Regulatoriske rammer, databeskyttelse og personvern

Vedlegg til KVU 4-2 Databeskyttelse og personvern

Innholdsfortegnelse

1. Innledning 3
2. Retten til privatliv og sporfri ferdsel 3
3. Personopplysningsloven og EUs personvernforordning 3
   3.1 Om forordningen 3
   3.2 Grunnleggende personvernprinsipper 4
   3.3 Behandlingsgrunnlag 4
   3.4 Rettigheter for de registrerte 5
   3.5 Innebygd personvern 6
   3.6 Informasjonssikkerhet 8
4. Elementer av særlig betydning for konseptvalgutredningen 8
   4.1 Hvilke opplysninger er nødvendig – behovet 8
   4.2 Roller og grensesnitt – hvem er ansvarlig? 9
   4.3 Datakvalitet – grunnlag for forvaltning og metoder for innsamling 9
   4.4 Formålsbegrensning og viderebehandling 9
   4.5 Dataminimering 10
   4.6 Lagring og sletting av data 11
   4.7 Sikkerheten i løsningen 12
   4.8 Hvem skal kunne påberope seg rettigheter etter regelverket? 12
   4.9 Et rettferdig og forutsigbart system 13
5. Personvernkonsekvenser 13
6. Sikkerhetsrelaterte betraktninger 14
   6.1 Aktualitet 14
   6.2 Sikkerhetsloven og beskyttelsesinstruksen 15
7. Andre føringer 15
   7.1 Datatilsynets strategi for samferdselssektoren 15
   7.2 Presiseringer i EETS-direktivet 16
8. Sammenfattende – anbefalinger 17
Appendiks A: Endringslogg 18
Appendiks B: Distribusjonsliste 18
Appendiks C: Viktige referanser 18

1. Innledning

Et nytt system for veibruksavgift og bompenger for alle kjøretøy utløser noen prinsipielle, juridiske og systemtekniske spørsmål knyttet til personvern og informasjonssikkerhet.

Formålet i denne delutredningen er å redegjøre for relevante rammer som personvernregelverket oppstiller, og samtidig gi noen føringer for hvordan disse best kan ivaretas ved utforming av systemet og den tekniske løsningen.

Delutredningen må leses i sammenheng med redegjørelse av øvrige regulatorisk rammeverk som underlag til KVU kap 4.

2. Retten til privatliv og sporfri ferdsel

Enhver skal sikres sin rett til privatliv og vern om sin integritet. Fra dette kan det avledes en rett til å kunne ferdes fritt og ikke være gjenstand for unødig myndighetsovervåkning. Slike rettigheter står sterkt i enhver rettstat og demokratisk samfunn. Retten til privatliv er imidlertid ikke absolutt, og må ofte vektes mot andre viktige samfunnsinteresser.

Dersom myndighetsovervåkningen kan oppfattes som overdreven, uforholdsmessig eller på annen måte krenkende, så vil dette kunne medføre flere uønskede og utilsiktede konsekvenser som for eksempel sviktende tillitt, nedkjølingseffekt, forsøk på unndragelser/juks, økt risiko for (myndighets)misbruk, etc.

Retten til privatliv er forankret i norsk rett gjennom både grunnloven § 102 og i Den Europeiske Menneskerettighetskonvensjon (EMK) art. 8. Et tiltak som utgjør et inngrep i denne retten må følgelig ha tilstrekkelig lovhjemmel, forfølge et legitimt formål og må være forholdsmessig. Dette utgangspunktet legger sentrale føringer for den rettslige reguleringen av et nytt system for veibruksavgift og bompenger.

Det eksisterer også en rett til bevegelsesfrihet innenfor riket som er regulert i grunnloven § 106 og EMK prototokoll 4 art. 2.

3. Personopplysningsloven og EUs personvernforordning

3.1 Om forordningen

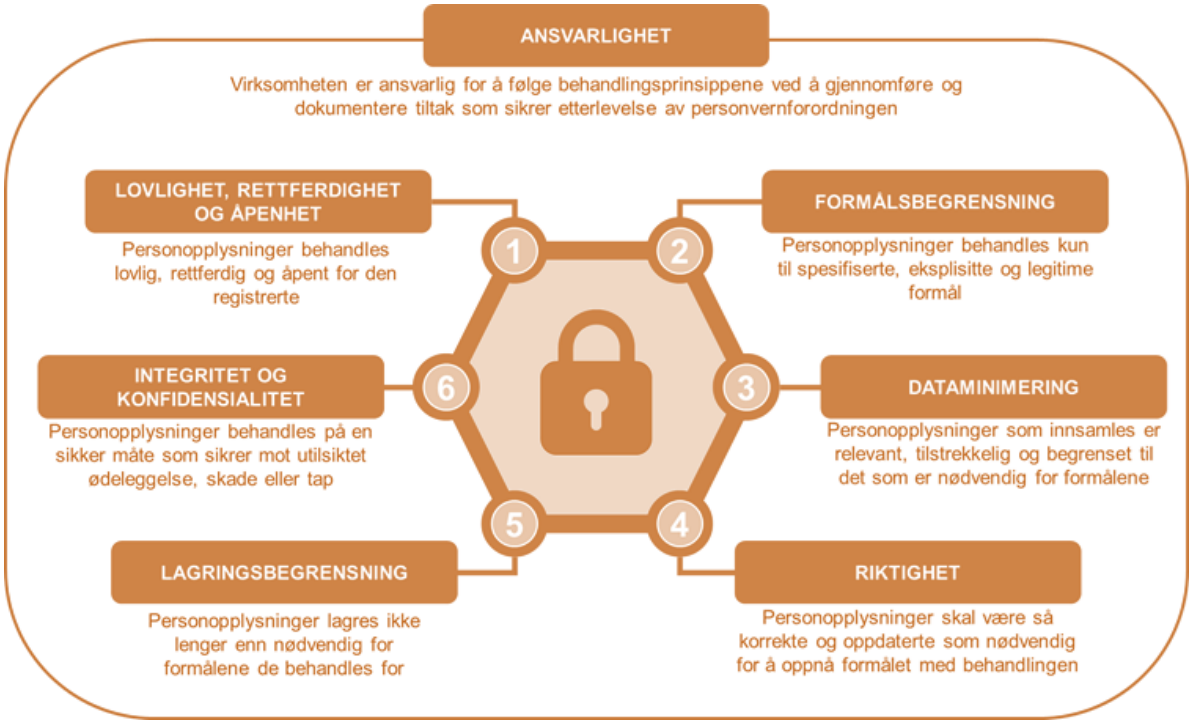
Lov om behandling av personopplysninger ble vedtatt 15. juni 2018 og trådte i kraft 20. juli 2018. Fra samme tidspunkt ble EU-direktiv 95/46, personverndirektivet, og personopplysningsloven fra 2000, opphevet.

Den nye loven gjennomfører EUs personvernforordning (GDPR) i Norge og gjør personvernforordningen til norsk rett ved inkorporasjon, slik dette er foreskrevet i EØS-avtalens artikkel 7 bokstav a. I tillegg supplerer loven forordningen på områder der forordningen overlater til landene å fastsette nasjonale regler. Personopplysningsloven og GDPR har betydning for innføring av et nytt system for veibruksavgift og bompenger, ettersom systemet vil rette seg mot enkeltpersoner og behandle personopplysninger.

For øvrig oppstiller personvernforordningen flere plikter som påhviler den virksomhet som behandler personopplysninger til ulike formål (behandlingsansvarlig). Eksempler på dette er krav om rettslig grunnlag for alle behandlinger av personopplysninger, krav om åpenhet og transparens, krav til informasjonssikkerhet og risikovurdering, samt krav til innebygd personvern. I tillegg knesetter forordningen ett sett med grunnleggende rettigheter som skal gjelde for de personene som det behandles personopplysninger om (de registrerte). Noen av de mest sentrale er retten til informasjon og innsyn i behandlinger, retten til å bli glemt (sletting), rett til å protestere, samt en rett til å ikke være gjenstand for helautomatiserte avgjørelser.

3.2 Grunnleggende personvernprinsipper

Personvernforordningen art. 5 lister opp grunnleggende personvernprinsipper den behandlingsansvarlige må påse at overholdes. Prinsippene er som følger:



Figur 1

Personvernprinsippene kommer til anvendelse ved alle behandlinger av personopplysninger. En gjennomgang av hvordan de ulike prinsippene vil kunne påvirke utformingen av et nytt konsept for veibruksavgift og bompenger er behandlet under pkt. 4.

3.3 Behandlingsgrunnlag

All behandling av personopplysninger må ha et rettslig behandlingsgrunnlag. Behandlingsgrunnlaget har til hensikt å legitimere den aktuelle bruken av personopplysninger som en behandlingsansvarlig virksomhet eller offentlig myndighet utfører. I personvernforordningen er de aktuelle behandlingsgrunnlagene listet opp i artikkel 6 nr. 1.

For behandlinger som gjelder fastsetting og innkreving av avgifter eller bompenger, så vil de mest aktuelle behandlingsgrunnlagene være at behandling av personopplysninger er nødvendig for å:

- oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige (artikkel 6 nr. 1 bokstav c), eller
- utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt (artikkel 6 nr. 1 bokstav e)

Begge disse alternative behandlingsgrunnlagene fordrer et supplerende rettsgrunnlag i nasjonal rett, hvor behandlingens formål og den aktuelle forpliktelsen, oppgave eller myndighet kan utledes. Kravet til tydelighet i det supplerende rettsgrunnlaget skjerpes i tråd med inngrepet i retten til privatliv, jf. redegjørelsen i pkt. 4.2 over. Det vil også kunne være behov for å fastsette egnede tiltak i lov, for å verne den registrertes rettigheter, friheter og berettigede interesser.

Bruk av samtykke (art. 6 nr. 1 bokstav a) vil ikke være et godt egnet grunnlag for myndighetenes innsamling og bruk av kjøretøydata for å fastsette og innkreve avgift og bompenger. Grunnen til dette er

det skjeve styrkeforholdet mellom partene, og personvernforordningens krav til frivillighet vil presumtivt ikke være oppfylt i en slik situasjon.[1]

En ny løsning for veibruksavgift og bompenger som baserer seg på posisjon og/eller distanse vil nødvendigvis innebære et element av overvåkning av kjøretøy, i større eller mindre grad. En slik behandling bør hjemles i lov, der rettsgrunnlaget er tilstrekkelig spesifisert og presist slik at det kan utledes hvilke data som samles inn, hvilke(t) formål opplysningene skal brukes til, hvem som har tilgang til disse, eventuell adgang/begrensning til viderebehandling, deling, og lagringsbetingelser – altså behandlingens ytre rammer. Et eventuelt krav eller plikt til å utstyre kjøretøy med teknisk utstyr bør også fremgå av rettsgrunnlaget.

Vurdering om hvorvidt det kan utledes et dekkende og tilstrekkelig behandlingsgrunnlag for valgt konsept ut fra gjeldende rett faller utenfor vurderingstemaet for denne konseptutredningen. Rettsgrunnlaget for et tiltak må imidlertid vektes mot graden av inngrep tiltaket medfører i privatlivet til borgerne, ref. pkt. 2. Således kan valg og vekting av ulike konsepter for veibruksavgift og bompenger påvirkes av hvorvidt de antas utgjøre et uforholdsmessig inngrep overfor bilistene eller ikke. Et konsept som presumtivt utgjør et uforholdsmessig inngrep vil vanskelig la seg realisere fra et rettslig perspektiv.

3.4 Rettigheter for de registrerte

De registrerte har flere rettigheter overfor den behandlingsansvarlige virksomheten. Det betyr at de registrerte kan kreve oppfyllelse av sine rettigheter og at det er virksomheten sin plikt å påse at rettighetene etterkommes. Rettighetene er i all hovedsak forankret i personvernforordningen art. 12-22.

Et nytt konsept for veibruksavgift og bompenger må utformes og designes på en slik måte at disse rettighetene ivaretas på en god måte, og at de er lette å håndheve.

For det første har de registrerte rett til informasjon om behandlingen. Dette henger sammen med virksomhetene sin plikt til å behandle personopplysninger på en åpen måte. For at den registrerte skal få oppfylt sin rett, må informasjonen gjøres forståelig. Det stilles derfor krav til hvordan virksomheter kommuniserer med enkeltpersoner. En virksomhet kan kommunisere med enkeltpersoner på mange måter – for eksempel gjennom personvernerklæringer, når brukerne/kundene skal ivareta rettighetene sine eller når det skal informeres om avvik. Virksomheten må da kommunisere på en kortfattet, åpen, forståelig og lett tilgjengelig måte.

Deretter har de registrerte rett til innsyn i egne opplysninger. Innsynsretten går mer konkret ut på at de registrerte har de rett på å vite hvilke opplysninger som er lagret, hvilket formål de benyttes til, om opplysningene utleveres til andre og i så fall til hvem, hvor lenge opplysningene lagres eller eventuelt hva som avgjør hvor lenge de lagres, hvor er opplysningene hentet fra og om virksomheten foretar automatiserte individuelle avgjørelser og i så fall hvilken logikk som ligger bak og hvilke følger det kan få for den registrerte.

Videre finnes en rett til sletting, altså en “rett til å bli glemt”. De mest relevante tilfellene vil her være når det ikke lenger er nødvendig å beholde opplysningene, fordi formålet med dem er oppnådd, og eventuelt hvis virksomheten har en lovpålagt sletteplikt. Unntak fra denne retten kan gjøres gjeldende av virksomheten bla. hvis det foreligger bokføringsplikt, arkivplikt eller der lagring er nødvendig for å fastsette, gjøre gjeldende eller forsvare rettskrav.

De registrerte har også rett på retting. Dersom det oppdages at virksomheten behandler personopplysninger som er uriktige, kan den registrerte kreve retting, eventuelt supplering dersom retting ikke er praktisk mulig eller gir et uriktig inntrykk. Virksomheten skal utføre retting uten ugrunnet opphold og normalt senest innen én måned. Virksomheten har også normalt en plikt til å si fra til eventuelle mottakere om rettingen.

[1] Se også fortalen til personvernforordningen pkt. 43

Rett til begrensning innebærer at den registrerte i noen tilfeller kan be om at måten virksomheten bruker personopplysningene på begrenses. I så fall kan personopplysningene lagres, men ikke brukes til noe. Retten til begrensing kan benyttes dersom den registrerte mener opplysningene som er lagret er uriktige. Mens den behandlingsansvarlige kontrollerer opplysningene, kan behandlingen begrenses i en periode. Retten kan også benyttes dersom den registrerte har benyttet sin rett til å protestere og virksomheten holder på å avgjøre om innsigelsen skal tas til følge.

De registrere har i enkelte tilfeller rett til å protestere mot en behandling av personopplysninger, for eksempel der grunnlaget er utøvelse av offentlig myndighet. Vilkåret er at det må foreligge grunner knyttet til vedkommendes særlige situasjon. Den behandlingsansvarlige skal i slike tilfeller ikke lenger behandle personopplysningene, med mindre vedkommende kan påvise at det foreligger tvingende berettigede grunner for behandlingen som går foran den registrertes interesser, rettigheter og friheter, eller for å fastsette, gjøre gjeldende eller forsvare rettskrav.

Dernest kommer retten til dataportabilitet. Det går ut på at den registrerte kan få utlevert personopplysninger om seg selv og gjenbruke dem som vedkommende vil på tvers av ulike systemer og tjenester. Rettigheten er til for at den registrerte enkelt skal kunne ta med deg opplysningene sine til den leverandøren som tilbyr de beste vilkårene. En lovpålagt behandling av personopplysninger som avgiftsgrunnlag vil ikke bli påvirket av denne retten.

Til sist kommer den registrertes rett ved helautomatiserte avgjørelser. Hovedregelen i personvernsforordningen (GDPR) art. 22 er forbud mot avgjørelser som er både helautomatiserte og har rettsvirkning for den registrerte. Ved helautomatisert menes her en avgjørelse der et dataprogram tar avgjørelsen uten at et menneske har innvirkning på den. Det finnes unntak fra forbudet, hvor det mest aktuelle er der det finnes en lovhjemmel for å ta automatiserte individuelle avgjørelser, og der den aktuelle loven sikrer rettighetene og interessene til den registrerte på en fullgod måte.

I en ny løsning for veibruksavgift og bompenger er det ikke usannsynlig at helautomatiserte beslutninger vil kunne innarbeides som en del av systemet. Eksempelvis kan en automatisert fastsetting bidra til at mennesker ikke får eller behøver tilgang til geolokaliserende kjøretøydata, og bidra til likebehandling i beregning av avgiften/bompenger. Det er viktig at løsningen tar opp i seg de begrensninger og pålegg som følger av personvernforordningen art. 22, og sikrer brukerne en transparent og trygg løsning.

3.5 Innebygd personvern

Løsningen må utformes og innrettes etter kravene om innebygd personvern, jf. personvernforordningen art. 25. Kjernen bak dette prinsippet er at man skal tenke personvern helt fra start (konseptfasen) til slutt (forvaltning) når det utvikles nye løsninger.

I en ny løsning for veibruksavgift og bompenger er det ikke usannsynlig at ett av konseptene eksempelvis vil medføre registrering av kjøretøyets bevegelser både med GNSS og veikantutstyr, og at det etableres tre ulike datastrømmer for å benytte innsamlede data til innkreving, kontroll og klagebehandling/innsyn for bruker. Det er i alle tilfeller den helhetlige løsningen som skal utformes med innebygget personvern.

Innebygd personvern er et sentralt krav i personopplysningsloven og betyr at det tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning. Dette skal sørge for at informasjonssystemene oppfyller personvernprinsippene, og at de ivaretar de registrertes rettigheter. Datatilsynet har samlet veiledning om innebygd personvern og viser på sine hjemmesider til syv steg til innebygd personvern[2]:

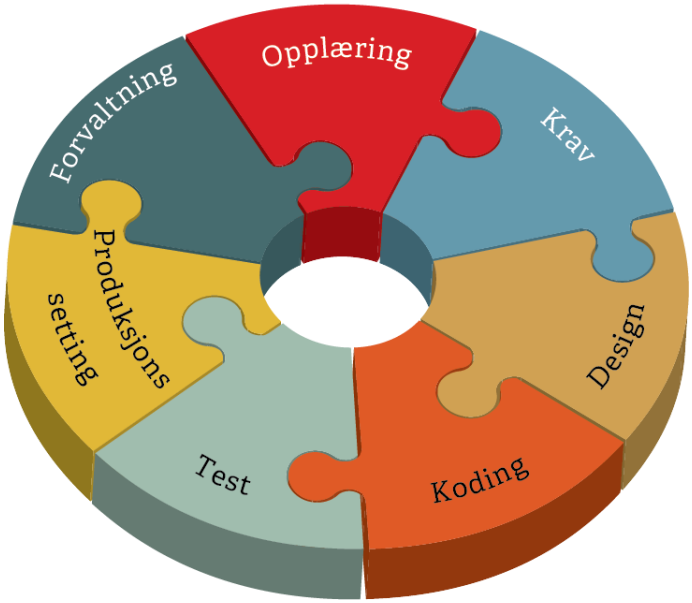
Steg	Kommentar
Steg 1: **Vær i forkant, forebygg fremfor å reparere**	For å lage en personvernvennlig løsning, er det viktig å vurdere risikoene for personvernet så tidlig som mulig i utviklingsprosessen. Kostnadene ved å rette feil og mangler ved et ferdig system kan være høye. Dersom du tar hensyn til personvernet tidlig i utviklingen, kan du unngå unødvendige

[2] Informasjonselementene i tabellen er hentet fra Datatilsynets hjemmesider, Innbygd personvern | Datatilsynet

	krenkelser av personvernet. Eksempler på krenkelse av personvernet er manglende tilgangsstyring, at det samles inn flere personopplysninger enn nødvendig, og manglende sletting av personopplysninger.
Steg 2: **Gjør personvern til standardinnstilling**	Standardinnstillinger er førende for hvordan et system blir brukt, og hvordan personopplysninger blir lagret. For at et system skal ha innebygd personvern, må standardinnstillingene settes opp slik at ikke flere personopplysninger enn nødvendig samles inn eller vises, at det finnes et lovlig formål med innsamlingen, at det er satt tekniske begrensninger for bruken av opplysningene, at opplysningene slettes når formålet er oppnådd, og at man bare får tilgang til å se hvilke opplysninger som er registrert på seg selv. Et slikt system vil automatisk styre brukeren til en arbeidsmåte som gir bedre personvern.
Steg 3: **Bygg personvern inn i designet**	Personvern skal være innebygd i IT-systemets design og arkitektur, samt i forretningspraksisen. Det bør ikke være en funksjon lagt til i etterkant. Dermed blir personvernet en viktig del av kjernefunksjonaliteten. Det vil si at personvern er en integrert del av systemet uten at det går på bekostning av funksjonaliteten.
Steg 4: **Skap full funksjonalitet**	Gjennom innebygd personvern ivaretar virksomheten både brukerens personvern, og sine egne behov. Det er viktig å ta hensyn til personvernet fra start for å unngå reparasjoner som går utover funksjonaliteten til løsningen. Noen ganger er det ikke mulig å gjøre endringer i etterkant uten at systemet blir dårligere. Målet er en både-og-tilnærming fremfor en enten-eller, for å ivareta virksomhetens behov og interesser, og samtidig ta hensyn til de registrertes personvern.
Steg 5: **Ivareta informasjonssikkerheten fra start til slutt**	Informasjonssikkerhet **må** være del av løsningen. Det betyr at alt som skjer i systemet på forhånd er risikovurdert og hensiktsmessig sikret, helt fra før personopplysningene samles inn, mens de behandles, og til de er slettet. Personopplysningene skal sikres mot uautorisert tilgang, endring, ødeleggelse og spredning.
Steg 6: **Vis åpenhet**	Det skal være åpenhet om hvordan systemet fungerer, og hvordan personvernet blir ivaretatt. Virksomheten skal sørge for at brukerne får god informasjon og at det legges til rette for innsyn i egne opplysninger. Det skal være mulig å kontrollere at systemet ivaretar personvernet slik leverandøren oppgir.
Steg 7: **Respekter brukerens personvern**	Fremfor alt krever innebygd personvern at utviklerne, bestillerne og administratorene gir brukerens personvern høy prioritet. Dette vil si å sørge for at personvernet ivaretas gjennom standardinnstillinger, tydelige brukervilkår, og løsninger for at brukeren skal kunne kontrollere opplysningene sine selv.

Datatilsynet har også utarbeidet en egen veileder for programvareutvikling med innebygd personvern[3], se Figur 2**Feil! Fant ikke referansekilden.**.

[3] Programvareutvikling med innebygd personvern | Datatilsynet



Figur 2

3.6 Informasjonssikkerhet

Personopplysninger skal sikres på tilfredsstillende måte, der opplysningenes konfidensialitet og integritet ivaretas. Dette kommer til uttrykk flere steder i personvernforordningen, mest relevant er art. 5 nr. 1 bokstav f, art. 24 og art. 32.

Sikkerhetsnivået skal fastslås ved bruk av risikobasert tilnærming, der alle aspektene av behandlingen tas med i vurderingen. Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

I ny løsning for veibruksavgift og bompenger er sikkerhet i løsningen helt sentralt, både for brukernes tillitt til systemet, men også for å hindre uønskede eller utilsiktede hendelser. Sikkerhetsnivået må vurderes i samsvar med det løsningsalternativet som velges. Kravene til sikkerhet i løsningen kommenteres nærmere under pkt. 4.7.

4. Elementer av særlig betydning for konseptvalgutredningen

4.1 Hvilke opplysninger er nødvendig – behovet

For å kunne ta stilling til de reelle personvernkonsekvensene, så er det avgjørende å ha et klart forhold til hva slags personopplysninger som skal behandles i en aktuell løsning eller system.

Helt uavhengig av hvilken teknisk løsning som velges, så må databehovet for valgt konsept avklares i en tidlig fase. Databehovet, herunder hvordan data skal prosesseres og flyte gjennom hele verdikjeden, setter grunnlaget for den øvrige utformingen av løsningen. Dersom et konsept kan realiseres uten bruk av identifiserende opplysninger, så vil også personvernulempene være minimale. På en annen side vil innsamling av sanntids posisjonsdata og bevegelsesmønster, knyttet til både kjøretøy og eier, utgjøre en mer inngripende behandling som vil kreve betydelige risikoreduserende tiltak for å kunne realisere.

For eksempel kan en løsning slå ut mer inngripende hvis avgifter og bompenger skal differensieres over mange takstgrupper og mange ulike takster. Presumtivt vil det da kunne fordre tilgang til mer detaljerte kjøredata for å kunne fastsette og dokumentere betalingskrav.

Prinsippet om dataminimering skal ivaretas ved at det kun er personopplysninger som er egnet, relevante og begrenset til det som er nødvendig for å gjennomføre formålet, se pkt.4.5.

Behovsvurderingen må dessuten gjøres uten hensyn til løsninger for lagring eller tilganger. Selve innsamlingen anses å skje som en del av løsningen selv om posisjonsdata kun lagres lokalt, eller slettes umiddelbart.

Dersom løsningen tar sikte på å bruke anonyme data, så må det kvalitetssikres at anonymitet er reelt. For at opplysningene skal regnes som anonymiserte, er det krav om at re-identifisering av opplysningene er umulig. I dagens teknologisamfunn er det lav terskel før noe anses som personopplysninger, ettersom det finnes mange lett tilgjengelige verktøy for å knytte av-identifiserte data til fysiske personer. Posisjonsdata er et vanlig eksempel på slike data, der enheten som måler posisjoner ikke behøver å være knyttet til en person eller kjøretøy, men bevegelsesmønsteret (posisjonsdataene) vil likevel ganske lett kunne avsløre hvem de gjelder.[4]

I den utstrekning konseptet vil benytte eller utlede særlige kategorier av personopplysninger som omfattes av personvernforordningens art. 9, må dette fremgå tydelig da behandling av denne type opplysninger er vurdert som mer inngripende. Eksempler er opplysninger om rasemessig eller etnisk opprinnelse, helseopplysninger, eller biometriske kjennetegn.

4.2 Roller og grensesnitt – hvem er ansvarlig?

Nytt system for veibruksavgift og bompenger vil sannsynligvis realiseres på en måte som fordrer et tett samarbeid mellom offentlige myndigheter og ulike private aktører.

Valgt konsept må kunne definere rollene, ansvaret og grensesnittene mellom de involverte aktørene. Dette er en nødvendig forutsetning for en effektiv forvaltning av ny løsning, men også for å avklare hvilke aktører som bærer behandlingsansvaret etter personvernregelverket. Videre kan man identifisere behovet for eventuelle avtaler om felles behandlingsansvar eller databehandleravtaler.

4.3 Datakvalitet – grunnlag for forvaltning og metoder for innsamling

Dataene som skal samles inn, må være av en slik kvalitet av de egner seg for formålet de skal brukes til. Kravene til datakvalitet må vurderes særskilt, men ofte vil det være vurderinger om hvilke minimumskrav det stilles til dataenes riktighet, fullstendighet og integritet.

Datakvalitet vil få betydning både i relasjon til selve metoden for innsamling (datafangst), men også i relasjon til de senere leddene i behandlingen (fastsetting, innkreving og kontroll). Dette betyr at det eksempelvis på forhånd må avklares hvorvidt f.eks. utstedere, operatører, Skatteetaten eller Statens Vegvesen vil ha behov for tilgang til enkelte grunnlagsdata fra kjøretøyet for å kunne oppnå en rettferdig og effektiv forvaltning og kontroll med løsningen. Dersom det er tilfelle, så utelukker det i praksis en løsning der alle data kun registreres, bearbeides og aggregeres lokalt i kjøretøyet, før det sendes ut til innkrever og slettes uten adgang for innsyn i eller kontroll av kjøredata.

Videre må løsningen for informasjonsfangst, eksempelvis en OBU med GNSS mottaker, være tilstrekkelig egnet og sikret mot uriktige registreringer, tekniske feil, juks, jamming, mv. Det må også legges til rette for å kunne foreta en etterrettelig kontroll med at enhet faktisk finnes i kjøretøy og fungerer som tilsiktet. Brukerne må ha tillitt til at løsningen sikrer riktig avgiftsbetaling og motvirker forskjellsbehandling og manipulering.

4.4 Formålsbegrensning og viderebehandling

Det stilles krav om at behandlingen av personopplysningene må være for uttrykkelig fastsatte og

[4] Se eksempelvis NRK-saken «Avslørt av mobilen» fra 9. mai 2020

spesifiserte formål. Viderebruk for uforenlige formål[5] er forbudt med mindre det foreligger samtykke eller hjemmel i lov som eksplisitt tillater viderebehandlingen. Det må derfor på forhånd klart og tydelig fastsettes for hvilke(t) formål personopplysningene skal behandles i konseptet som velges.

I et slikt konsept er det kanskje like viktig å hindre formålsutglidning ved at data som samles inn i løsningen ikke benyttes til andre formål enn veiprising, f.eks. straffeforfølgning, forsikring, erstatningssaker, forskning, analyse, etc. Det bør implementeres både rettslige rammer, samt organisatoriske og tekniske virkemidler, for å sikre at tilgjengelige data om kjøremønster, passeringer eller lignende, ikke benyttes videre på en måte som er utilsiktet eller uønsket. Dette gjelder både viderebehandling hos involverte parter, men også utlevering for viderebruk hos andre aktører.

Dersom konseptet skal legge til rette for integrering mot andre tjenester som benytter kjøretøyets posisjon eller kjøredata, så må dette være transparent for brukeren/føreren og helst være basert på samtykke. Et slikt samtykke må oppfylle kravene i personvernforordningen i art. 7, særlig med henblikk på frivillighet, informert og mulighet for å trekke tilbake.

4.5 Dataminimering

Prinsippet om dataminimering regnes som en av de aller viktigste rettssikkerhetsgarantiene i personvernretten. Dataminimering innebærer at den behandlingsansvarlige har en aktiv plikt til å begrense innsamlingen eller bruken av personopplysninger til det som er nødvendig og relevant for å oppnå formålene med den aktuelle behandlingen. Prinsippet relaterer seg til så vel opplysningenes kvalitet som kvantitet, og får anvendelse på alle stadier i en behandling av personopplysninger. Vurderinger om dataminimering kan således gi ulike utslag avhengig av sammenhengen der behandlingen skjer, f.eks. kan det innebære at:

- enkelte personopplysninger skal ikke samles inn i det hele tatt,
- noen personopplysninger, eller kategorier av personopplysninger, kan unntas fra et datagrunnlag i forbindelse med utlevering eller videreformidling
- personopplysninger skal slettes eller sperres når de ikke lenger er nødvendig for den behandlingen de brukes til (sammenlign også med prinsippet om lagringsbegrensing)
- tilgangen til opplysningene i et system begrenses til enkelte roller eller personer som har et tjenstlig behov for tilgang til opplysningene

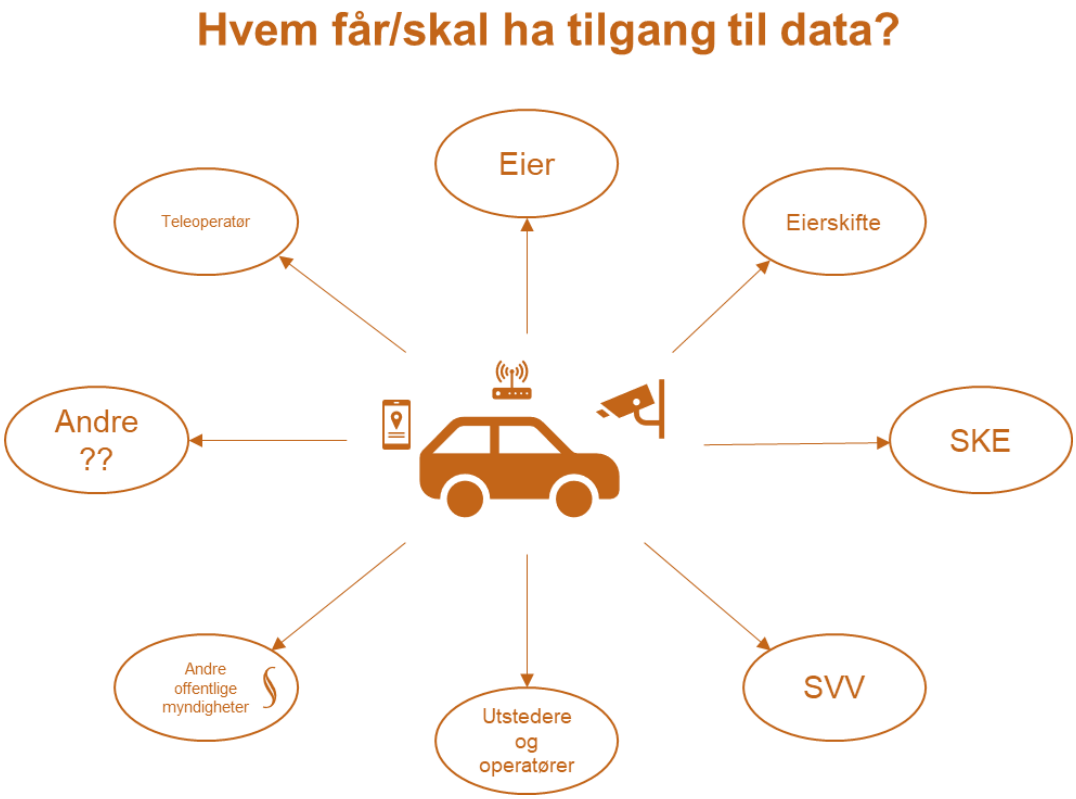
For løsningen som skal velges for nytt avgifts- og betalingssystem for bruk av vei er det sentralt å tenke dataminimering fra starten. Slik det er fremhevet under pkt. 4.1, så må det avklares hvilke opplysninger som er nødvendig å samle inn for å kunne realisere formålet – fortrinnsvis fastsettelse og innkreving av avgifter og bompenger for bruk av vei.

Videre blir det viktig å avklare hvilke aktører som må ha adgang til hvilke data, og i så fall i hvilke situasjoner. Her kan det tenkes mange ulike aktører eller interessenter (se **Feil! Fant ikke r eferansekilden.**), som på ulikt grunnlag kan ha interesse i innsamlede data. Ettersom geolokaliserende kjøredata regnes som veldig personlige opplysninger, er det en målsetning i et personvernperspektiv å redusere bruk og innsyn i disse til det som er legitime og strengt nødvendige formål.

---

[5] Personvernforordningen art. 6 nr. 4 fremhever at man ved forenlighetsvurderingen blant annet skal ta hensyn til følgende momenter ved behandlingen:
a) enhver forbindelse mellom formålene som personopplysningene er blitt samlet inn for, og formålene med den tiltenkte viderebehandlingen,
b) i hvilken sammenheng personopplysningene er blitt samlet inn, særlig med hensyn til forholdet mellom de registrerte og den behandlingsansvarlige,
c) personopplysningenes art, især om særlige kategorier av personopplysninger behandles, i henhold til artikkel 9, eller om personopplysninger om straffedommer og lovovertredelser behandles, i henhold til artikkel 10,
d) de mulige konsekvensene av den tiltenkte viderebehandlingen for de registrerte,
e) om det foreligger nødvendige garantier, som kan omfatte kryptering eller pseudonymisering

Det er grunn til å hevde at løsningens evne til å innfri prinsippet om dataminimering blir en sentral faktor for realiseringen. Datatilsynet har også fremholdt prinsippet om dataminimering som helt sentralt for å kunne lykkes med en løsning for veiprising, se pkt. 7.1.



Figur 3

4.6 Lagring og sletting av data

Den nye løsningen må kartlegge hvor lenge det er nødvendig å oppbevare data som samles gjennom kjøretøyet. Hovedregelen etter personvernforordningen er at personopplysninger ikke skal lagres lenger enn det som er nødvendig for å realisere formålet de er samlet inn for. Dette punktet henger tett sammen med prinsippene om lagringsbegrensning, dataminimering og innebygd personvern.

Lagringstiden for ulike data vil kunne påvirkes av flere faktorer ved den nye løsningen, eksempelvis vurderinger knyttet til forvaltning av det nye systemet og valg av teknisk løsning. Dette er også faktorer som er avhengig av hverandre; hvorvidt opplysninger om en bils kjøremønster kun skal registreres og lagres lokalt i kjøretøyet, sentralt i en database eller hos den enkelte innkrever vil også avhenge av hvem som skal/må ha tilgang til og befatning med de aktuelle dataene som samles inn.

Det vil være flere interessenter for tilgang til kjøredata, med mer eller mindre legitime behov, se **Feil! Fant i kke referansekilden.**. Flere ulike faktorer kan få betydning for oppbevaringstiden:

- Lovkrav
  - Gjeldende bompengepasseringer lagres og oppbevares i inntil 5 år basert på oppbevaringskrav for salg av tjenester (nytten av å bruke veien) i **bokføringsloven**. Datatilsynet mener dette er en praksis som ikke bør videreføres ved utforming av nye løsninger for eks. veiprising (se pkt. 7.1)
  - Arkiv- og dokumentasjonskrav
- Fakturering og innkreving
  - Er det hensyn som tilsier at kjøredata må oppbevares som grunnlag for korrekt fakturering og innkreving?

  - Dokumentasjonsbehov ved tvangsinnfordring og foreldelse?
- Forvaltning og kontroll
  - Kan en løsning forvaltes forsvarlig uten at grunnlagsdataene vil være tilgjengelige for kontroll eller etterprøvbarhet?
  - Klagerett og klageordning
  - Dokumentasjonskrav?
- Førerens/eierens innsyn og kontroll med løsningen
  - Førerens rettssikkerhetsgarantier

For en slik løsning for veibruksavgift og bompenger så er det i all hovedsak lagring og oppbevaring av data som er egnet til å kartlegge en persons kjøremønster som er viktig å redusere. Det understrekes likevel at hovedregelen i personvernforordningen gjelder alle personopplysninger, også de som oppleves mindre inngripende (kjennemerke, eierinformasjon, personalia, fakturert beløp mv.). Her vil imidlertid oppbevaringsbehovene være legitime og godt dokumentert gjennom virksomhetenes oppgaver.

Løsningens evne til å redusere oppbevaring og lagring av kjøredata vil kunne få betydelig virkning på realiseringen. Kan det utarbeides en løsning der opplysninger om kjøredata aggregeres og betales løpende slik at det ikke er behov for lagring av sporingsdata i eller utenfor kjøretøyet? Kan det sikres at evt. lagring kun skjer på kryptert ombordløsning der avtale-/kjøretøyeier alene kan ha befatning og kontroll med dataene, og selv bestemme hvor lenge de skal oppbevares ut fra egne behov? I motsatt fall må de legitime behovene for en videre bruk og oppbevaring av kjøredata kartlegges og redegjøres for.

4.7 Sikkerheten i løsningen

Sikkerheten for ny løsning må være robust, og ivaretatt fra start til slutt. Informasjonssikkerheten i løsningen skal blant annet ivareta opplysningenes konfidensialitet, integritet (korrekthet), og tilgjengelighet. Fra et personvernperspektiv så det særlig viktig å hindre utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til de registrerte personopplysningene.

Det må gjøres en risikovurdering for å identifisere trusler og sårbarheter, og tiltakene herfra må tas i betraktning ved utforming og design av ny løsning.

Løsningen må blant annet stille strenge krav til tilgangsstyring og kryptering, både ved lagring og under transport av data. Løsningen må utvikles på en slik måte at brukerne kan ha tillit til at opplysningene om deres bruk av kjøretøyet eller adferdsmønster ikke kan aksesseres eller misbrukes av uvedkommende. Et element her er at risikoen for utilsiktet spredning øker eksponentielt med hvor mange aktører som skal ha tilgang til informasjonen, ref. også punktene om dataminimering og lagringsbegrensning.

At opplysningene som innsamles og genereres i løsningen er korrekte er viktig både av hensyn til brukerens tillit til et slikt betalingssystem, men også for forvaltningen av løsningen. Løsningen må således ha mekanismer som effektivt hindrer ulovlig eller utilsiktet endring, manipulering eller sletting av datagrunnlaget. Ved datafangst må det også tas høyde for ulike metoder for juks, f.eks. jamming av GPS signaler, lokal utkobling av mottaker, utilsiktede feil, eller manipulering av grunnlagsdata som betalingssubjekt, kjørte strekninger, etc. Det vil også kunne være brukere som helt mangler registreringsenheter.

4.8 Hvem skal kunne påberope seg rettigheter etter regelverket?

Slik det er redegjort for under pkt. 3.4, så oppstiller personvernforordningen flere rettigheter for den/de registrerte. Rettighetene skal bidra til medbestemmelse og transparens og skal være lette å håndheve.

Et spørsmål som utmerker seg i relasjon til denne konseptutredningen er hvem som skal kunne utøve retten til innsyn, jf. personvernforordningen art. 15.

Det er flere subjekter/roller som kan være aktuelle for å utøve rettigheter i et nytt betalingssystem for bruk av vei. Både kjøretøyeier, avtale-/brikkeeier og fører av et kjøretøy kan ha interesser i å kunne få innsyn i personopplysninger som løsningen registrerer. Da blir det et spørsmål om hvordan disse rettighetene skal ivaretas (og evt. begrenses) i praksis, f.eks. ved eierskifte eller der fører eller brikkeeier er en annen enn

kjøretøyeier. Personvernforordningen gir en begrensing i retten til innsyn, der dette kan få en negativ innvirkning på andres rettigheter eller personvern, jf. art. 15 nr. 4.

Det er gode grunner for å hevde at eieren av et kjøretøy må kunne utøve rettigheter knyttet til det aktuelle kjøretøyet. Samtidig er det ikke uvanlig for familier å ha flere kjøretøy registrert på samme person, men at disse i praksis disponeres fullt ut av andre, f.eks. en ektefelle, samboer eller barn. Det samme kan hevdes overfor leiebil- eller leasingselskaper der eier av kjøretøyet er en virksomhet, men disponeres av privatpersoner som igjen kan ha en avtale med utsteder av brikke. At den registrerte eieren av et kjøretøy skal kunne få innsyn i kjøredata som andre har generert, kan virke negativt for privatlivet til den det gjelder.

Samtidig er eierrettigheter en viktig rettssikkerhetsgaranti for den som eier et formuesobjekt. Det er også nærliggende og forutsigbart for en som velger å låne eller disponere et kjøretøy de ikke eier, at vedkommende vil kunne foreta sjekk på hvor bilen befinner seg, enten ved å undersøke bomringpasseringer eller montert GPS i bilen. Det skal presumtivt mye til for at hensynet til en potensiell/hypotetisk tredjepart skal kunne tilsidesette eiers rettigheter over kjøretøyet. Dersom valgt konsept vil innebære montering av ekstern enhet med tilhørende abonnement/avtale, så kan det være nærliggende at avtaleeier vil være rettighetshaver til kjøredata fremfor en potensiell annen juridisk eier (f.eks. et leasingsselskap).

Det må gjøres en avveining av avtale- og/eller kjøretøyeierens legitimerte interesse i å kunne utøve rettigheter overfor sitt objekt, herunder gjøre seg kjent med registreringer om sitt kjøretøy, mot eventuelle andre hensyn, slik som personers rett til privatliv. Hvem som skal kunne utøve eller påberope seg rettigheter i nytt avgiftssystem for bruk av kjøretøy burde presumtivt avklares i det rettslige grunnlaget for løsningen, slik at man unngår tvil om dette i ettertid.

4.9 Et rettferdig og forutsigbart system

Forutsigbarhet og medbestemmelse er sentrale målsettinger etter personvernregelverket. Åpenhet omkring det offentliges virksomhet bidrar også til å ivareta borgernes rettssikkerhet, og motvirker vilkårlighet og myndighetsmisbruk. Disse hensynene gjør seg spesielt gjeldende ved behandlinger som kan innebære elementer av overvåkning, kontroll og myndighetsinngrep.

Det finnes flere måter å realisere disse målsetningene på, eksempelvis ved å legge til rette for at samtykke, frivillighet og medbestemmelse kan integreres i de deler av løsningen der dette er aktuelt. Behandlingen i seg selv (fastsette og innkreve avgift og bompenger for bruk av veinettet) vil ikke baseres på samtykke som behandlingsgrunnlag, men samtykke for enkelte del-funksjoner eller eksterne integrasjoner (f.eks. betalingsløsninger eller forsikringsselskap) kan være gode virkemidler for å gi brukeren reell medbestemmelse og innsikt i behandlingen.

For å ivareta fysiske personers integritet og tillitt så må konseptet være forutsigbart, lett forståelig og rettferdig. Det rettslige grunnlaget for behandlingen bør være såpass spesifisert at de ytre rammene som datafangst, formål, virkemidler, tilgangsbegrensning, kontrolladgang, oppbevarings- og sletteplikter og den enkeltes rettigheter er lett forståelig.[6]

5. Personvernkonsekvenser

Både personvernforordningen (art. 35) og utredningsinstruksen[7] stiller krav til at personvernkonsekvenser av et aktuelt tiltak skal vurderes før behandlingen starter.

I personvernforordningen er det et vilkår for slik plikt at behandlingen vil medføre høy risiko for de registrertes rettigheter og friheter. Det blir derfor et spørsmål om ny løsning for veibruksavgift og

[6] Se også flere tiltak i anbefaling fra European Data Protection Board (EDPB) om nødvendige garantier ved overvåkningstiltak, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures | European Data Protection Board (europa.eu)
[7] Se Veileder til utredningsinstruksen: Vurdering av personvernkonsekvenser (pdf)

bompenger vil medføre en høy risiko for fysiske personers rettigheter og friheter. Dette må bero på en konkret vurdering må ut fra hvilke konsekvenser og trusler ny løsning vil ha for personvernet til de registrerte. Presumtivt vil en løsning som i stor skala innsamler og benytter data om fysiske personers kjøremønster med det formål å fastsette og innkreve avgifter og bompenger utgjøre en høy risiko.

Personvernhensyn tar sikte på å beskytte enkeltmenneskets personlige integritet og privatlivets fred. En avveining av personvernmessige konsekvenser mot andre interesser vil bidra til å skape tillit hos borgerne som kan gjøre iverksettingen av tiltaket eller beslutningen enklere, eventuelt etter justeringer for å ivareta personvernet på en bedre måte.

Aktuelle momenter i en vurdering av personvernkonsekvenser kan være:

- Posisjonsdata er svært personlige da de gir detaljerte beskrivelser av bevegelsesmønster
- Gjelder mange personer
- Myndighetsovervåkning – redusert/ingen selvbestemmelse
    - Uønsket nedkjølingseffekt
    - Risiko for juks eller manipulering av systemet
    - Redusert tillit til systemet og forvaltningsmyndighetene
- Fare for feil
    - Dårlig datakvalitet
- Risiko for misbruk
    - Formålsutglidning, «function creep»
    - Lekkasje og salg av posisjonsdata
    - Sosial manipulering
    - Utpressing?
- Krav til teknisk løsning
    - Innebygde mekanismer for å sikre personvern
    - Sikkerhet
- Åpenhetsbetraktninger
    - Fremstår løsningen som rimelig og forutsigbar?
    - Lett/utfordrende å håndheve rettigheter etter forordningen?
- Fordeler med løsningen
- Risikoreduserende tiltak som er identifisert
- Nøkkelfaktorer ved valg av system/løsning

Listen er ikke ment å være uttømmende.

6. Sikkerhetsrelaterte betraktninger

6.1 Aktualitet

Før realisering av valgt konsept må det utredes hvorvidt løsningen kan utgjøre en trussel mot rikets sikkerhet, eller mot andre beskyttelses- og skjermingsverdige interesser og personer.

Dersom løsningen eksempelvis vil innebære sporing av alle kjøretøy i Norge (både norske og utenlandskregistrerte), så bør det avklares hvorvidt sporing av kjøretøy tilhørende Forsvaret, PST, politikere, diplomater mv. kan medføre utilsiktede konsekvenser for sikkerheten. Det samme kan også hevdes om registrering av geolokaliserende informasjon om personer med særskilt beskyttelsesbehov og som av ulike årsaker bor på graderte adresser (kode 6 og 7).

Det bør vurderes om det kan implementeres unntaksløsninger, nye eller eksisterende, der sikkerhetsmessige betraktninger krever det.

6.2 Sikkerhetsloven og beskyttelsesinstruksen

Lov om nasjonal sikkerhet (sikkerhetsloven) med forskrifter regulerer det forebyggende sikkerhetsarbeidet knyttet til nasjonale sikkerhetsinteresser i Norge. Formål med bestemmelsene i sikkerhetsloven er å trygge Norges suverenitet, territoriell integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser. Sikkerhetsloven skal bidra til å forebygge, avdekke og motvirke sikkerhetstruende virksomhet, og sørge for at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.

Sikkerhetsloven stiller krav til sikring av skjermingsverdige verdier som informasjon, informasjonssystemer, og objekt- og infrastruktur. Disse kravene blir i sikkerhetsloven omtalt som «informasjonssikkerhet», «informasjonssystemsikkerhet» og «objekt- og infrastruktursikkerhet», og vil helt eller delvis inngå i en virksomhets helhetlige arbeid med informasjonssikkerhet.

Informasjon er skjermingsverdig etter sikkerhetsloven dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig. Skjermingsverdig informasjon kan være både gradert og ugradert, og informasjonen kan lagres og formidles på flere måter.

Beskyttelsesinstruksen brukes på materiale som ikke kan graderes etter sikkerhetsloven. Den brukes på informasjon som kan skade offentlige interesser, en bedrift, institusjon eller enkeltperson. Det er to grader i stigende rekkefølge:

- Fortrolig
- Strengt fortrolig

7. Andre føringer

7.1 Datatilsynets strategi for samferdselssektoren

Datatilsynet er engasjert i personvern og teknologisk utvikling innenfor samferdselssektoren. Tilsynet har blant annet etablert en egen strategi for et godt personvern i samferdselssektoren, der veiprising, tilkoblede kjøretøy og kollektivtransport er fremhevet som prioriterte områder. Målsettinger for sektoren som fremheves er:

- at den enkelte skal kunne bevege seg og foreta reiser uten at det blir foretatt unødvendige registreringer
- at aktørene i sektoren aktivt benytter teknologien til å ivareta personvernet fremfor å utfordre det
- at innebygd personvern og personvern som standardinnstilling kommer på plass i sektoren
- dataminimalisering der det er nødvendig å registrere data om ferdsel som kan knyttes til individer ut fra vektige samfunnsinteresser eller berettigede private eller kommersielle interesser
- åpenhet og informasjon om hvordan personopplysninger lagres ved ferdsel i samfunnet
- god og dokumentert informasjonssikkerhet i alle informasjonssystemer som registrerer data om ferdsel som kan knyttes til enkeltindivider

Angående veiprising mener Datatilsynet:

- at morgendagens løsninger for betaling for ferdsel langs vei bør innrettes slik at det samles inn minimalt med informasjon om kjøretøyets bevegelser. Dette kan gjøres enten ved tiltrodde betalingsløsninger hvor «kjøretøyet» betaler digitalt og uten registrering av personopplysninger fortløpende mens det kjører, eller ved hjelp av ombordløsninger hvor detaljinformasjon om ferdsel

aldri forlater kjøretøyet. Det er sektorens ansvar å komme frem til gode løsninger her, men Datatilsynet skal bidra til dette.
- at det ikke er grunnlag for å kreve bokføring av den enkelte bompassering. Dersom noen personopplysninger må lagres for bokføring, må disse lagres klart adskilt fra data som brukes til rutinemessig fakturering.
- at bruk av innsamlet data til annet enn veiprising må baseres på informert og frivillig samtykke

7.2 Presiseringer i EETS-direktivet

Europaparlamentets- og Rådsdirektiv (EU) 2019/520 av 19. mars 2019 om interoperabilitet mellom elektroniske bompengesystemer og tilrettelegging for utveksling av opplysninger mellom medlemslandene om manglende bompengebetaling i EU omtales gjerne som EETS-direktivet.

EETS-regelverket skal legge til rette for at elektroniske betalingssystemer på veg skal kunne kommunisere med hverandre (interoperabilitet). Regelverket bygger opp under en visjon om at trafikanten skal kunne kjøre gjennom betalingssystemer i hele Europa med én avtale, bompengebrikke og faktura, ved at innkrevingen håndteres av en utsteder som er godkjent som EETS-utsteder. Dette kalles en europeisk elektronisk betalingstjeneste (EETS: European Electronic Toll Service).

EETS-direktivet inneholder enkelte særskilte bestemmelser om innsamling og behandling av opplysninger og «Data protection» som skal gjelde innenfor direktivets virkeområde. Følgelig må også en ny løsning for veibruksavgift og bompenger ivareta disse kravene for den delen av løsningen som skal/må operere innenfor EETS-direktivet.

Bestemmelsene om behandling av personopplysninger i EETS-direktivet presiserer og henviser i stor grad videre til de generelle kravene som følger i EUs personvernforordning (GDPR), se eksempelvis direktivets art. 5 nr. 5 og nr. 10, art. 10 nr. 1, art. 14 nr. 2, og art. 27 nr. 1, 2 og 3. Likevel er det enkelte presiseringer som behandlingsansvarlig må ta særskilt hensyn til for behandlinger som omfattes av EETS-direktivet. Et utvalg av de mest relevante omtales punktvis under, men må gjennomgås nærmere ved utforming av en konkret løsning:

- Særskilt informasjonsplikt overfor kunde/bruker om behandlingen av personopplysninger ved tegning av EETS-avtale, jf. art. 10 nr. 1
- Begrensinger i viderebruk av eventuelle trafikkdata som EETS-utstedere pålegges å rapportere, jr. art. 14 nr. 2. Slike data skal heller ikke benyttes til å identifisere brukerne/kundene.
- Behandlingen av personopplysninger til formålene i direktivets art. 23, 24 og 25 skal begrenses til de som er angitt i Vedlegg 1, jf. art. 27 nr. 2 bokstav a
- Særskilt rett til innsyn i hvilke opplysninger som er utvekslet til annen stat ved betalingsmislighold, jf. art. 27 nr. 4

Videre presiserer art. 27 at medlemstatene må foreta nødvendig tiltak for å sikre at personopplysninger som behandles etter EETS-direktivet kun benyttes til følgende formål:

a) Å identifisere personer som mistenkes for å ha overtrådt sin plikt til å betale bompenger eller veibruksavgift innenfor rammene av art. 5 nr. 8
b) Å sikre bompengeselskapets etterlevelse av sine forpliktelser overfor skattemyndighetene innenfor rammene av art. 5 nr. 9
c) Å identifisere et kjøretøy, samt eier eller fører av kjøretøyet, der mislighold av betalingsforpliktelse er konstatert innenfor rammene av art. 23 og 24.

8. Sammenfatning – anbefalinger

Retten til privatliv er en grunnleggende menneskerettighet, forankret i Grunnloven og EMK. Når det gjøres inngrep i rettigheten for å oppnå et legitimt formål, må inngrepet være forholdsmessig. I dette ligger bla. at opplysningene som tenkes innhentet må være nødvendige og korrekte, samt minimaliseres så langt det lar seg gjøre for å oppnå det ønskede formålet.

Kravet til forholdsmessighet innebærer at man må ta stilling til om inngrepet er nødvendig, og at det ikke finnes mindre inngripende alternativ. Finnes flere alternativ skal det alternativet som er minst inngripende velges, forutsatt at dette alternativet oppnår formålet i tilstrekkelig grad.

Ved valg av ulike konsepter og innretninger for en ny veibruks-/veiprisingsavgift, bør man søke etter minst inngripende løsninger. I praksis vil det bety at kartlegging av et kjøremønster bør reduseres så langt det lar seg gjøre.

Kravet til presisjon i lovverket som regulerer avgiften, innebygde sikkerhetsmekanismer i den teknologiske løsningen, utforming av informasjons- og rettighetsgarantier mv. vil øke progressivt i takt med graden av inngrep i retten til privatliv.

I henhold til personvernforordningens art. 35 vil det presumptivt måtte gjennomføres en personvernkonsekvensvurdering (DPIA) av løsninger/konsept det ønskes å gå videre med.

Appendiks A: Endringslogg

Versjon	Dato	Endring	Produsert/endret av	Godkjent av
0.8	14.12.2021	Første utkast	Fredrik Bache	Prosjektleder
1.0	12.10.2022	Oppdatering før sluttleveranse	Ingrid Elvesæter	Prosjektleder Morten Tveit

Appendiks B: Distribusjonsliste

Versjon	Dato	Navn
0.8	14.12.2021	Styringsgruppe, Oppfølgingsforum FIN og SD
1.0	17.10.2022	Styringsgruppe SKE-SVV FIN og SD Ekstern Kvalitetssikrer

Appendiks C: Viktige referanser

Dokumentreferanser:	
Eksterne referanser:	