendelsen er vurdert som moderat. Motivasjonen kan være stor, samtidig som videre analyse av data krever tid og ressurser.

Endring av personopplysninger – brudd på integritet

Integritet innebærer at personopplysningene skal beskyttes mot uønskede og ikke-autoriserte endringer.

Hendelse 6 (endring) *Risikonivå: 3 x 1 = 3*	Informasjon om posisjon, sted og kjøretøy-id blir endret. Dette kan evt. ha betydning for økonomisk oppgjør for bilfører, eller for spørsmål om skyld.
Årsak og evt. utløsende person(er)	[1] Programtekniske feil i sporingssystemet [2] Feil utført av databehandler ved evt. manuell databehandling. [3] En utenforstående skaffer seg tilgang til databehandlers sentralsystem pga for dårlige sikkerhetsrutiner og adgangskontroll (hacking) og endrer data, eksempelvis endrer kjøretøy-id eller posisjonsdata for et eller flere kjøretøy.
Konsekvensvurdering *K = 3*	Både for næringstransport og ved mistanke om kriminalitet kan endring av lagrede data ha vesentlige konsekvenser.
Sannsynlighetsvurdering *S = 1*	Slike endringer krever normalt spisskompetanse og gode muligheter. I noen tilfeller kan det være vanskelig å oppdage evt. databehandlerfeil eller programtekniske feil, slik at feilen kan vedvare over tid.

Personopplysningene er utilgjengelige for behandling

Tilgjengelighet innebærer at personopplysningene skal være relevante, tilstrekkelige og tilgjengelige for autorisert behandling.

Hendelse 7 (utilgjengelighet) *Risikonivå: 2 x 2 = 4*	Sporingsdata er ikke er tilgjengelig. Et eksempel kan være at ledig bil ikke blir tildelt oppdrag fordi vedkommendes posisjon ikke blir registrert på korrekt måte.
Årsak og evt. utløsende person(er)	[1] Manglende registrering av posisjon pga teknisk feil, dårlige rutiner eller svikt i rutiner. [2] Kjøretøy-id er ikke registrert som følge av teknisk feil, databehandlerfeil, dårlige rutiner eller svikt i rutiner.
Konsekvensvurdering *K = 2*	For de fleste anvendelser er konsekvensene moderate; f.eks. manglende tildeling av kjøreoppdrag eller at det tar lengre tid å spore en stjålet bil (K = 2). For eCall er utilgjengelighet svært alvorlig.
Sannsynlighetsvurdering *S = 2*	Sannsynligheten for tekniske feil eller mangelfulle rutiner regnes som moderat.

Hendelse 8 (utilgjengelighet) *Risikonivå: 2 x 1 = 2*	En kunde blir utsatt for økonomisk tap fordi nærmeste ledige bil ikke blir tildelt oppdraget.
Årsak og evt. utløsende person(er)	[1] Teknisk feil eller manglende oppdatering av sentralsystemet på grunn av dårlige rutiner eller svikt i rutiner.
Konsekvensvurdering *K = 2*	Hendelsen kan medføre økonomisk tap, men dette vil være gjenopprettelig.
Sannsynlighetsvurdering *S = 1*	Sannsynligheten for tekniske feil eller mangelfulle rutiner regnes som liten, dvs. feil vil bli rettet relativt raskt.

Hendelse 9 (utilgjengelighet) *Risikonivå: 2 x 2 = 4*	En trafikant (bileier/bilfører) blir utsatt for økonomisk tap fordi gjennomførte turer ikke kan dokumenteres.
Årsak og evt. utløsende person(er)	[1] Manglende registrering av posisjon pga teknisk feil, dårlige rutiner eller svikt i rutiner. [2] Kjøretøy-id er ikke registrert som følge av teknisk feil, databehandlerfeil, dårlige rutiner eller svikt i rutiner.
Konsekvensvurdering *K = 2*	Hendelsen kan medføre økonomisk tap, men dette vil være gjenopprettelig.
Sannsynlighetsvurdering *S = 2*	Sannsynligheten for tekniske feil eller mangelfulle rutiner regnes som moderat og feil vil bli rettet relativt raskt når de først oppdages.

Hendelse 10 (utilgjengelighet) *Risikonivå: 2 x 2 = 4*	En trafikant (bilfører/bileier) får ikke vite hvilke personrelaterte data som lagres i sporingssystemet.
Årsak og evt. utløsende person(er)	[1] Bilfører/bileier kjenner ikke sine rettigheter [2] Databehandler kjenner ikke den registrertes rettigheter [3] Data er ikke tilgjengelig på en slik form at de er egnet for utlevering til den registrerte. [4] Dataene som etterspørres kan ikke knyttes til identifiserbart kjøretøy (anonyme data).
Konsekvensvurdering *K = 2*	Hendelsen kan oppleves som krenkende i og med at dette er en rettighet som den registrerte har iht. Personopplysningsloven.
Sannsynlighetsvurdering *S = 2*	Bevisstheten rundt den registrertes rettigheter vil variere mye mellom ulike virksomheter og anvendelsesområder. Sannsynligheten vurderes som moderat ut fra 1) at den registrerte ikke kjenner sine rettigheter, 2) at databehandler ikke kjenner den registrertes rettigheter eller at dataene ikke er på en slik form at de egner seg for utlevering. Dataene som etterspørres kan også være anonyme; dvs. at de ikke kan knyttes til identifiserbar person.

Vedlegg 3: Risikovurdering ved lokasjonsbaserte tjenester

I dette vedlegget presenterer vi vurderingen av konsekvens og sannsynlighet for hver av de identifiserte uønskede hendelsene for behandling av personopplysninger for lokasjonsbaserte tjenester (se kap. 3.4). Lokasjonsbaserte tjenester har mange bruksområder og alle vurderinger vil ikke gjelde alle bruksområdene.

Skalaen for konsekvens (1-4) og for sannsynlighet (1-4) er presentert i kapittel 3. Vi viser først en oppsummerende tabell og deretter vurderingen av årsaker og evt. medvirkende personer, konsekvens, sannsynlighet og resulterende risikonivå for hver hendelse.

Tabell v3: Lokasjonsbaserte tjenester:
Oversikt over identifiserte hendelser, vurdert konsekvens og sannsynlighet

	Hendelse	Vurdert konsekvens	Vurdert sannsynlighet	Resulterende risikonivå
Utlevering				
1	Informasjon utlevert til uvedkommende	2	3	**6**
2	Informasjon ikke slettet så snart som mulig	2	2	**4**
3	Det innhentes flere opplysninger enn nødvendig	3	3	**9**
4	Informasjon formidles til andre aktører	2	2	**4**
5	Informasjon benyttes til andre formål	2	2	**4**
Endring				
6	Registrerte opplysninger blir endret	2	1	**2**
Utilgjengelighet				
7	Data er ikke tilgjengelig for kunden (fare for helse etc.)	2	2	**4**
8	Data er ikke tilgjengelig for kunden (økonomiske konsekvenser)	2	2	**4**
9	Data er ikke tilgjengelig for tjenestetilbydere	3	2	**6**
10	Trafikanten kjenner ikke hvilke data som er registrert	2	2	**4**

Utlevering av personopplysninger – brudd på konfidensialitet

Konfidensialitet innebærer at informasjonen ikke skal være tilgjengelig for uvedkommende.

Hendelse 1 (utlevering) *Risikonivå: 2 x 3 = 6*	Informasjon om posisjon (evt. beskrivelse av et reisemønster) til en identifiserbar trafikant blir utlevert til noen som ikke skal ha tilgang til slik informasjon. Trafikantens integritet kan eller vil svekkes.
Årsak og evt. utløsende person(er)	[1] En utenforstående skaffer seg tilgang til databehandlers pc, mobiltelefon eller sentralsystem pga for dårlige sikkerhetsrutiner og adgangskontroll (hacking, evt. fysisk tilgang), kopierer data og bringer disse videre eller bruker de selv. [2] En ansatt får tilgang til data vedkommende ikke burde ha tilgang til, pga dårlige sikkerhetsrutiner og adgangskontroll, og bringer disse videre eller bruker de selv. [3] En ansatt som har tilgang til informasjon knyttet til en trafikant, bryter taushetserklæringen og bringer data videre eller bruker de selv. [4] Data om reiser (posisjon og tid) blir utlevert/sendt til en utenforstående pga feil i sentralsystemet eller databehandlerfeil. [5] En utenforstående får tilgang til registrerte posisjoner og kan sjekke personens identitet eller eier av kjøretøy.
Konsekvensvurdering *K = 2*	Dette kan oppleves som særlig krenkende og som tillitsbrudd i forhold til tjenesteyter. K = 3: Dersom hendelsen gjelder svært mange trafikanter eller personer som trenger særlig beskyttelse, kan den evt. kategoriseres som en hendelse med konsekvens K = 3.
Sannsynlighetsvurdering *S = 3*	Det kan være forskjellig bevissthet rundt behovet for å skjerme slike data. Sannsynlighetsnivå S = 3 er knyttet til sikkerhetsbrudd ved uaktsomhet hos egne medarbeidere eller at utenforstående aktivt går inn for å bryte sikkerhetstiltak.

Hendelse 2 (utlevering) *Risikonivå: 2 x 2 = 4*	Data om posisjon (evt. beskrivelse av et reisemønster) blir ikke slettet så snart som mulig, f.eks. etter gjennomført oppdrag eller etter betaling for tjenesten.
Årsak og evt. utløsende person(er)	[1] Programtekniske feil i sporingsprogrammet [2] Svikt i rutiner og/eller dårlige rutiner [3] Databehandler har manglende bevissthet i forhold til lagring av data, evt. lagring med forsett.
Konsekvensvurdering *K = 2*	Dette kan oppleves som særlig krenkende og som tillitsbrudd i forhold til tjenesteyter. K = 3: Dersom hendelsen gjelder svært mange trafikanter eller personer som trenger særlig beskyttelse, kan den evt. kategoriseres som en hendelse med konsekvens K = 3.
Sannsynlighetsvurdering *S = 2*	For noen anvendelser kan lagring av data for statistikk etc. synes hensiktsmessig, for andre anvendelsesområder synes det bare å medføre ekstra arbeid og ressurser. Bevisstheten om sletting av data varierer mellom virksomheter og anvendelsesområder. For noen virksomheter er bevisstheten høy og sannsynligheten på nivå 1. For andre anvendelsesområder og virksomheter er begrunnelsene for sletting kanskje ikke like åpenbare. Dermed er det mer avhengig av at virksomheten har ansatte med god kompetanse på datasikkerhet.

Hendelse 3 (utlevering) *Risikonivå: 3 x 3 = 9*	Databehandler innhenter personopplysninger som ikke er nødvendige for de lokasjonsbaserte tjenestene.
Årsak og evt. utløsende person(er)	[1] Databehandler bygger opp registre med data som gjør det mulig å danne typiske kundeprofiler, reisemønstre og avanserte statistikker for bruk i planlegging. [2] Databehandler har manglende bevissthet i forhold til data som innhentes fra kunde/trafikant.
Konsekvensvurdering *K = 3*	Hendelsen kan oppleves som tap av integritet ved at kunden oppgir opplysninger om seg selv som vedkommende ellers ikke ville gitt fra seg eller som vedkommende ikke forstår hensikten med å gi fra seg.
Sannsynlighetsvurdering *S = 3*	Sannsynligheten for denne hendelsen er vurdert som høy, begrunnet med at sikkerhetsbrudd kan skje ved uaktsomhet hos egne ansatte, eksempelvis kobling av ulike registre.

Hendelse 4 (utlevering) *Risikonivå: 2 x 2 = 4*	Databehandler formidler eller selger innhentede personopplysninger til parter utenfor de lokasjonsbaserte tjenestene, som ønsker å benytte slike opplysninger til produktutvikling eller markedsføring av egne produkter eller tjenester, for eksempel reklame.
Årsak og evt. utløsende person(er)	[1] Databehandler selger deler av eller hele kunderegisteret til firma som tilbyr ulike tjenester. [2] Svikt i rutiner mht utlevering av personopplysninger til myndigheter. [3] Svikt i rutiner mht utlevering av personopplysninger til kunde.
Konsekvensvurdering *K = 2*	Hendelsen kan oppleves som krenkende og et brudd på tilliten mellom trafikant og databehandler. Dersom hendelsen omfatter mange kunder og bruken oppfattes som meget krenkende kan konsekvensen kategoriseres som K = 3.
Sannsynlighetsvurdering *S = 2*	Sannsynligheten for denne hendelsen er vurdert som moderat. Motivasjonen for å få tilgang til informasjonen kan være stor hos utenforstående aktører. Samtidig vil hendelsen ha vesentlig betydning for omdømme til den databehandler (tjenesteyter) som er årsak til hendelsen.

Hendelse 5 (utlevering) *Risikonivå: 2 x 2 = 4*	Databehandler bruker innhentede personopplysninger til annen databehandling enn det som framgår av formål, avtaler og databehandlers sikkerhetspolicy.
Årsak og evt. utløsende person(er)	[1] Databehandler utarbeider typiske kundeprofiler, reisemønstre og avanserte statistikker for bruk i salg og planlegging. [2] Databehandler har manglende bevissthet i forhold til data som innhentes fra kunde/trafikant.
Konsekvensvurdering *K = 2*	Hendelsen kan oppleves som krenkende og et brudd på tilliten mellom trafikant og databehandler. Dersom hendelsen omfatter mange kunder og bruken oppfattes som meget krenkende kan konsekvensen kategoriseres som K = 3.
Sannsynlighetsvurdering *S = 2*	Sannsynligheten for denne hendelsen er vurdert som moderat. Motivasjonen kan være stor, samtidig som videre analyse av data krever tid og ressurser.

Endring av personopplysninger – brudd på integritet

Integritet innebærer at personopplysningene skal beskyttes mot uønskede og ikke-autoriserte endringer.

Hendelse 6 (endring) *Risikonivå: 2 x 1 = 2*	Lagret informasjon om posisjon, sted eller identitet blir endret. Dette kan ha betydning for omdømme eller for spørsmål om skyld.
Årsak og evt. utløsende person(er)	[1] Programtekniske feil i systemet for lokasjonsbaserte tjenester [2] Feil utført av databehandler ved evt. manuell databehandling. [3] En utenforstående skaffer seg tilgang til databehandlers sentralsystem pga for dårlige sikkerhetsrutiner og adgangskontroll (hacking) og endrer data, eksempelvis identitet eller posisjonsdata for en eller flere personer.
Konsekvensvurdering *K = 2*	Hendelsen kan være krenkende.
Sannsynlighetsvurdering *S = 1*	Slike endringer krever normalt spisskompetanse og gode muligheter. I noen tilfeller kan det være vanskelig å oppdage evt. databehandlerfeil eller programtekniske feil, slik at feilen kan vedvare over tid.

Personopplysningene er utilgjengelige for behandling

Tilgjengelighet innebærer at personopplysningene skal være relevante, tilstrekkelige og tilgjengelig for autorisert behandling.

Hendelse 7 (utilgjengelighet) *Risikonivå: 2 x 2 = 4*	En kunde går glipp av en eller flere tjenester fordi vedkommendes posisjon ikke blir registrert på korrekt måte.
Årsak og evt. utløsende person(er)	[1] Manglende registrering av posisjon pga teknisk feil, dårlige rutiner eller svikt i rutiner. [2] Identiteten blir ikke registrert som følge av teknisk feil, databehandlerfeil, dårlige rutiner eller svikt i rutiner.
Konsekvensvurdering *K = 2*	For de fleste anvendelser er konsekvensene moderate ved manglende tilgang til lokasjonsbaserte tjenester. Mer alvorlige konsekvenser kan oppstå når lokasjonsbaserte tjenester benyttes til å overvåke personer som ikke kan passe på seg selv (navigasjonstjenester for fotgjengere, informasjonstjenester for kollektivtrafikanter), eller dersom bilførere stoler på informasjonen i for stor grad, f.eks fra intelligente fartstilpassere (K = 3).
Sannsynlighetsvurdering *S = 2*	Sannsynligheten for tekniske feil eller mangelfulle rutiner regnes som moderat.

Hendelse 8 (utilgjengelighet)	En kunde blir utsatt for økonomisk tap fordi vedkommendes posisjon ikke blir registrert på korrekt måte.
Risikonivå: 2 x 2 = 4	
Årsak og evt. utløsende person(er)	[1] Teknisk feil eller manglende oppdatering av sentralsystemet på grunn av dårlige rutiner eller svikt i rutiner.
Konsekvensvurdering K = 2	Hendelsen kan medføre økonomisk tap, men dette vil være av begrenset karakter.
Sannsynlighetsvurdering S = 2	Sannsynligheten for tekniske feil eller mangelfulle rutiner regnes som moderat, dvs. feil vil bli rettet relativt raskt.

Hendelse 9 (utilgjengelighet)	En kunde blir utsatt for økonomisk tap fordi data (f.eks. knyttet til avregning) ikke er tilgjengelig for kundens kontroll.
Risikonivå: 2 x 2 = 4	
Årsak og evt. utløsende person(er)	[1] Manglende oppdatering i sentralsystemet pga. svikt i rutiner, dårlige rutiner eller teknisk feil. [2] Brukerterskelen er for høy. [3] Kunden er ikke kjent med muligheten.
Konsekvensvurdering K = 2	Hendelsen kan medføre økonomisk tap.
Sannsynlighetsvurdering S = 2	Sannsynligheten vurderes som moderat, knyttet til alle tre årsaker.

Hendelse 10 (utilgjengelighet) *Risikonivå: 2 x 2 = 4*	En kunde får ikke vite hvilke personrelaterte data som lagres i systemet for lokasjonsbaserte tjenester.
Årsak og evt. utløsende person(er)	[1] Kunden kjenner ikke sine rettigheter [2] Databehandler kjenner ikke den registrertes rettigheter [3] Data er ikke tilgjengelig på en slik form at de er egnet for utlevering til den registrerte. [4] Dataene som etterspørres kan ikke knyttes til identifiserbar person eller kjøretøy (anonyme data).
Konsekvensvurdering *K = 2*	Hendelsen kan oppleves som krenkende i og med at dette er en rettighet som kunden har iht. Personopplysningsloven.
Sannsynlighetsvurdering *S = 2*	Bevisstheten rundt den registrertes rettigheter vil variere mye mellom ulike virksomheter og anvendelsesområder. Sannsynligheten vurderes som moderat ut fra 1) at den registrerte ikke kjenner sine rettigheter, 2) at databehandler ikke kjenner den registrertes rettigheter eller at dataene ikke er på en slik form at de egner seg for utlevering. Dataene som etterspørres kan også være anonyme; dvs. at de ikke kan knyttes til identifiserbar person.

Vedlegg 4: Risikovurdering ved intelligent fartstilpasningssystem med lagring av data

I dette vedlegget presenterer vi vurderingen av konsekvens og sannsynlighet for hver av de identifiserte uønskede hendelsene for behandling av personopplysninger for intelligente fartstilpasningssystem, når disse innebærer lagring av data (se kap. 3.5).

Skalaen for konsekvens (1-4) og for sannsynlighet (1-4) er presentert i kapittel 3. Vi viser først en oppsummerende tabell og deretter vurderingen av årsaker og evt. medvirkende personer, konsekvens, sannsynlighet og resulterende risikonivå for hver hendelse.

Tabell v4: ISA: Oversikt over identifiserte hendelser, vurdert konsekvens og sannsynlighet

	Hendelse	Vurdert konsekvens	Vurdert sannsynlighet	Resulterende risikonivå
Utlevering				
1	Informasjon utlevert til uvedkommende	3	3	**9**
2	Informasjon ikke slettet så snart som mulig	3	3	**9**
3	Det innhentes flere opplysninger enn nødvendig	3	3	**9**
4	Informasjon formidles til andre aktører	3	3	**9**
5	Informasjon benyttes til andre formål	2	2	**4**
Endring				
6	Registrerte opplysninger blir endret	2	1	**2**
Utilgjengelighet				
7	Data (tjeneste) er ikke tilgjengelig for kunden	3	1	**3**
8	Data er ikke tilgjengelig for behandling	2	2	**4**
9	Data er ikke tilgjengelig for kundens kontroll	3	2	**6**
10	Trafikanten kjenner ikke hvilke data som er registrert	2	2	**4**

Utlevering av personopplysninger – brudd på konfidensialitet

Konfidensialitet innebærer at informasjonen ikke skal være tilgjengelig for uvedkommende.

Hendelse 1 (utlevering) *Risikonivå: 3 x 3 = 9*	Informasjon om posisjon, fartsnivå, overholdelse av fartsgrenser og kjørestil til en identifiserbar trafikant blir utlevert til noen som ikke skal ha tilgang til slik informasjon. Trafikantens integritet kan eller vil svekkes.
Årsak og evt. utløsende person(er)	[1] En utenforstående skaffer seg tilgang til databehandlers pc, mobiltelefon eller sentralsystem pga for dårlige sikkerhetsrutiner og adgangskontroll (hacking, evt. fysisk tilgang), kopierer data og bringer disse videre eller bruker de selv. [2] En ansatt får tilgang til data vedkommende ikke burde ha tilgang til, pga dårlige sikkerhetsrutiner og adgangskontroll, og bringer disse videre eller bruker de selv. [3] En ansatt som har tilgang til informasjon knyttet til en trafikant, bryter taushetserklæringen og bringer data videre eller bruker de selv. [4] Data om reiser (posisjon og tid) blir utlevert/sendt til en utenforstående pga feil i sentralsystemet eller databehandlerfeil. [5] En utenforstående får tilgang til registrerte posisjoner og kan sjekke personens identitet eller eier av kjøretøy.
Konsekvensvurdering *K = 3*	Dette kan oppleves som særlig krenkende og som tillitsbrudd i forhold til tjenesteyter. Opplysningene er potensielt interessante for publisering eller andre måter som påvirker den registrertes omdømme. Det er også alvorlig å avsløre posisjon dersom personen trenger særlig beskyttelse.
Sannsynlighetsvurdering *S = 3*	Mest sårbar for manglende skjerming er data som oppbevares privat (vil da gjelde et lite antall registrerte). Det kan være forskjellig bevissthet rundt behovet for å skjerme slike data. Sannsynlighetsnivå S = 3 er knyttet til sikkerhetsbrudd ved uaktsomhet hos egne medarbeidere eller at utenforstående aktivt går inn for å bryte sikkerhetstiltak.

Hendelse 2 (utlevering) *Risikonivå: 3 x 3 = 9*	Data om posisjon, kjørestil, fartsnivå osv. blir ikke slettet så snart som mulig.
Årsak og evt. utløsende person(er)	[1] Programtekniske feil i sporingsprogrammet [2] Svikt i rutiner og/eller dårlige rutiner [3] Databehandler har manglende bevissthet i forhold til lagring av data, evt. lagring med forsett.
Konsekvensvurdering *K = 3*	Dette kan oppleves som særlig krenkende og som tillitsbrudd i forhold til tjenesteyter. Dersom hendelsen gjelder svært mange trafikanter eller personer som trenger særlig beskyttelse, kan den evt. kategoriseres som en hendelse med konsekvens K = 3.
Sannsynlighetsvurdering *S = 3*	Høy sannsynlighet. For de fleste anvendelser vil lagring av data medføre ekstra arbeid og ressursbruk, men for noen anvendelser vil det være aktuelt å lagre data for å bygge opp en førerprofil, f.eks. for forsikring og evt. i yrkessammenheng.

Hendelse 3 (utlevering) *Risikonivå: 3 x 3 = 9*	Databehandler innhenter personopplysninger som ikke er nødvendige for de lokasjonsbaserte tjenestene.
Årsak og evt. utløsende person(er)	[1] Databehandler bygger opp registre med data som gjør det mulig å danne typiske kundeprofiler, reisemønstre og avanserte statistikker for bruk i planlegging. [2] Databehandler har manglende bevissthet i forhold til data som innhentes fra kunde/trafikant.
Konsekvensvurdering *K = 3*	Hendelsen kan oppleves som tap av integritet ved at kunden oppgir opplysninger om seg selv som vedkommende ellers ikke ville gitt fra seg eller som vedkommende ikke forstår hensikten med å gi fra seg.
Sannsynlighetsvurdering *S = 3*	Sannsynligheten for denne hendelsen er vurdert som høy, begrunnet med at sikkerhetsbrudd kan skje ved uaktsomhet hos egne ansatte, eksempelvis kobling av ulike registre.

Hendelse 4 (utlevering) *Risikonivå: 3 x 3 = 9*	Databehandler formidler eller selger innhentede personopplysninger til eksterne parter.
Årsak og evt. utløsende person(er)	[1] Databehandler selger deler av eller hele registeret til eksterne firma. [2] Svikt i rutiner mht utlevering av personopplysninger til myndigheter. [3] Svikt i rutiner mht utlevering av personopplysninger til kunde.
Konsekvensvurdering *K = 3*	Hendelsen kan oppleves som svært krenkende og et brudd på tilliten mellom trafikant og databehandler. Dersom hendelsen omfatter mange kunder eller utsatte kunder og bruken oppfattes som meget krenkende kan konsekvensen kategoriseres som K = 3.
Sannsynlighetsvurdering *S = 3*	Sannsynligheten for denne hendelsen er vurdert som høy. Motivasjonen for å få tilgang til informasjonen kan være stor hos utenforstående aktører.

Hendelse 5 (utlevering) *Risikonivå: 2 x 2 = 4*	Databehandler bruker innhentede personopplysninger til annen databehandling enn det som framgår av formål, avtaler og databehandlers sikkerhetspolicy.
Årsak og evt. utløsende person(er)	[1] Databehandler utarbeider typiske kundeprofiler, reisemønstre og avanserte statistikker for bruk i salg og planlegging. [2] Databehandler har manglende bevissthet i forhold til data som innhentes fra kunde/trafikant.
Konsekvensvurdering *K = 2*	Hendelsen kan oppleves som krenkende og et brudd på tilliten mellom trafikant og databehandler. Dersom hendelsen omfatter mange kunder og bruken oppfattes som meget krenkende kan konsekvensen kategoriseres som K = 3.
Sannsynlighetsvurdering *S = 2*	Sannsynligheten for denne hendelsen er vurdert som moderat. Motivasjonen kan være stor, samtidig som videre analyse av data krever tid og ressurser.

Endring av personopplysninger – brudd på integritet

Integritet innebærer at personopplysningene skal beskyttes mot uønskede og ikke-autoriserte endringer.

Hendelse 6 (endring) *Risikonivå: 3 x 1 = 2*	Lagret informasjon blir endret. Dette kan ha betydning for omdømme eller for spørsmål om skyld.
Årsak og evt. utløsende person(er)	[1] Programtekniske feil i systemet [2] Feil utført av databehandler ved evt. manuell databehandling. [3] En utenforstående skaffer seg tilgang til databehandlers sentralsystem pga for dårlige sikkerhetsrutiner og adgangskontroll (hacking) og endrer data, eksempelvis identitet eller posisjonsdata for en eller flere personer.
Konsekvensvurdering *K = 3*	Hendelsen kan være svært krenkende og det kan være vanskelig for trafikanten å bevies at opplysningene ikke stemmer.
Sannsynlighetsvurdering *S = 1*	Slike endringer krever normalt spisskompetanse og gode muligheter (evt. S = 2). Samtidig kan det være vanskelig å oppdage evt. databehandlerfeil eller programtekniske feil, slik at feilen kan vedvare over tid.

Personopplysningene er utilgjengelige for behandling

Tilgjengelighet innebærer at personopplysningene skal være relevante, tilstrekkelige og tilgjengelig for autorisert behandling.

Hendelse 7 (utilgjengelighet) *Risikonivå:3 x 2 = 6*	En kunde går glipp av en eller flere tjenester fordi data ikke blir registrert på korrekt måte.
Årsak og evt. utløsende person(er)	[1] Manglende registrering av posisjon pga teknisk feil, dårlige rutiner eller svikt i rutiner. [2] Identiteten blir ikke registrert som følge av teknisk feil, databehandlerfeil, dårlige rutiner eller svikt i rutiner.
Konsekvensvurdering *K = 3*	For de fleste anvendelser er konsekvensene moderate ved manglende tilgang til lokasjonsbaserte tjenester. I noen tilfeller kan det oppstå farlige situasjoner dersom bilfører stoler i for stor grad på fartsgrenseinformasjonen som blir presentert.
Sannsynlighetsvurdering *S = 1*	Sannsynligheten for tekniske feil eller mangelfulle rutiner regnes som liten til moderat.

Hendelse 8 (utilgjengelighet)	En kunde blir utsatt for fare eller ulemper fordi vedkommendes data ikke blir registrert på korrekt måte.
Risikonivå: 2 x 2 = 4	
Årsak og evt. utløsende person(er)	[1] Teknisk feil eller manglende oppdatering av sentralsystemet på grunn av dårlige rutiner eller svikt i rutiner.
Konsekvensvurdering K = 2	Hendelsen kan evt. medføre ulemper, kontakt med byråkrati etc., men dette vil være av begrenset karakter.
Sannsynlighetsvurdering S = 2	Sannsynligheten for tekniske feil eller mangelfulle rutiner regnes som moderat, dvs. feil vil bli rettet relativt raskt.

Hendelse 9 (utilgjengelighet)	Opplysningene er ikke tilgjengelige for trafikantens kontroll.
Risikonivå: 3 x 2 = 6	
Årsak og evt. utløsende person(er)	[1] Manglende oppdatering i sentralsystemet pga. svikt i rutiner, dårlige rutiner eller teknisk feil. [2] Terskelen for brukerkontroll er for høy, eksempelvis pga. manglende tilgang til internett eller fordi dataene er vanskelig forståelig for kunden. [3] Kunden kjenner ikke til muligheten.
Konsekvensvurdering K = 3	Hendelsen kan medføre økonomisk tap.
Sannsynlighetsvurdering S = 2	Sannsynligheten for tekniske feil eller mangelfulle rutiner regnes som moderat, dvs. feil vil bli rettet relativt raskt.

Hendelse 10 (utilgjengelighet) *Risikonivå: 2 x 2 = 4*	En kunde får ikke vite hvilke personrelaterte data som lagres i systemet for lokasjonsbaserte tjenester.
Årsak og evt. utløsende person(er)	[1] Kunden kjenner ikke sine rettigheter [2] Databehandler kjenner ikke den registrertes rettigheter [3] Data er ikke tilgjengelig på en slik form at de er egnet for utlevering til den registrerte. [4] Dataene som etterspørres kan ikke knyttes til identifiserbar person eller kjøretøy (anonyme data).
Konsekvensvurdering *K = 2*	Hendelsen kan oppleves som krenkende i og med at dette er en rettighet som kunden har iht. Personopplysningsloven.
Sannsynlighetsvurdering *S = 2*	Bevisstheten rundt den registrertes rettigheter vil variere mye mellom ulike virksomheter og anvendelsesområder. Sannsynligheten vurderes som moderat ut fra 1) at den registrerte ikke kjenner sine rettigheter, 2) at databehandler ikke kjenner den registrertes rettigheter eller at dataene ikke er på en slik form at de egner seg for utlevering. Dataene som etterspørres kan også være anonyme; dvs. at de ikke kan knyttes til identifiserbar person.

Trondheim
Adress: P.O. Box 4760 Sluppen, 7465 Trondheim, Norway
Phone +47 73 59 30 30

Oslo
Adress: P.O. Box 124 Blindern, 0314 Oslo, Norway
Phone: +47 22 06 73 00

www.sintef.com