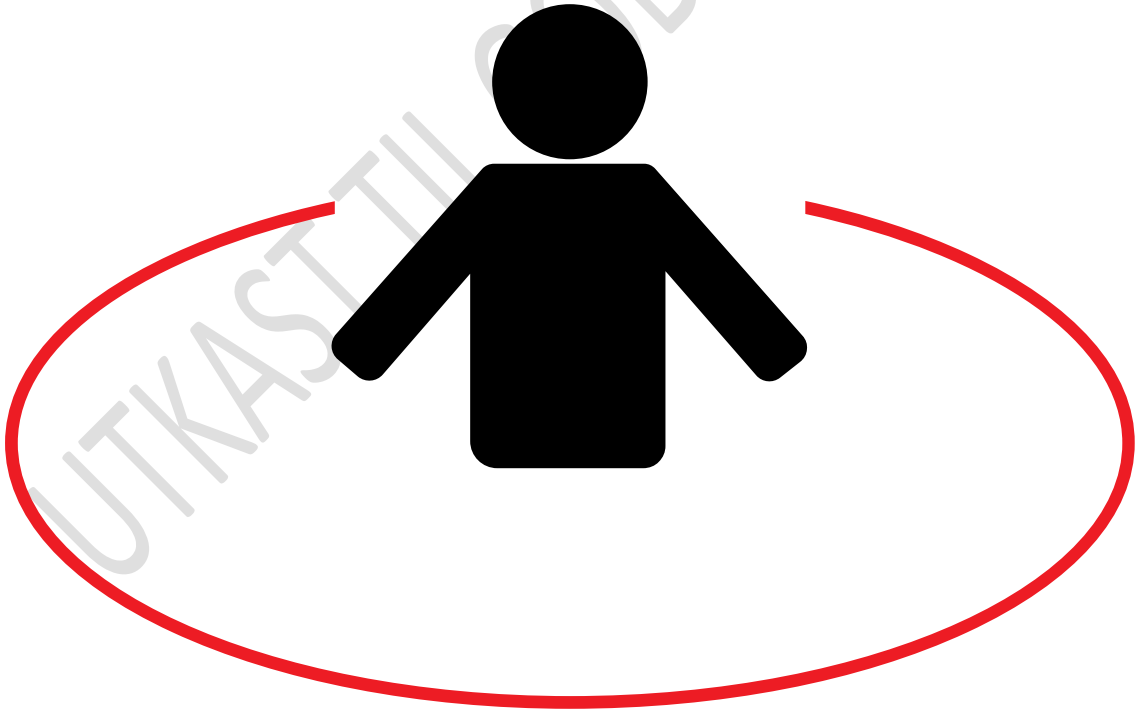
Jernbane-
direktoratet

Veileder
Håndbok V821 Del 5

Atferdsnorm

for personvern og informasjonssikkerhet i kollektivtransport



Dokument nr.: UTKAST FOR GODKJENNING
Dato: 01.02.2021

Forord

Atferdsnorm for personvern og informasjonssikkerhet i kollektivtransport er utarbeidet av representanter fra kollektivtransportsektoren og Jernbanedirektoratet. Normen er godkjent av Datatilsynet i vedtak av [sett inn]. Normen er både et frittstående dokument og en del av Håndbok V821 Elektronisk billettering. Den erstatter tidligere Bransjenorm for personvern i elektronisk billettering.

I denne versjonen er normen utvidet til å gjelde personvern for all kundehåndtering i kollektivtransport, ikke bare for billettering. Normen er oppdatert med hensyn på EUs personvernforordning (EU) 2016/679 (GDPR).

Jernbanedirektoratet, februar 2021

Prosjektnummer: 600002	Ansvarlig avdeling: Marked og Samfunn Faglig ansvar: Markedskunnskap
Versjon: Utkast til godkjenning	Forsidefoto/illustrasjon: Statens vegvesen/Trond Foss
ISBN: [xxxx]	

Innhold

1 Bakgrunn og formål

Kollektivtransportbransjen i Norge implementerer løsninger for reiseplanlegging, elektronisk billettering, passasjertellinger, reisemønsterkartlegging, informasjonstjenester og andre kunderettede tjenester. Implementering av sømløse løsninger for dette er en politisk målsetting. Relevante virksomheter har allerede innført mange løsninger, men er på forskjellig implementasjonsstadium. Det er en politisk målsetting at man skal kunne reise "sømløst" med elektronisk billett i Norge uavhengig av hvilke transportselskap som benyttes. Det innebærer blant annet at data fra en tjeneste brukes i neste tjeneste, f.eks. at en reiseplanlegger gir grunnlag for billettkjøp, at en elektronisk lagret billett kan gi enklere tilgang til sanntids- og avviksinformasjon for den aktuelle reisen osv. Samtidig bidrar ny teknologi som «big data» og kunstig intelligens til stadig nye muligheter.

Bruk av elektronisk billettering og andre tjenester i kollektivtransporten reiser en rekke personvernrettslige spørsmål som må løses i henhold til bestemmelsene i lov om behandling av personopplysninger av 15.5.2018 nr. 35 (pol) med tilhørende forskrifter. Personopplysningsloven bygger på EU-Forordning 2016/679 (GDPR), om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger.

For å etablere en felles forståelse av hvordan bestemmelsene skal tolkes i Norge, er denne atferdsnormen utarbeidet av sentrale aktører i bransjen, transportmyndigheter i fellesskap og med innspill fra Datatilsynet og deretter godkjent av Datatilsynet. Formålet er å sikre effektiv anvendelse av personvernregelverket og å skape forutsigbarhet for aktørene i tolkningen av regelverket, samt å skape et tillitvekkende og godt personvern for de reisende. Det er tatt spesielt hensyn til sårbare personvers personverninteresser i utformingen av atferdsnormens innhold. Kollektivtransportbransjen skal kunne utvikle gode tjenester for alle reisende, samtidig som man utarbeider verktøy for å ivareta personvern og god informasjonssikkerhet. Der tidligere versjoner av bransjenormen var begrenset til billettering vil denne versjonen også dekke de andre leddene i kundekjeden, som reiseplanlegging og reisemønsterkartlegging.

2 Forholdet mellom atferdsnormen og andre regler

Atferdsnormen er godkjent av Datatilsynets vedtak av [sett inn].

Denne atferdsnormen er en del av Jernbanedirektoratets Håndbok V821[1]. Alle Virksomheter som omfattes av yrkestransportloven eller jernbaneloven er forpliktet til å følge håndboken. Håndbok V821, tidligere HB 206 og V821, er forankret i yrkestransportforskriften og Forskrift om billettering ved jernbanetransport, samt rundskriv Samferdselsdepartementet og Jernbanedirektoratet. HB V821 inkluderer denne atferdsnormen, og atferdsnormen er således gjeldende for aktørene. Atferdsnormen er et uttrykk for hvordan Datatilsynet vil tolke til dels skjønnsmessige bestemmelser i regelverket.

Virksomheter som ikke er forpliktet til å følge HB V821 kan velge å tilslutte seg atferdsnormen, og gir skriftlig melding om dette til Jernbanedirektoratet. Dette kan f.eks. være reisebyråer. Oversikt over Virksomheter som velger å tilslutte seg normen vedlikeholdes av Jernbanedirektoratet.

Andre aktører som selger reiser der Personopplysninger tilknyttet reisen tilflyter Tjenesteyter eller Transportør, typisk noen reisebyråer, anses da som Formidler og skal følge atferdsnormen. Den som inngår slik avtale med andre aktører skal informere aktørene om atferdsnormen.

Normen angir grunnleggende prinsipper for håndtering av kundedata i kollektivtransport, men den er ikke uttømmende. Den enkelte Virksomhet er forpliktet til å påse at regelverket i øvrig overholdes og at det utarbeides lovpålagte internkontrollsystemer for å ivareta dette.

[1] Håndbok V821 er under revisjon, og vil etter revisjonen bli Håndbok N803.

3 Behandling av personopplysninger i kollektivtransport

Utformingen av elektroniske billetteringsløsninger bygger på HB V821 som er utarbeidet av Jernbanedirektoratet og aktører i bransjen.

Tradisjonelt har kollektivtransportsektoren håndtert kundedata i forbindelse med salg og billettering, men i nyere tid har også andre kunderettede tjenester blitt utviklet, som reiseplanleggere, tellesystemer, systemer for kartlegging av reisemønstre for å gi grunnlag for ruteplanlegging osv. I dag kobles disse forskjellige tjenestene stadig tettere sammen for å skape mer kundevennlige løsninger.

Reiseplanleggere tilbyr gjerne reisesøk dør-til-dør. Lagring av slik informasjon kan være sporbar, spesielt i områder med lav bosetting. Enkelte tellesystemer og systemer for reisemønsterkartlegging benytter kundens mobiltelefon som grunnlag for sporing, herunder både Bluetooth, trådløst nett og posisjonering i mobilnettet. Stadig flere virksomheter tilbyr også sine kunder online tjenester og brukerprofiler, og det vil i enkelte tilfeller være behov for oppfølging av kunden i etterkant, som ved avvikssituasjoner.

Elektroniske billettsystemer er ofte transaksjonsbasert hvor opplysninger samles inn for å ivareta visse formål med behandlingen. HB V821 bygger på ISO/DIS 24014-1, inkludert nyere utgaver som omfatter kontobasert billettering. En avtale om tilgang til en transporttjeneste kan være i forskjellige former, som billetter, forhåndsdefinert reiserett eller avtaler som gir fri adgang til transportmidler og krever registrering av reise for etterskuddsvis betaling. Moderne løsninger tilbyr mer fleksibilitet for både transportør og kunde, men resulterer gjerne i mer omfattende generering av data.

Avtalen mellom reisende og transportør må lagres, enten på papir, elektroniske reisekort, i kundens mobiltelefon eller i baksystemer. Andre billettbærere kan også være relevante. Rettigheter for den reisende ligger i en "kontrakt". Kontrakten verifiseres ved reise, noe som normalt generer en transaksjon som samler inn de reiseopplysningene som er beskrevet i Vedlegg 1. Noen av systemene er offline, og det skjer en asynkron overføring av data.

Ved håndtering av reisehjemler, både billetter og andre reiseavtaler, lagres informasjon elektronisk. Dette gjøres for å vedlikeholde informasjon om reisehjemmelens status og integritet, samt gjøre prisberegning, inntektssikring, avregning og feilsøking. Informasjonen som lagres inkluderer nødvendig informasjon for å identifisere reisehjemmel, tilknyttet identifikator og billettbærer. For feilsøking er det f.eks. for reisekort nødvendig å ta vare på kortnummer og kortets transaksjonsteller for å sikre at det ikke mangler transaksjoner. For avregning er det f.eks. nødvendig at alle transaksjoner for hver reisehjemmel inngår i beregningsgrunnlaget for å sikre at alle parter mottar riktig oppgjør. Dessuten vil avtalen være avgjørende for å kunne yte tilleggstjenester til kunden som for eksempel abonnement og rekonstruksjon.

Ikke all aktivitet medfører innsamling eller lagring av reiseopplysninger. Et eksempel vil være når kunden bare sjekker hvilket produkt vedkommende innehar, eller om et abonnement er gyldig.

Enkelte Virksomheter har etablert løsninger der den reisende kan benytte seg av et reiseprodukt utstedt av en samarbeidende Virksomhet. For å kunne gjennomføre et riktig oppgjør mellom Virksomhetene, er det nødvendig å behandle opplysninger om hvilke produkter som er benyttet hvor.

Ved slik avregning er det ikke nødvendig å identifisere hvem som har gjennomført reisen. Virksomhetene skal sikre at den som gjennomfører avregningen ikke får tilgang til opplysninger som gjør

det mulig å koble innehaver av et produkt med gjennomført reise. Dette skal løses ved at Virksomhetene ved avregningen kun utleverer Kortnummer/app-id el. Tilsvarende, samt tilhørende bruk, og at det blir inngått en Databehandleravtale med selskapet som gjennomfører avregningen.

Følgende grunnprinsipper gjelder for sektorens behandling av personopplysninger og aktørene skal kunne dokumentere at prinsippene overholdes:

- Aktørene skal iht GDPR sikre at personopplysningene behandles på en lovlig, rettferdig og gjennomsiktig måte slik at de reisende kan forstå hvordan deres personopplysninger blir behandlet.
- Personopplysningene skal bare samles inn for spesifikke, uttrykkelig angitte og berettigede formål og skal ikke viderebehandles på en måte som er uforenlig med disse formålene.
- Personopplysningene skal være adekvate, relevante og ikke strekke seg utover det som er nødvendig for formålene de behandles for, noe som også kalles prinsippet om «dataminimering».
- Personopplysningene skal være korrekte og oppdateres om nødvendig.
- Personopplysningene skal ikke lagres lenger enn det som er nødvendig for formålene som personopplysningene behandles for og visse lagringstider er nærmere spesifisert i denne atferdsnormen.
- Ved hjelp av tekniske og organisatoriske tiltak skal personopplysningene behandles med tilstrekkelig sikkerhet, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade.

Kap 5 angir en oversikt over rollene i sektoren.

4 Behandlingsgrunnlag og krav om anonyme alternativer

4.1 Utgangspunkt

Bruk av Personopplysninger i elektronisk billettering må ha et Behandlingsgrunnlag, hvor de mest praktiske er lov, avtale, samtykke eller berettiget interesse. Typiske personopplysninger er:

- Navn
- Bilde
- Adresse
- Postnummer/sted
- Adresse 2
- E-post
- Mobiltelefon
- Telefonnummer
- Fødselsdato
- Kjønn
- Kundenummer for registrerte kunder
- Kortnummer for registrerte kort
- Applikasjons-ID for registrerte kunder
- Alle ID-er for kontobasert billettering for registrerte kunder
- Opplysninger som registreres ved salg, validering eller kontroll, som kan knyttes til en kunde og/eller passasjer via en identifikator (som f.eks. kortnummer eller applikasjons-ID).

Listen er ikke uttømmende.

Dersom Betaler er en annen enn den som skal benytte reisehjemmelen, skal Betaler videreføre informasjon til den reisende om behandlingsgrunnlaget og tilhørende behandling av personopplysninger.[2]

4.1.1 Avtale

Avtalevilkårene skal være tydelige på om det vil skje behandling av Personopplysninger eller ikke og tilfredsstille kravene til åpenhet, se under i punkt 6.

Hvorvidt det er nødvendig å behandle Personopplysninger avhenger av hvilken tjeneste avtalen angår, se nærmere om anonyme alternativer under. En avtale kan kun omfatte Personopplysninger som er nødvendig for å gjennomføre Reiseretten.

Der Behandlingsgrunnlaget er avtale, skal omfanget av behandling av Personopplysninger være begrenset til det som er nødvendig for å levere reisetjenesten, herunder informasjon om avvikssituasjoner knyttet til den konkrete reisen. Tilleggstjenester som ikke er strengt nødvendige for reisen, skal baseres på samtykke, separat avtale eller annet relevant behandlingsgrunnlag.

4.1.2 Samtykke

Der behandlingsgrunnlaget er Samtykke, skal det være uttrykkelig, frivillig og informert. Med enkelte unntak anses frivilligheten først å være reell når det foreligger reelle anonyme alternativer til personlige

[2] For eksempel vil dette gjelde for arbeidsgivere som betaler for ansattes bruk av reisekort i arbeidstiden.

reiseprodukter, se mer om dette under. Samtykke kan typisk gis av Kunden på basis av den informasjon Virksomheten har gitt. Informasjonen om hvordan personopplysningene skal behandles skal gis innen samtykket gis.

Samtykke skal avgis til et spesifikt formål og skal ikke «bundles»/sammenblandes med andre formål. Eksempelvis kan ikke et samtykke til å få bedre kundeservice dersom man ønsker rekonstruksjon av mistet billett, blandes sammen med at man samtidig gir samtykke til behandling av personopplysninger i forbindelse med avviksmeldinger (utover det som er beskrevet i pkt 4.1.1, tredje ledd) – eller omvendt. Samtykke kan avgis muntlig, men av hensyn til etterprøvbarhet anbefales at det innhentes skriftlig eller ved avkryssing i elektronisk skjema el.

Samtykker har begrenset varighet. Behandlingsansvarlig skal derfor minimum kontakte den registrerte hvert tredje år for å gi vedkommende anledning til å fornye eller avslå videre samtykke.

4.1.3 Berettiget interesse

Der Behandlingsgrunnlaget er berettiget interesse, skal Virksomheten ha gjennomført og kunne dokumentere interesseavveiningen før behandlingen tar til. Det finnes sjekklister for hva en slik interesseavveining bør inneholde. Kundene skal gjøres oppmerksom på at dette er behandlingsgrunnlaget.

Det kan være at Virksomheten har behov for å bruke Kundens Personopplysninger (produksjonsdata) til bruk i test av ny eller forbedret programvare dersom det er uforholdsmessig vanskelig å oppnå formålet ved å bruke anonyme eller fiktive opplysninger. Slik test på produksjonsdata skal imidlertid skje på en kontrollert og forsvarlig måte, herunder med riktig tilgangskontroll og sletterutiner, og i henhold til øvrige krav i art 32. Det skal også foreligge en skriftlig interesseavveining som dokumenterer at Virksomheten har en berettiget interesse og at det ikke foreligger ulemper for Kundene.

4.1.4 Generelt om formålsbegrensning og om forenelige formål

Virksomheten kan ikke benytte Personopplysninger til andre formål enn det de opprinnelig ble samlet inn for, men kan likevel benytte Personopplysninger til nye formål som er forenelige med det opprinnelige formålet, jf art 6,4. Virksomheten skal ha gjennomført avveiningen før slik forenlig behandlingen tar til og gjort Kundene oppmerksom på dette før behandlingen påbegynnes.

4.1.5 Særlige behandlinger

4.1.5.1 Direkte markedsføring i og utenfor eksisterende kundeforhold

I henhold til markedsføringsloven § 15, tredje ledd, er det adgang til direkte markedsføring kun i eksisterende kundeforhold, dersom ikke Kunden på forhånd eller ved mottagelse av tilbud og informasjon reserverer seg mot dette. Kunden skal ved innsamling av personopplysninger og ved hver henvendelse gis en mulighet til enkelt å reservere seg. Den enkelte Virksomhet må ta stilling til om vilkåret for slik markedsføring er til stede, hensyntatt Tjenestens karakter og varighet. I andre tilfeller krever direkte markedsføring eksplisitt samtykke, jf. markedsføringslovens § 15, første ledd.

4.1.5.2 Bruk av personprofiler

For å kunne tilby Kunden tilpassede tilbud og informasjon i forhold til Kundens bruk, må Kunden avgi et eget samtykke til dette og kunden skal være orientert om hvilke behandlinger profileringen medfører.

Ved henvendelse til Kunden må det gjøres særskilt oppmerksom på hvilke opplysninger som ligger til grunn for henvendelsen og hvor de er hentet fra.

4.1.5.3 Billettkontroll – ivareta en berettiget interesse

Passasjer som ikke kan fremvise Gyldig billett, kan med hjemmel i yrkestransportloven § 33 og Virksomhetenes transportvedtekter/transportvilkår ilegges tilleggsavgift.

Virksomhetene anses å ha en berettiget interesse til å behandle Personopplysninger om Passasjer som ved kontroll ikke kan fremvise Gyldig billett. Formålet med Behandlingen er å sørge for en rettmessig og effektiv inndrivning av tilleggsavgiften.

4.1.5.4 Skoleskyss

Skoleskyss er en rettighet for skoleelever på vilkår som er omhandlet i opplæringsloven kapittel 7[3]. Den enkelte fylkeskommune delegerer i noen tilfelle myndighet til sitt administrasjonsselskap. Den som er behandlingsansvarlig er ansvarlig for at regelverket overholdes, herunder informasjon til eleven.

Formålet med Behandling av Personopplysningene er å utøve delegert offentlig myndighet og sørge for at elever tildeles skoleskyss på riktig grunnlag. For å oppnå sikker identifisering, er det nødvendig å benytte personnummer.

Spesialtransport innvilges til skolelever som av helsemessige årsaker er berettiget til skoleskyss.

Rettslig grunnlag for behandlingen er å ivareta viktige samfunnsinteresser og at det er fastsatt i lov at det er adgang til slik behandling, jf. GDPR art 9 nr.2 g).

4.1.5.5 Bruk av automatiserte beslutningsprosesser

Automatiserte beslutningsprosesser forutsetter at de er nødvendige for gjennomføring av en avtale eller at det foreligger samtykke eller hjemmel i lov.

4.1.5.6 Statistikk

Transportør og transportmyndigheter vil ha behov for å utarbeide statistikk over reisemønsteret for å kunne utarbeide best mulig kollektivtransport. Etter en konkret vurdering kan i mange tilfelle en slik behandling hjemles i artikkel 6 nr. 1, bokstav e og personopplysningsloven § 8. Dette forutsetter at nødvendig sikringstiltak, herunder slik angitt i artikkel 89. Et eksempel på en fremgangsmåte er angitt i punkt 8.4, fjerde ledd.

4.2 Anonyme alternativer

Det å bevege seg fritt i et demokratisk samfunn uten at bevegelsene registreres, anses for å være en viktig del av privatlivet, jf. den europeiske menneskerettskonvensjonen artikkel 8 nr. 1, FNs konvensjon om sivile og politiske rettigheter artikkel 17 og menneskerettsloven § 2.

Virksomhetene skal sikre at det for sentrale reiseprodukter finnes anonyme alternativer i tillegg til eventuelle personifiserte Billetter og tjenester. Med sentrale reiseprodukter menes f.eks. enkeltbillett og periodebillett. Kunden har en grunnleggende rett til å kunne bestemme over sine Personopplysninger og til å kunne velge å ferdes anonymt i samfunnet så langt det er mulig. For eksempel vil bruk av ferge med lovpålagt identifikasjon av reisende og bruk av visse personlige tilleggstjenester ikke kunne gjennomføres anonymt. Se for øvrig kap 8 for nye løsninger og ny teknologi.

[3] I høringsrunden for GDPR er det spilt inn til Justisdepartementet at lovhjemmelen for skoleskyss i Opplæringsloven bør klargjøres.

4.2.1 Konsekvens for behandling av personopplysninger

Under angis hvordan Virksomheten skal sikre at det finnes anonyme alternativer, slik at det anonyme alternativ utgjør et valgbart alternativ for den reisende. Et kort som ikke er registrert på innehavers navn hos Kortutsteder er tilstrekkelig anonymt.

Virksomheten skal veilede i hvordan man kan foreta en avlesning av Reisehjemmelen som ikke medfører innsamling eller lagring av Reiseopplysninger, eksempelvis når Kunden kun ønsker å sjekke innhold på et reisekort. Kunder som ønsker anonymitet skal ikke uforvarende kunne skrive inn identifiserende opplysninger som for eksempel navn, telefonnummer eller e-postadresse i faste tekstbokser ved kjøp eller administrasjon av Anonyme produkter.

E-postadresse kan benyttes som identifikator i anonyme løsninger, men Virksomheten skal da informere om at om anonymitet ikke er sikret dersom e-postadressen åpenbart angir navn eller annen klar identifikasjon. I anonyme løsninger skal Virksomheten ikke kreve mobiltelefonnummer som identifikator.

4.2.2 Pris

For like reiseprodukter som enkeltbillett, periodebillett o.l., skal det også tilbys tilsvarende Anonyme produkter som er like økonomisk fordelaktig for Kunden som den personifiserte Billett. Reiseprodukter som er basert på etterskuddsvis prisberegning skal også tilbys anonymt til en økonomisk like fordelaktig pris for kunden som tilsvarende personifisert produkt, og i disse tilfellene oppnås tilstrekkelig anonymitet ved bruk av tredjeparts betalingsløsninger.

Kravet om å tilby Anonyme alternativer som er like økonomisk fordelaktige gjelder ikke dersom produktet knyttes til tilleggstjenester der identifisering er nødvendig. Et eksempel på dette er hvis prisen på en periodebillett reduseres fordi den knyttes til avtale om bruk av bysykkel som fordrer identifisering.

Andre eksempler er dersom det i samband med tilleggstjenester tilbys rabatter, for eksempel poeng eller prisavslag for å ha syklet, gått og tatt kollektivtrafikk eller lignende fordelsprogrammer eller ved bedriftsavtaler hvor det inngås avtale om rabattordninger for ansatte eller medlemmer.

4.2.3 Salgskanaler

For produkter som skal kunne kjøpes anonymt skal de anonyme produktene kunne kjøpes gjennom salgskanaler med tilsvarende tilgjengelighet som personifiserte produkter.

Dersom man f.eks. tilbyr å kjøpe billetter på transportørens vanlige nettsider, så skal disse også kunne kjøpes anonymt der. Dersom transportøren tilbyr kjøp via mobil app skal også denne løsningen som hovedregel åpne for anonyme kjøp.

Alternativt kan transportøren tilby anonyme reiser på nettsider eller mobil app gjennom en tredjepart, f.eks. Entur. Dersom transportøren ønsker å bruke en tredjepart for å sikre sine anonyme alternativer, må transportøren tydelig opplyse om hvor alternative anonyme tjenester finnes og linke til disse, og dette skal skje innledningsvis i kundedialogen, før noen person- eller reiseopplysninger innhentes eller anmodes om å bli avgitt. Der linking ikke er mulig skal det som minimum refereres i tekst til hvor anonyme tjenester finnes.

Tilsvarende skal gjelde for nye salgskanaler.

4.2.4 Tilleggstjenester

Ved kjøp av personifiserte tilleggstjenester kan dette når det er nødvendig medføre at det ellers anonyme, tilhørende reiseproduktet blir identifiserbart.

En tilleggstjeneste kan også være særlig tilrettelagt transport eller bestillingstransport, så lenge det finnes et akseptabelt grunntilbud av transporttjenester og det uansett bygges inn personvern i løsningene slik at så få personopplysninger som mulig behandles for å gjennomføre tjenesten og slettes så raskt som mulig.

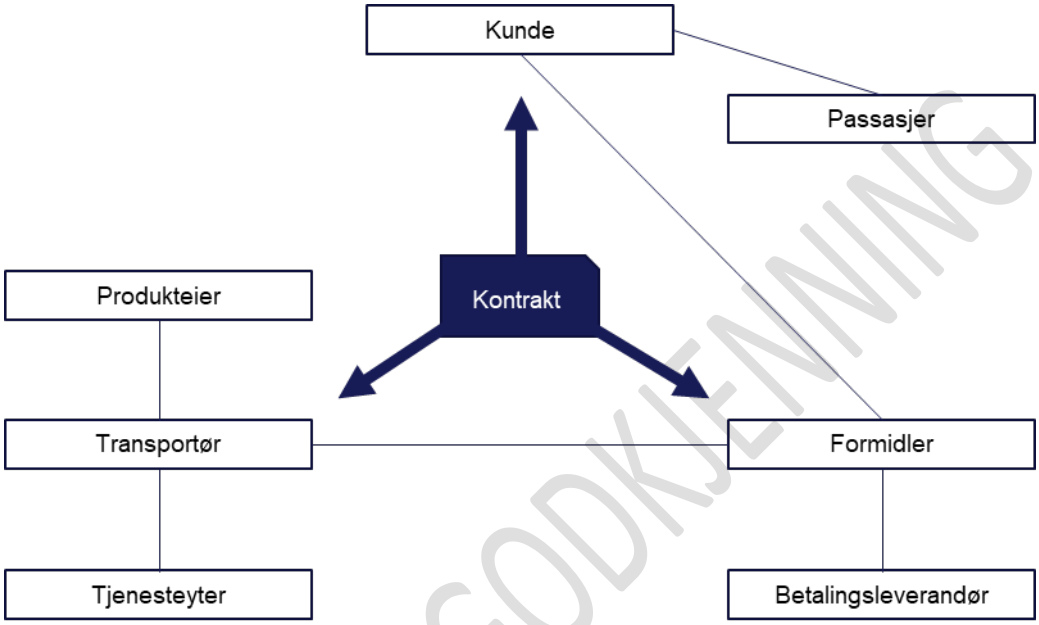
Rekonstruksjon og Refusjon av tapte Kort bør så langt som mulig tilbys anonymt, også ved implementering av nye løsninger, revisjoner, videreutvikling eller endringer.

4.2.5 Skoleskyss

Skoleskyss som nevnt i punkt over i punkt 4.1.5.4 kan ikke gjennomføres anonymt. Ved spesielle behov, som for eksempel elever som bor på hemmelig adresse, må behandling av personopplysninger foretas i så liten grad som overhodet mulig, og tilgangsbegrensning skjerpes.

5 Roller og ansvar

Rollene omfattet i dette kapittelet er begrenset til det som er relevant i en personvernkontekst, altså aktører som er behandlingsansvarlige eller databehandlere for personopplysninger hjemlet i et gyldig behandlingsgrunnlag.



Figur 5-1 Rollemodell

For fullstendig rolleliste for kollektivtransport vises til Håndbok V821 Del 1.

Merk at ulike roller i denne modellen i mange sammenhenger vil bekles av samme Virksomhet eller aktør. Dette blir tydeligere illustrert gjennom eksemplene i kapittel 5.3.

5.1 Kontraktsbegrepet og utveksling av personopplysninger

En kontrakt i skissen er en rett til å benytte et transporttilbud. Kontrakten kan ha ulikt antall parter avhengig av hvordan det enkelte avtaleforhold settes opp.

Utveksling av personopplysninger skjer langs linjene i skissen og må være basert på et behandlingsgrunnlag Merk at en relasjon i modellen kun indikerer at det kan flyte personopplysninger mellom to parter, ikke at det dermed nødvendigvis gjør det. Ved utlevering av personopplysninger mellom aktører i modellen, må den som avgir opplysninger ha hjemmel for utleveringen og den som mottar må ha gyldig hjemmel for å ta dem imot. Slik hjemmel kan finnes i lov, avtale, berettiget interesse eller samtykke. Alternativt kan mottaker opptre som underleverandør/databehandler og derved bygge på en databehandleravtale og behandlingsgrunnlaget fra behandlingsansvarlig.

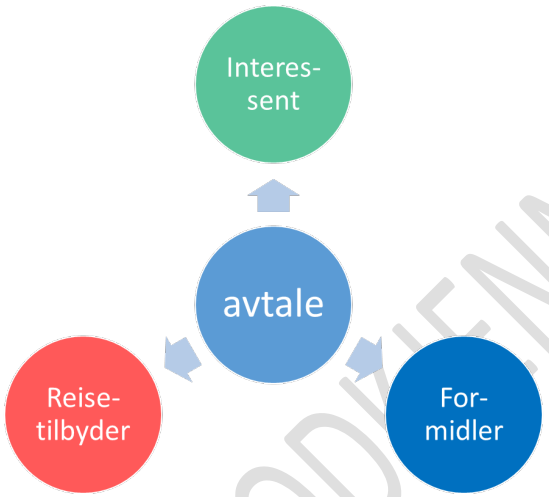
5.2 Personvern gjennom faser av kundereisen

5.2.1 Generiske roller

Modellen presentert i Figur 5-1 Rollemodell kan forenkles ytterligere til en generisk rollemodell som kun fremstiller de parter som er direkte involvert i en avtale som kan omfatte behandling av

personopplysninger. Slike avtaler inngås i separate faser av en kundereise som f.eks salg, billettering og transport.

Interessent er en enkeltperson som kjøper eller benytter seg av en tjeneste. Tjenesten blir tilgjengeliggjort av Formidler og levert av Reisetilbyder. Formidleren og Reisetilbyderen kan være to forskjellige selskap, eller det kan være samme selskap. Avtale om tilgang til tjenesten inngås mellom Interessent og Formidler. Leveranse av tjenesten skjer i relasjonen mellom Interessent og Reisetilbyder. Når Formidler og Reisetilbyder er to ulike selskap, kan de ha inngått databehandleravtale eller avtale om delt behandlingsansvar.



Figur 5-2 Generiske roller

5.2.2 Rollefordeling pr fase

De generiske rollene Reisetilbyder og Formidler bekles av ulike aktører i de ulike faser. Selv om en Virksomhet kan bekle både røde og blå bokser, har Virksomheten ulikt ansvar og mulighetsrom knyttet til behandlingen av personopplysninger i hver av rollene.

Reisetilbyders behandling av personopplysninger i forbindelse med selve befordringen er normalt hjemlet i et behandlingsgrunnlag i relasjonen til Formidler. Når en aktør opptrer som sin egen salgskanal eller kontaktpunkt for kundeservice har aktøren en rolle som formidler med selvstendig behandlingsgrunnlag i relasjonen til interessenten.

Fordeling av roller i de ulike fasene er presentert i tabellform nedenfor, mens de følgende delkapitlene redegjør nærmere for rollefordelingen i hver fase av verdikjeden.

Fase	**Interessent**	**Reisetilbyder**	**Formidler**
Rutesøk	Kunde	Forvalter av rutedata	Kanaleier
Kjøp	Kunde	Produkteier	Selger
Billettering	Passasjer	Transportør	Leverandør av billettbærer
Reise	Passasjer	Transportør	Produkteier
Kundeservice	Kunde	Produkteier / Transportør / Selger	Kontaktpunkt

5.2.3 Behandling av personopplysninger i hver av fasene

1. Rutesøk
Informasjon om rutesøk kan knyttes til en brukerprofil hos kanaleier og brukes til personalisering av søke- og informasjonstjenester. Slik profilering for bruk til personalisering bør være omfattet av avtalen som bruker har inngått ved opprettelse av profil, eventuelt må annet behandlingsgrunnlag finnes f.eks. i avtale. Dersom avtale om behandling av personopplysninger ikke er inngått eller ikke dekker bruk til profilering kan søkehistorikk kun lagres i aggregert anonymisert form for evt analyseformål. Det er vanskelig å finne behandlingsgrunnlag for at personopplysninger og identifiserbar søkehistorikk skal kunne deles med forvalter av rutedata eller leverandører av rutedata.

2. Kjøp
Ved kjøp er det selger som har kundeforholdet og behandlingsgrunnlag for personopplysninger i forbindelse med salget. Kjøpskontrakten omfatter betingelser fra produkteier/transportør og selger. Med mindre det er dekket av kjøpskontrakten, kreves det eksplisitt samtykke for å dele personopplysninger med produkteier og/eller produkteiers underleverandører. Ved deling av personopplysninger omfattet av avtale kan produkteier fungere som databehandler for selger, mens deling basert på samtykke typisk gjør produkteier til behandlingsansvarlig med eget behandlingsgrunnlag uavhengig av grunnlaget benyttet av selger. Produkteiers underleverandører (i.e. transportør og tjenesteyter) vil normalt fungere som databehandlere på vegne av produkteier.

3. Billettering
Den reisende kan ha et kundeforhold med leverandør av billettbærer (e.g. reisekort, kundekort, mobilapp) og velge å få billetten levert til denne billettbæreren. Leverandør av billettbærer er da behandlingsansvarlig og behandlingsgrunnlaget er avtalen mellom leverandør av billettbærer og den reisende. Transportøren kan bruke berettiget interesse som behandlingsgrunnlag for innsyn i personopplysninger i forbindelse med validering og kontroll av reisebevis.

4. Reise
Gjennom kjøpskontrakten gir produkteier den reisende en reiserett i form av en reisehjemmel. Tjenesten leveres av transportøren eller dennes underleverandør (i.e. tjenesteyter). Transportørens behandling av personopplysninger er normalt knyttet til informasjonstjenester/kundebehandling og ikke selve befordringen. Slik behandling kan hjemles i kjøpskontrakten, i avtale med utsteder av billettbærer, eller samtykke. Når behandlingen er hjemlet i samtykke kan transportøren være behandlingsansvarlig på separat behandlingsgrunnlag.

5. Kundeservice
Behandling av personopplysninger i forbindelse med henvendelser til kundeservice kan hjemles i berettiget interesse i og med at kontaktpunkt trenger kontaktopplysninger og annen relevant informasjon i forbindelse med saksbehandlingen. Kontaktpunkt er behandlingsansvarlig som selvstendig aktør. Henvendelsen kan knyttes mot en eksisterende brukerprofil hos produkteier, transportør eller selger. Denne aktøren er da behandlingsansvarlig og kontaktpunkt blir databehandler som underleverandør av kundeservicetjenesten.

5.3 Eksempler

Fordelingen av roller i ulike faser og kontekster er forsøkt illustrert i det følgende gjennom 3 ulike eksempler. For hvert eksempel er rollefordelingen angitt i tabellform. Med unntak av Entur er det brukt generiske betegnelser på aktørene i eksemplene slik at "Fylke A" betegner et fylkeskommunalt administrasjonsselskap og "Tog P" betegner en togoperatør.

5.3.1 Eksempel A: Ruter enkeltreise med produktsamarbeid

Kari Nordmann kjøper enkeltbillett med Fylke A som pålogget bruker i Fylke A sin app. Hun bruker reiserettigheten til å reise med Tog P sitt lokaltog innenfor Fylke A sitt takstområde. Hun samtykker ikke til deling av personopplysninger med transportøren.

5.3.1.1 Rollefordeling – Eksempel A

Fase	Interessent	Reisetilbyder	Formidler
Rutesøk	Kari	Fylke A	Fylke A
Kjøp	Kari	Fylke A	Fylke A
Billettering	Kari	Tog P	Fylke A
Reise	Kari	Tog P	Fylke A
Kundeservice	Kari	Fylke A	Fylke A

5.3.1.2 Analyse – Eksempel A

Opplysninger om rutesøk, kjøp, reisemønster, og evt henvendelser til Fylke A sitt kundesenter lagres og behandles av Fylke A som aktør i ulike roller og med ulikt behandlingsgrunnlag. Rutesøk og reisemønster kan inkluderes i avtalen som Kari har med Fylke A som formidler av informasjons- og salgs-kanal der hun har opprettet en bruker. Tidsrommet for oppbevaring og behandling av disse dataene må likevel begrenses oppad til 410 dager. Kjøpshistorikken må oppbevares med hjemmel i bokføringsloven, men det er ikke hjemlet i lov at transaksjonen skal kunne knyttes til identifiserbar bruker etter en gitt tid. Siden Kari ikke samtykker i deling av kontaktopplysninger med transportøren, vil Tog P kun motta informasjon om at det er solgt en billett til en gitt avgang dersom det er et «til avgang»-produkt. Dersom enkeltbilletten som er kjøpt er et åpent produkt som Kari kan benytte fritt hos flere transportører, vil transportøren ikke få tilgang til personopplysninger og heller ikke informasjon om reisemønster siden dette kun er indirekte tilgjengelig fra rutesøket som evt ble gjort i forkant av kjøpet.

5.3.2 Eksempel B: Gjennomgående reise

Kari Nordmann kjøper gjennomgående enkeltbillett med Tog P og Tog Q som pålogget bruker i Entur appen. Hun knytter kjøpet til sin Tog P bruker og får billetten levert på sitt Tog P sitt kundekort. Hun samtykker til at hennes kontaktopplysninger deles med begge transportørene for bruk til informasjonstjenester.

5.3.2.1 Rollefordeling – Eksempel B

Fase	Interessent	Reisetilbyder	Formidler
Kjøp 1	Kari	Tog P	Entur
Kjøp 2	Kari	Tog Q	Entur
Billettering 1	Kari	Tog P	Tog P
Billettering 2	Kari	Tog Q	Tog P
Reise 1	Kari	Tog P	Tog P
Reise 2	Kari	Tog Q	Tog Q

5.3.2.2 Analyse – Eksempel B

Salgstransaksjonen, og det tilhørende reiseforslaget, lagres hos Entur og overleveres kun til reisetilbyder eller andre formidlere dersom slik utlevering er dekket av avtale, nødvendig for å levere tjenesten eller omfattet av samtykke gitt av kunden. Siden Kari har samtykket, i Enturs kanal, til at hennes kontaktopplysninger deles med transportørene for informasjonsformål, så vil Entur ha hjemmel for å utlevere opplysningene og både Tog P og Tog Q ha hjemmel for å ta imot og lagre og behandle disse personopplysningene til det formålet. Tog P vil videre også behandle Karis personopplysninger i kraft av rollen som utsteder av billettmediet (Tog P sitt reisekort).

5.3.3 Eksempel C: Gjennomgående reise til andre med flere billettmedier

Kari Nordmann kjøper gjennomgående reise som pålogget bruker i Fylke B sin app til sin datter, Eva, og hennes kjæreste, Knut. Reisen er med Fylke B og Fylke C, men Kari samtykker ikke til deling av personopplysninger med Fylke C. Kari betaler med reisepenger fra sitt Fylke D reisekort. Hun velger å få Eva sin Fylke B-billett på hennes datterens Fylke D reisekort, og Eva sin Fylke C-billett i Entur-Appen. Kari oppgir Knut sin epostadresse for at han skal få begge sine billetter tilsendt på epost via Entur sin billetteringsløsning på pdf.

5.3.3.1 Rollefordeling – Eksempel C

Fase	Interessent	Reisetilbyder	Formidler
Kjøp 1	Kari	Fylke B	Fylke B
Kjøp 2	Kari	Fylke C	Fylke B
Billettering 1a	Eva	Fylke B	Fylke D
Billettering 1b	Knut	Fylke B	Entur
Billettering 2a	Eva	Fylke C	Entur
Billettering 2b	Knut	Fylke C	Entur
Reise 1	Eva & Knut	Fylke B	Fylke B
Reise 2	Eva & Knut	Fylke C	Fylke C

5.3.3.2 Analyse – Eksempel C

Kjøpet kobles mot Kari sin Fylke B-bruker. Fylke B kan bruke avtalen om etablering av brukerprofil som behandlingsgrunnlag for å lagre ordreinformasjonen koblet mot Karis profil. Fylke C som produkteier (les Reisetilbyder) har ikke behandlingsgrunnlag for Karis personopplysninger.

Kari må informere Eva og Knut om at hun oppgir deres personopplysninger til Fylke B som formidler og transportør og til Entur som billettmediumutsteder, men ikke til Fylke C som transportør. Fylke D bruker avtalen om leveranse av billettbærer som behandlingsgrunnlag for å registrere reisehjemmel mot Evas profil for Fylke B-reisen, mens Entur bruker tilsvarende avtaler om etablering av profil i Entur-appen som behandlingsgrunnlag for lagring av reisehjemmel på Evas brukerprofil. Entur registrerer Knut sin epostadresse som en temporær brukerprofil og bruker adressen til å distribuere pdf-billett. Knuts temporære Entur-profil og kontaktopplysninger slettes når reisen er gjennomført.

I reise-fasen er Eva en kjent reisende for Fylke B og Fylke C. Fylke B kan bruke evt samtykker og profilinformasjon til å gi Eva tilleggsinformasjon eller evt drive markedsføring. Fylke C derimot har ikke kontaktopplysninger for Eva og evt informasjon om avvik eller annen kommunikasjon må gjøres basert på samtykker eller profildata for hennes Entur-bruker. Verken Fylke B eller Fylke C har kontaktopplysninger til Knut og kan derfor ikke kommunisere med ham i forbindelse med reisen. Entur

har fått kontaktopplysninger for distribusjon av billett, men kan ikke bruke dette til annen kommunikasjon med mindre det i salgsforløpet eller på annen måte er tegnet avtale om, eller innhentet samtykke til dette.

6 Åpenhet, personvernerklæringer og den reisendes rettigheter

Den reisende har en rekke rettigheter som beskrives under. Dels handler disse om at Behandlingsansvarlig skal være åpen om for hvilke formål personopplysningene brukes til og hvilke underliggende prosesser som foregår. Dette har betydning for utforming av personvernerklæringer og samtykkeformuleringer. Dels handler det om spesifikke rettigheter som den reisende har. Under gjennomgås dette.

6.1 Åpenhet og betydning for personvernerklæringer og samtykker

Det er et krav, jf artikkel 5, at Kunden gis full oversikt over hvilke formål som personopplysningene benyttes til og hvilke underliggende prosesser som understøtter disse formålene. Informasjonen skal gjøres enkelt tilgjengelig for Kunden før behandling av Personopplysninger skjer. EU har utgitt en veileder om hva dette innebærer. Her hitsettes sentrale og overordnede krav til en Personvernerklæring:

- Informasjonen skal være lett tilgjengelig og lett forståelig for målgruppen
- I tillegg til formål og behandlinger, skal det gis en beskrivelse av konsekvensene av behandlingen(e) for Kunden
- En link til personvernpolicy skal stå på hver side i et nettsted og posisjonering, form eller fargebruk som gjør personvernpolicyen mindre synlig er ikke i tråd med regelverket
- I en app bør personvernerklæringen aldri være lenger enn to klikk unna
- Endringer i vilkår eller annet må gis beskjed om i god tid før endringer skjer slik at Kunden kan gjøre bruk av sine rettigheter. Beskjed om endringer skal aldri inkluderes i markedsføringshenvendelser
- I løpende kundeforhold bør Kunden minnes på innholdet i Personvernerklæringen med jevne mellomrom, for eksempel kan slik påminnelse sendes ut hvert annet år
- Personvernvilkår kan godt presenteres lagvis, men da skal de elementer med størst personvernkonsekvens for Kunde og det som kan overraske Kunden mest, stå i det første laget
- For behandlinger som det er utført en Personvernkonsekvensvurdering for, kan deler av denne inkluderes i informasjonen til Kunden
- Hvor lenge Personopplysningene vil bli lagret og dersom det ikke kan tidfestes konkret skal det angis hvilke vurderingstema som vil anvendes for å ta stilling til når Personopplysningene skal slettes
- Informasjon om klagerett til Datatilsynet
- Hvorvidt Behandlingsansvarlig vil behandle Personopplysningene for andre forenlige formål enn de ble samlet inn for

Den informasjonen som gis skal angi at transportøren følger denne atferdsnormen og skal som minimum inneholde:

- Hvem som er ansvarlig for Behandlingen av Personopplysninger og vedkommende kontaktinformasjon
- Kontaktinformasjon til Behandlingsansvarliges Personvernombud, dersom Behandlingsansvarlige har dette
- Formålene med Behandlingen og Behandlingsgrunnlaget
- Dersom behandlingen baseres på berettiget interesse, så skal disse berettigede interessene identifiseres

- Dersom man ber om samtykke, skal det informeres om at samtykket er frivillig og at det kan trekkes tilbake når som helst
- Hvem Personopplysningene utleveres til, samt kategorier av Databehandlere som benyttes
- Om Personopplysningene overføres til, eller er tilgjengelig fra, land utenfor EU eller EØS
- Hvilke typer opplysninger som samles inn skal spesifiseres detaljert; typisk Kundeopplysninger (grunndata som navn, adresse o.l.), Reiseopplysninger med detaljeringsnivå på tid og sted for bruk, reisehistorikk og salgsopplysninger
- Lagringstid for opplysninger, med konkret tidsangivelse eller angivelse av hvilke kriterier som vil bli lagt til grunn for sletting av personopplysningene
- Informasjon om adgang til å kreve innsyn, retting av feil informasjon, sletting, og retten til å fremme innsigelser for de behandlinger der dette er en rettighet

Slik angitt i pkt 4.1 kan den reisende være en annen enn den som betaler. For at den reisende skal være kjent med hvordan personopplysningene behandles, typisk at det kan gis innsyn i reiseopplysninger for upersonlige billetter, skal den betalende videreføre informasjon til den reisende om dette. Denne forpliktelsen skal fremkomme i aktørenes personvernerklæring.

6.2 Spesifikke rettigheter

6.2.1 Rett til innsyn

Personer har krav på å begjære innsyn i hvilke konkrete personopplysninger som er registrert om seg selv og da få følgende informasjon i tillegg til det som er nevnt over:

- hvilke konkrete opplysninger som er registrert om vedkommende
- mottakerne eller kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, særlig mottakere i tredjestater eller internasjonale organisasjoner
- dersom det er mulig, hvor lenge det forventes at personopplysningene vil bli lagret, eller, dersom dette ikke er mulig, kriteriene som brukes for å fastsette denne perioden
- retten til å anmode den behandlingsansvarlige om korrigering eller sletting av personopplysninger eller begrensning av behandlingen av personopplysninger som gjelder den registrerte, eller til å protestere mot nevnte behandling
- retten til å klage til en tilsynsmyndighet
- dersom personopplysningene ikke er samlet inn fra den registrerte, all tilgjengelig informasjon om hvor personopplysningene stammer fra
- forekomsten av automatiserte avgjørelser, herunder profilering, som nevnt i artikkel 22 nr. 1 og 4, og, i det minste i nevnte tilfeller, relevant informasjon om den underliggende logikken samt om betydningen og de forventede konsekvensene av en slik behandling for den registrerte. Innsynsretten omfatter ikke opplysninger som er nevnt i personopplysningslovens § 16.

En innsynsbegjæring skal resultere i utlevering av de personopplysninger om vedkommende som den behandlingsansvarlige har på tidspunktet for innsynsbegjæringen, det skal altså ikke slettes personopplysninger om vedkommende før utlevering.

Virksomheten skal utarbeide interne rutiner som sikrer at kun den som det er registrert opplysninger om, får utlevert disse. Forslag til hvordan rett identitet kan sikres er utdypet i Vedlegg 1. Følgende prinsipper skal uansett legges til grunn:

- Betaler (som ikke selv reiser) har i etterkant av kjøpet innsyn i opplysninger som vedrører selve salget, men ikke informasjon knyttet til bruk av reiseretten slik at faktisk tid og sted for reise ikke skal oppgis. Dette gjelder likevel ikke der denne informasjonen inngår i salgstransaksjonen, f.eks. ved plassreserverte reiser med tog.

- Som hovedregel skal man av hensyn til de ansattes sikkerhet ikke utlevere navnet på ansatte som har behandlet kundeopplysninger
- Den Registrerte som innehar et Kort eller en app har krav på alle opplysninger som behandles om vedkommende
- Innsyn kan for enkelhets skyld avgrenses til alle relevante Personopplysninger samt aksesslogg for bruk av "Min Side"-løsninger, men ikke tekniske logger som kan misbrukes til dataangrep
- Virksomheter som er underlagt offentleglova hensyntar de unntak fra innsyn som angis der.
- Personopplysningsloven angir unntak fra innsynsretten hvor de mest praktiske unntakene er at innsyn ikke kan gis grunnet behov for hemmelighold av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger eller at personopplysningene utelukkende finnes i tekst som er utarbeidet for intern saksforberedelse, og som heller ikke er utlevert til andre, så langt det er nødvendig å nekte innsyn for å sikre forsvarlige interne avgjørelsesprosesser. Merk at dette medfører at den registrerte vil ha innsyn i mange dokumenter, også mange interne dokumenter og f.eks. fritekstfelt/chat hvor vedkommende er omtalt. Innsynet gjelder kun personopplysningene om vedkommende, slik at annen informasjon kan sladdes
- Den Registrerte har også innsynsrett i sikkerhetstiltakene knyttet til den aktuelle Behandling, likevel slik at det ikke skal leveres ut tekniske logger slik at sikkerheten svekkes

Sikkerhetstiltakene knyttet til behandling av Personopplysninger skal være tydelig beskrevet og enkelt tilgjengelig. Dette gjelder kun så langt innsyn ikke svekker sikkerheten. Det er eksempelvis tilstrekkelig med en typebenevnelse av den aktuelle sikkerhetsløsning, typisk at man oppgir at Kortene er beskyttet med ”DESFire”-teknologi uten å gjengi sikkerhetsløsningen på Kortet i detalj.

Anonyme Kunder skal i den grad det er nødvendig og mulig ha rett til innsyn i Reiseopplysninger for å sikre kontroll med funksjonalitet og transaksjoner, samt rett til å klage ved feil. Dette kan for eksempel gjøres ved å bruke App Id, QR-kode eller Reisekortnummer som referanse r, i kombinasjon med andre opplysninger slik det er beskrevet i Vedlegg 1.

6.2.2 Hvordan skal innsyn gis

For å få innsyn i hvilke opplysninger som behandles, må henvendelsen enten skje gjennom personlig oppmøte, være skriftlig og undertegnet, eller sendes inn per e-post. Personen som spør skal kunne identifiseres som den Registrerte[4].

Innsyn kan gis via elektroniske hjelpemidler, for eksempel via en ”Min Side”-løsning Svaret kan alternativt sendes per post til den adressen som er registrert i registeret, eller ved at vedkommende møter opp fysisk, og kan identifiseres som den Registrerte, men skal ikke sendes per e-post .

6.2.3 Retting av opplysninger

Virksomheten plikter å rette opplysninger om den Registrerte. Hovedmålet med retting er å sørge for at Virksomheten har oppdatert og korrekt informasjon om Kunden.

Virksomheten har plikt til uoppfordret å sørge for at opplysninger som behandles er riktige, herunder at det foretas nødvendig oppdatering og retting av opplysningene. Ved tvil om riktigheten av opplysningene kontrolleres de nærmere, for eksempel ved at Kunden kontaktes.

Ved henvendelse fra den berørte Kunde skal retting skje så snart som mulig, med mindre Virksomheten har grunn til å betvile at henvendelsen kommer fra rette vedkommende eller at det som opplyses er korrekt.

[4] Eksempelvis kan dette gjøres ved at innsyn gis mot fremvisning av kort.

Dersom den Registrerte begjærer retting skal behandlingen av personopplysningen om ham stilles i bero til kravet er avgjort, jf. 6.7.

Retting innebærer normalt at uriktige opplysninger slettes. Kravet til oppdatering og retting innebærer likevel ikke at opplysninger skal slettes dersom opplysningene kan ha betydning som dokumentasjon (for eksempel i sak om billettkontroll). Oppdatering skjer i tilfelle på den måten at opplysningene tydelig markeres og suppleres med korrekte opplysninger.

6.2.4 Rett til sletting, nødvendig oppbevaringstid

Den Registrerte har rett til å få opplysninger om seg selv slettet i en rekke situasjoner, jfr GDPR art 17. De viktigste grunnlag for sletting er angitt under.

Sletting eller anonymisering skal foretas når det ikke er nødvendig å behandle personopplysninger lengre. Vurderingen av dette skal foretas av den behandlingsansvarlige. Dersom personopplysningene ikke slettes er Behandlingsansvarlig ansvarlig for at behandlingen fortsetter på lovlig grunnlag.

Sletting av opplysninger som kan kobles til et individ kan skje ved at alle opplysninger slettes/fjernes eller at identifikatorer som knytter opplysningene til den registrerte slettes, slik at opplysningene ikke kan reidentifiseres.

Pseudonymisering og hashing godtas ikke som sletting. Det å stille en Registrert i «passiv» i et datasystem er heller ikke det samme som å slette Personopplysningene. Behandlingsansvarlig skal utarbeide interne retningslinjer på hvordan anonymisering skal skje.

Opplysninger som er nødvendige for fakturerings- eller arkivformål følger særlige regler, se Vedlegg 2[5].

6.2.4.1 Særlige slettefrister grunnet kollektivsektorens art

De fleste opplysninger brukes til å gi bedre service, følge opp avtalen med kunden eller å inndrive krav. Reiseopplysninger brukes også til avregning.

Salgsopplysninger viser når kunden har kjøp en billett eller lastet opp reisepenger, trukket av konto, men gir ikke noen opplysninger om selve reisen (reiseopplysninger). Salgsopplysninger er aktuelle når kunden har innsigelser til bruken av billetten/reisepengene og for å kunne kontrollere kjøpshistorikk i billettkontrollsaker i tilfeller hvor den Registrerte har reist innsigelser mot kravet.

Virksomheter som er omfattet av atferdsnormen er underlagt ordningen med klage på transporttjenesten til Transportklagenemda. Klagefristen er 1 år etter at Virksomheten har avgitt sitt svar.

Reiseopplysninger og salgsopplysninger[6] kan lagres i inntil 410 dager etter at reisehjemmelen er utløpt, og skal deretter slettes[7]. Dersom kunden klager til Transportklagenemnda kan opplysningene lagres til saken er avgjort.

[5] Dette vedlegget opprettes etter at spørsmål om lagring iht. Bokføringslovgivningen er utredet.
[6] Salgsopplysninger inneholder i begrenset grad opplysninger som kan si noe om kundens reisemønster, men oppbevaring er viktig for å kunne tilby kunder avtaler som "capping", dvs at man betaler for hver reise som utføres, men etter man har betalt over et visst beløp så belastes ikke kunden mer. Ved capping kan sone og strekning behandles. Dette kan ved uenighet også føre til klage til Transportklagenemnda fra kunder som mener de har betalt for mye, jf note 4.
[7] Inntil enhver reiserett (også helårs billetter) er utløpt har kunden en klagerett og i noen tilfeller vil kunden først bli klar over behovet for å klage etter at reiseretten er utløpt (typisk hvor første validering er feil i en periodebillett og ny billett utstedes/innkreves på uventet tidspunkt for den reisende). Klagen må så

Kundeopplysninger kan lagres så lenge Kunden har et kundeforhold til Virksomheten, deretter skal opplysningene slettes/ anonymiseres innen 14 dager fra det tidspunktet at kundeforholdet er avsluttet.

Virksomhetene kan lagre reiseopplysninger som anses nødvendig for å oppfylle krav til dokumentasjon i samsvar med bokføringsregelverket og arkivloven. I vedlegg 2 er det nærmere beskrevet hva dette innebærer i forhold til bokføringsregelverket[8]. For regler om sletting i back-up, se punkt 9.5.3.

Virksomhetene som er underlagt atferdsnormen har behov for å kartlegge statistikk over reisemønster for å ha tilstrekkelig grunnlag for ruteplanlegging. Slik aktivitet skal så langt som mulig gjøres anonymt, men kortvarig bruk av opplysninger om MAC adresse, typisk 24 timer, er akseptabelt dersom det er nødvendig for dette formål.

For å sikre at de slettefristene overholdes, skal alle Virksomheter ha rutiner for sletting av Personopplysninger, det skal tilstrebes å ha automatisk sletterutiner som kan kontrolleres manuelt. Dokumenter inneholdende Personopplysninger skal sikkerhetsmakuleres på forsvarlig måte.

Status med hensyn til sletting av unødvendige Personopplysninger skal beskrives av virksomheten med sikte på ledelsens årlige gjennomgang og vurdering av etterlevelse av regelverket. Under gjennomgås ulike typesituasjoner der Personopplysningene skal slettes.

6.2.4.2 Personopplysningene er ikke lengre nødvendige for formålet

Vurderingen av hvor lenge personopplysninger er nødvendige for formålet skal foretas av den behandlingsansvarlige. Vurderingen skal hensynta at Personopplysningene skal lagres så kort som mulig, men legge vekt på konkrete behov for å lagre Personopplysningene, herunder behov knyttet til klage til Transportklagenemnda, inngåtte avtaler med den Registrerte og eventuelle nye behandlingsformål.

Dersom personopplysningene ikke slettes vil Behandlingsansvarlig være ansvarlig for ulovlig behandling.

6.2.4.3 Samtykke trekkes tilbake

Personopplysninger som er registrert på grunnlag av samtykke, skal slettes så snart som mulig dersom samtykket trekkes tilbake og det ikke foreligger et annet behandlingsgrunnlag som gjør at personopplysningene må beholdes videre, typisk lovgrunnlag.

6.2.4.4 Avtaleforhold sies opp

Dersom Kunden avslutter et avtaleforhold, skal ikke Reisebeviset sperres/leveres inn før Reiserettigheten er utgått/brukt opp. Hvis mulig skal Reisebeviset konverteres til et anonymt alternativ og innenfor avtalt oppsigelsestid skal den Reisende alltid informeres om hva konsekvensene av oppsigelsen er for gjenværende Reiserettigheter. Deretter skal Personopplysninger slettes så snart som mulig dersom annen oppbevaringshjemmel (f.eks. bokføringsregelverket) ikke finnes.

Kunden skal få informasjon om slettefrister for produkter og tjenester når avtale inngås.

behandles hos Virksomheten. deretter har kunden rett til å klage i inntil ett år etter han reklamert, jf forskrift om klagenemnd for passasjertransport § 5-2. Transportklagenemnda legger jevnlig til grunn den reisendes påstand og for at dette ikke skal misbrukes i stor skala, må bransjen sikre sin mulighet til å føre bevis. I tillegg må det settes tilstrekkelig tid til håndtering av feil i avregning mellom selskapene; periodebillett løper i 366 dager (skuddår), innsamlingsperiode for transaksjoner fra kjøretøy er 14 dager, deretter 30 dagers betalingsfrist på utstedt faktura - og i denne perioden må fakturagrunnlaget kunne bestrides. Altså 410 dager.

[8] Dette vedlegget opprettes etter at spørsmål om lagring iht. Bokføringslovgivningen er utredet.

6.2.4.5 Inaktive kunder

For kunder som ikke kjøper eller benytter transportrelaterte tjenester innen tre år skal personopplysningene slettes med mindre behandlingsgrunnlaget fornyes. Eksempelvis kan da behandling som har vært basert på samtykke fortsette dersom nytt samtykke gis.

Kunder som selv aksesserer en profil eller konto anses som aktive. Ensidig aktivitet initiert fra tjenestetilbyder anses ikke som aktivitet fra kunde.

6.2.4.6 Andre årsaker til sletting

Dersom den registrerte gjør innsigelse mot behandlingen i henhold til artikkel 21, og det ikke finnes mer tungtveiende berettigede grunner til behandlingen, skal personopplysningene slettes. Dette gjelder i situasjoner der det rettslige grunnlag for behandlingen er at den er nødvendig for å ivareta en berettiget interesse eller å utøve offentlig myndighet og kunden har et særskilt behov for sletting.

Dersom Personopplysningene er blitt behandlet ulovlig, f.eks. til andre uforenlige formål, jf. art 6 nr. 4, skal man sikre at den ulovlige behandlingen umiddelbart opphører, herunder slette personopplysningene.

6.2.4.7 Effektuering av sletting

Alle opplysninger som identifiserer kunden skal slettes så raskt som mulig.

6.2.5 Dataportabilitet

Den registrerte har rett til å få utlevert til seg eller å få overført til en annen behandlingsansvarlig alle opplysninger som kan knyttes til ham selv. Dette gjelder opplysninger som den registrerte selv har gitt til den behandlingsansvarlige og kun dersom det rettslige grunnlaget for behandlingen er samtykke eller at behandlingen av personopplysninger er nødvendig for å oppfylle en avtale med den Registrerte.

Opplysningene skal gis i et strukturert, alminnelig anvendt og maskinleselig format, f.eks. ved hjelp av Excel eller på XML-format.

6.2.6 Rett til begrensning av bruken av Personopplysningene

Den registrerte har etter GDPR art 18 rett til at Behandlingsansvarlig begrenser behandling av personopplysningene i følgende tilfeller:

a) den registrerte bestrider riktigheten av personopplysningene,
b) behandlingen er ulovlig og den registrerte motsetter seg sletting av personopplysningene og isteden anmoder om at bruken av personopplysningene begrenses,
c) den behandlingsansvarlige ikke lenger trenger personopplysningene til formålet med behandlingen, men den registrerte har behov for disse for å fastsette, gjøre gjeldende eller forsvare rettskrav, uansett om det skjer innenfor rammen av en rettergang eller en administrativ eller utenrettslig prosedyre
d) den registrerte har gjort innsigelse mot behandling i henhold til artikkel 21 nr. 1 i påvente av kontrollen av om hvorvidt den behandlingsansvarliges berettigede grunner går foran den registrertes.

Med begrensning menes at den behandlingsansvarlige merker opplysningene og kun lagrer/kontrollerer dem.

6.2.7 Underretningsplikt

Den behandlingsansvarlige skal underrette enhver mottaker som har fått utlevert personopplysninger, om enhver korrigering eller sletting av personopplysninger eller begrensning av behandlingen med mindre dette viser seg å være umulig eller innebærer en uforholdsmessig stor innsats. Den

behandlingsansvarlige skal underrette den registrerte om nevnte mottakere dersom den registrerte anmoder om det.

6.2.8 Rett til å protestere

Den registrerte skal til enhver tid, av grunner knyttet til vedkommende særlige situasjon, ha rett til å protestere mot behandling av personopplysninger om vedkommende, og som har grunnlag i artikkel 6 nr. 1 bokstav e) - eller f). Dette gjelder også ved profilering med grunnlag i disse bestemmelser.

Innsigelsen fra den registrerte må være knyttet til vedkommende særlige situasjon. Dette kan for eksempel være et særlig behov for beskyttelse av identitet eller at vedkommende tilhører en særlig sårbar gruppe. Hvis den registrerte har rett til innsigelse, plikter den behandlingsansvarlige å avslutte behandlingen av personopplysningene, med mindre man 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.

For eksempel vil berettiget interesse oftest være behandlingsgrunnlaget for å kreve inn et krav fra en billettkontroll. En innsigelse mot interessevurderingen om at det foreligger en berettiget interesse i å inndrive krav om tilleggsavgift vil sjelden føre frem. Der den som ilegges tilleggsavgift grunnet manglende betaling protesterer mot registreringen på grunnlag av stort anonymitetsbehov, f.eks. vitnebeskyttelse, kan personopplysninger om vedkommende slettes så snart tilleggsavgiften er betalt.

Den registrerte skal i den første kommunikasjonen med behandlingsansvarlig gjøres oppmerksom på retten til innsigelse Informasjon om rettigheten skal framlegges på en klar måte og atskilt fra annen informasjon, for eksempel at det nevnes i et eget avsnitt i personverninformasjonen ved innsamling av opplysningene.

6.2.9 Automatiserte individuelle avgjørelser, herunder profilering

Den registrerte skal ha rett til ikke å være gjenstand for en avgjørelse som utelukkende er basert på automatisert behandling, herunder profilering, jf artikkel 22. Forordningen definerer profilering som enhver form for automatisert behandling av personopplysninger som innebærer å bruke personopplysninger for å vurdere visse personlige aspekter knyttet til en fysisk person, særlig for å analysere eller forutsi aspekter som økonomiske situasjon, personlige preferanser, interesser, pålitelighet, atferd, plassering eller bevegelser.

Bestemmelsen innebærer i utgangspunktet et forbud mot automatiserte avgjørelser, men gjelder bare dersom avgjørelsen har rettsvirkning for, eller på tilsvarende måte i betydelig grad påvirker den registrerte. Dette innebærer at bestemmelsen ikke får anvendelse der den automatiserte behandlingen kun er et støtteverktøy for saksbehandlere.

Det er likevel en del unntak som følger av art 22, nr. 2 – med den følge at automatiserte beslutninger kan tas og profilering gjennnomføres. De viktigste unntakene gjelder dersom avgjørelsen;

- er nødvendig for å inngå eller oppfylle en avtale mellom den registrerte og en behandlingsansvarlig
- er basert på lov
- er basert på den registrertes uttrykkelige samtykke

Dersom noen av unntakene i art 22, når 2 kommer til anvendelse skal behandlingsansvarlig fastsette egnede tiltak for å ivareta den registrertes rettigheter og et av tiltakene skal i det minste være retten til menneskelig inngripen fra den behandlingsansvarlige, til å uttrykke sine synspunkter og til å bestride avgjørelsen.

Den behandlingsansvarlige skal være nøye med å gi tilstrekkelig forhåndsinformasjon om hvordan behandlingen utføres og dens konsekvenser.

Automatiserte avgjørelser skal ikke bygge på særlige kategorier av personopplysninger, med mindre det rettslige grunnlaget for behandlingen er samtykke eller dersom avgjørelsen er viktig av hensyn til viktige samfunnsinteresser som følger av nasjonalretten eller EUs unionsrett, samt at det er innført egnede tiltak for å verne den registrertes rettigheter, friheter og berettigede interesser.

6.3 Frist for å besvare henvendelser

Svar på henvendelser fra den Registrerte skal gis uten ugrunnet opphold og senest innen 30 dager.

Dersom det vil ta lengre tid enn dette, skal det gis et foreløpig svar med opplysninger om grunnen til forsinkelsen og sannsynlig tidspunkt for når svar kan forventes.

7 Utlevering av personopplysninger til andre enn kunden

7.1 Hovedregel

Det skal foreligge Behandlingsgrunnlag for utlevering av Personopplysninger til en tredjepart. Kunden skal på generell basis informeres om utlevering og hvem opplysningene utleveres til.

7.2 Utlevering til politiet/påtalemyndigheten

Retten kan ved kjennelse pålegge Virksomhetene å utlevere Personopplysninger som kan antas å ha betydning i en pågående sak, jf. straffeprosessloven § 210, første ledd.

Dersom det er fare for at etterforskningen vil lide i påvente av rettens kjennelse, kan politiet også henvende seg til påtalemyndigheten for en ordre om utlevering av opplysninger, jf. straffeprosesslovens § 210, annet ledd. Påtalemyndighetens beslutning skal snarest mulig forelegges retten for godkjennelse.

Når krav om opplysninger fremmes, må Virksomheten kreve kopi av rettens kjennelse eller påtalemyndighetens skriftlige ordre.

Pålegget skal angi hvorvidt underretning til den registrerte om at personopplysningene er utlevert til politiet, skal utsettes i en nærmere bestemt periode. Der pålegget angir at den registrerte ikke skal informeres, skal dette respekteres.

7.3 Bruk av databehandlere

Dersom det benyttes helt eller delvis eksterne tjenesteleverandører for Behandling av Personopplysninger i Virksomheten, skal det inngås en Databehandleravtale med den eksterne leverandøren og Personopplysningsloven stiller en rekke krav til hva som må reguleres i Databehandleravtaler.

Virksomheten må etablere rutiner som sikrer at leverandøren gjennomfører Behandlingen i samsvar med avtalen.

8 Bruk av nye løsninger og ny teknologi, innebygget personvern

Det kommer stadig nye løsninger og teknologi som kan bidra til å forbedre kollektivtransporten. Bruk av ny teknologi eller nye løsninger skal vurderes opp mot prinsippene i normen både ut fra personvernkonsekvenser og informasjonssikkerhetsspørsmål. Arbeidsgruppen skal gjennomgå ny teknologi jevnlig og dette kan gi grunnlag for revisjon av normen, jf. punkt10.

For å påse at ny teknologi tas i bruk på en måte som ivaretar de fastsatte regler og prinsipper for personvern, skal bransjen legge til grunn hensynet til personvern allerede i designfasen av nye produkter og tjenester slik at bruken av personopplysninger minimaliseres. Prinsippene om innebygget personvern/privacy by design skal ivaretas. Visse tjenester er underlagt krav om anonymitet, jmf pkt 4.2, men også utover dette skal det vurderes om nye tjenester kan tilbys anonymt eller med så lite personidentifiserende opplysninger som mulig.

8.1 Særlig om internettløsninger

Ved bruk av Internett, skal Virksomheten sikre at de løsninger som blir utviklet ivaretar kravet om anonymitet, se punkt 4.2.

Anonymiteten kan for eksempel svekkes i forbindelse med logging av IP-adresser, bruk av cookies og lignende. Ved salg eller betjening av Anonyme produkter, skal bransjen ikke legge opp til loggføring av IP-adresser eller bruk av andre elementer som kan undergrave Kundenes anonymitet. Dette gjelder også bruk av tredjepartsverktøy og lignende. Tekniske logger kan av sikkerhetshensyn lagres så lenge som virksomheten finner det nødvendig[9].

I løsninger og skjermbilder hvor anonymitet er valgt, skal det ikke være unødvendige tekstfelt eller andre løsninger som åpner for avlevering av Personopplysninger.

8.2 Særlig om mobilbillettering

Dersom app/mobilbillettering tilbys som hovedløsning for billettering skal som minimum en tilsvarende tilgjengelig - og enkel løsning - kunne tilbys anonymt på samme type plattform. Se mer om dette under punkt 4.2 Anonyme alternativer.

Før applikasjonen lastes ned, må Kunden gis tilgang til informasjon om hvilke opplysninger i telefonen som applikasjonen benytter, hvorfor og til hva de benyttes og hva som lagres, samt øvrige informasjonskrav og krav til åpenhet. Denne informasjonen skal både være tilgjengelig der applikasjonen lastes ned og i selve applikasjonen.

Løsningen skal fungere uten unødvendig bruk av tilganger.

8.3 Særlig om ulike former for kontobasert billettering

Kontobasert billettering vil kunne innebære både online og offline lagring av reisehjemler. Reisehjemler kan være billetter eller andre avtaler om reise, f.eks. ved etterskuddsvis prisberegning for å gi kunden beste pris. I motsetning til for reisekort, hvor reisehjemmelen lagres på reisekortet, vil reisehjemmelen

[9] Undersøkelser viser at det gjennomsnittlig tar opptil et år før angrep avdekkes, og det er derfor behov for å kunne gå tilbake i tid i aksesslogger og tekniske logger. Såfremt disse loggene lagres forsvarlig og med begrenset tilgang er personverntrusselen lav.

ved kontobasert billettering lagres i et felles baksystem og aksesseres ved hjelp av en forhåndsvalgt identifikator ved reisen. Reisekortet kan være en slik identifikator, hvor reisekortets kortnummer benyttes som kobling til reisehjemmelen.

En konto er i seg selv ikke personidentifiserende, men kan inneholde et eller flere av disse elementene, hvorav ingen er obligatoriske:

- Kundedata for registrerte kontoer (navn og kontaktinformasjon)
- Logindata (brukernavn og passord)
- Billetter
- Avtaler om reise, som automatisk kjøp eller etterskuddsvis prisberegning og betaling
- Betalingsavtaler
- Identifikatorer for å finne riktig billett ved reise

Billetter, avtaler og identifikatorer lagres i et felles reisehjemmelslager, mens kundedata og login-data lagres av kontoeier. Betalingsavtaler kan lagres i felles lager der de skal kunne brukes av flere parter.

For reisekort vil det kunne finnes en konto som kun inneholder reisekortets kortnummer som identifikator og eventuelle billetter som er kjøpt i tilknytning til kortet.

Kontoeier vil normalt være transportør eller formidler. Personidentifiserende kundedata tilknyttet kontoen vil kun være tilgjengelig for kontoeier og den som kontoeier har databehandleravtale med. Deling av data for andre formål vil kreve kundens samtykke.

Produktselger/formidler vil ha tilgang til egne kundedata og kontoer, samt egne salg og betalingsavtaler dekket av samarbeidsavtaler. Produkteier vil ha tilgang til gjennomførte salg og bruk av egne produkter, men ikke kundedata de ikke selv er behandlingsansvarlig for. Tjenesteyter vil ha tilgang på aktuelle hjemler for bruk på egne transportmidler, samt relevante betalingsavtaler.

Avlesinger vil av hensyn til inntektssikring bli samlet og analysert med hensyn på å avdekke misbruk.

8.3.1 Capping og pay-as-you-go

Løsninger for capping (pristak) og pay-as-you-go (etterskuddvis prisberegning) vil ofte forutsette lagring av salgsopplysninger. Salgsopplysninger dekker geografisk gyldighet for reisehjemmelen. I enkelte tilfeller kan det være på stoppestednivå. For slike løsninger kan reiseinformasjon lagres så lenge som avtaleperioden dekker, og oppgjør mellom partene er gjennomført.

For kunder som ikke ønsker slike løsninger skal likevel anonyme løsninger for periodebilletter som gir tilsvarende pris være tilgjengelig.

8.4 Betalingsløsninger

Det anbefales å benytte selvstendige aktører for å besørge betaling som benytter Personopplysninger. Disse aktørene vil være Behandlingsansvarlige og deres behandling av Personopplysninger omfattes ikke av denne normen. Behandlingen skal skje så anonymt som mulig avhengig av hvilken tjeneste Kunden ønsker å kjøpe.

Dette bør så langt som mulig løses gjennom at betalingen foregår adskilt fra billetteringssystemet.

Hvis anbefalingen ikke følges, skal personopplysninger filtreres bort så fort transaksjonen er gjennomført for de tilfeller hvor betalingen ikke er separert fra billetteringssystemet.

Dersom det benyttes lokasjonsdata som grunnlag for prisberegning og/eller betaling, skal koblingen mellom id som kan identifisere brukeren og lokasjon gjøres på en slik måte at den behandlingsansvarlige ikke skal kunne gjøre denne koblingen og derved få vite noe om kundens posisjon.

8.5 Bruk av e-post og mobiltelefonnummer

E-postadresse kan benyttes som identifikator i anonyme løsninger, men Virksomheten skal da informere om at om anonymitet ikke er sikret dersom e-postadressen åpenbart angir navn eller annen klar identifikasjon.

I anonyme løsninger skal Virksomheten ikke benytte mobiltelefonnummer som identifikator.

8.6 Autonome kjøretøy, «hente hjemme»-tjenester

Testing og bruk av autonome kjøretøy følger den til enhver tid gjeldende særlovgivning om dette.

Ved bruk av «hente hjemmetjenester» som en tilleggstjeneste til ordinær transport kan det behandles nødvendige personopplysninger i samsvar med de grunnleggende prinsipper i GDPR. Der «hente hjemmetjenester» utgjør eneste produkt, skal dette tilbys uten krav om registrering av profil.

9 Dokumentasjon, internkontrollsystem

Utforming av dokumentasjon og system for internkontroll avhenger av de faktiske forhold i den enkelte Virksomhet, men det foreligger en omfattende forpliktelse til å kunne dokumentere at regelverket er etterlevd, jf art 5. Virksomhetens Personvernombud skal engasjeres i arbeidet med internkontrollsystem, men skal ikke ha en besluttende rolle i utformingen.

Virksomheten skal ha rutiner for vanlige arbeidsprosesser som omfatter Personopplysninger. Fordi bruk av statistikk og anonyme data kan reise særlige problemstillinger med hensyn på reidentifisering, anbefales at Virksomheten har en rutine på hva som utgjør anonyme data for den enkelte Virksomhet (da dette kan variere med geografisk utbredelse, antall reisende, osv).

9.1 Kartlegging, oversikt

Virksomheten skal ha oversikt over hvilke personopplysninger Virksomheten forvalter, hvor disse befinner seg, mv. Oversikten skal holdes oppdatert. Under er en liste over hva en slik oversikt minst må inneholde.

- Navnet på og kontaktopplysningene til den behandlingsansvarlige og eventuelt felles behandlingsansvarlige,
- Personvernombudet,
- Formålene med behandlingen,
- En beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger,
- Kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, herunder mottakere i tredjestater eller internasjonale organisasjoner,
- Dersom det er relevant, overføringer av personopplysninger til en tredjestat eller en internasjonal organisasjon,
- De planlagte tidsfristene for sletting av de forskjellige kategoriene av opplysninger,
- En beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene

I tillegg må Virksomheten ha en oppfatning av om det må lages en vurdering av personvernonsekvenser for behandlingen. For å ta stilling til dette er det nødvendig med en innledende konsekvensvurdering.

9.2 Innledende konsekvensvurdering

Ved innføring av nye Behandlinger av Personopplysninger, typisk nye arbeidsprosesser, skal det alltid gjennomføres en vurdering av om Behandlingen medfører en risiko for den Reisende og hvilke tiltak som må iverksettes for å motvirke disse. Dersom risikoen for den registrerte er betydelig, skal det gjennomføres en vurdering av personvernkonsekvenser (ofte kalt DPIA fra det engelske Data Protection Impact Assessment), se punkt 9.3under. I den innledende konsekvensvurderingen skal man bl a vurdere juridisk behandlingsgrunnlag, risiko for den registrerte (ikke for Virksomheten) og hvilke it-faglige tiltak og organisasjonsmessige tiltak som bør settes i verk for å ha en lovlig behandling av personopplysningene. Alle virksomheter bør ha en særskilt rutine for innføring av nye behandlinger av Personopplysninger/it-systemer.

Dersom det er trolig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige, før behandlingen starter opp, foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet. En vurdering av personvernkonsekvenser/DPIA er nødvendig dersom det legges opp til en systematisk og omfattende vurdering av personlige aspekter ved fysiske personer. Under er en liste over typiske

elementer som gjør det nødvendig med en vurdering av personvernkonsekvenser/DPIA. Det kan være tilstrekkelig at kun ett av disse forholdene foreligger, men avhengig av risikoen kan det noen ganger være nødvendig at to kriterier foreligge før man må gjennomføre en vurdering av personvernkonsekvenser/DPIA:

1. Det gjennomføres en evaluering av den registrerte - inkl profilering
2. Det gjennomføres automatiske avgjørelser
3. Det gjennomføres en systematisk monitorering
4. Det gjøres bruk av sensitive opplysninger, eller opplysninger av svært personlig art
5. Behandlingen omfatter personopplysninger i stort omfang - noe som skal vurderes etter følgende faktorer:
    a. antall subjekt som omfattes
    b. volum av data om subjektene
    c. behandlingslengde i tid
    d. geografisk omfang
6. Behandlingen kombinerer to datasett, f.eks. fra ulike databaser.
7. Innebærer opplysninger om personer som er særlig sårbare, hvor balanse forholdet mellom den Behandlingsansvarlige og den den Registrerte er skjevt, f.eks. opplysninger om barn, eldre mm.
8. Bruker innovative teknologiske løsninger og/ eller ny teknologi.
9. Har en avgjørende innvirkning for en den Registrertes rett til en tjeneste eller inngåelse av en kontrakt, f.eks. skoleskyss.

9.3 Personvernkonsekvensutredninger (DPIA)

Vurdering av personvernkonsekvenser skal gjennomføres når det foreligger en såkalt høy risiko for den registrerte. Terskelen for at risikoen kan defineres som høy er relativt lav, og under er type situasjoner der sektoren skal gjennomføre en vurdering av personvernkonsekvenser, basert på Datatilsynets veiledning.

- Personopplysninger samlet inn via en tredjepart i følge med minst ett annet kriterium.
    - For eksempel innsamling og sammenstilling av personopplysninger fra tredjeparter for å avgjøre om den registrerte skal få tilbud om, fortsette å motta, eller nektes et produkt, en tjeneste eller et tilbud, særlig når det gjelder sårbare registrerte (f.eks. unge), og ved evaluering/poengsetting.
- Behandling av biometriske opplysninger for å identifisere enkeltpersoner i følge med minst ett annet kriterium.
- Behandling av personopplysninger med innovativ teknologi i følge med minst ett annet kriterium.
- Behandling av personopplysninger, uten samtykke, for vitenskapelige eller historiske formål i følge med minst ett annet kriterium.
    - For eksempel behandling av reiseopplysninger om personer med nedsatt funksjonsevne for forskningsformål uten den registrertes samtykke.
- Behandling av lokasjonsdata i følge med minst ett annet kriterium.
- Systematisk monitorering, inkludert kameraovervåking, på offentlig tilgjengelige områder i stor skala, inklusive stasjonsområder og om bord i transportmidler.
- Behandling av særlige kategorier av personopplysninger eller svært personlige opplysninger i stor skala for algoritmetrening.
- Behandling av personopplysninger der formålet er å tilby en tjeneste eller utvikle produkter for kommersiell bruk som involverer å forutsi personlige preferanser eller interesser, pålitelighet, adferd, lokasjon eller bevegelsesmønster.
- Innsamling av personopplysninger gjennom «tingenes internett».

Listen er ikke uttømmende, og praksis på dette vil utvikles over tid.

Vurderingen skal minst inneholde:

a. en systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen, herunder, dersom det er relevant, den berettigede interessen som forfølges av den behandlingsansvarlige,
b. en vurdering av om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålene,
c. en vurdering av risikoene for de registrertes rettigheter og friheter som nevnt i nr. 1, og
d. de planlagte tiltakene for å håndtere risikoene, herunder garantier, sikkerhetstiltak og mekanismer for å sikre vern av personopplysninger og for å påvise at denne forordning overholdes, idet det tas hensyn til de registrertes og andre berørte personers rettigheter og berettigede interesser.

Vurderingene skal foretas hvert tredje år eller ved vesentlige endringer i behandlingen av personopplysninger.

Personvernombudet bør bistå vurdering av personvernkonsekvenser.

9.4 Avvik

Avvik skal registreres og iverksatte tiltak skal dokumenteres. Alle brukere er pliktig til å melde fra om avvik internt.

Med mindre brudd på personopplysningssikkerheten sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter skal behandlingsansvarlig melde brudd til Datatilsynet senest 72 timer etter å ha fått kjennskap til det. Dersom det er sannsynlig at bruddet på personopplysningssikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige uten ugrunnet opphold underrette den registrerte om bruddet.[10]

Behandling av personopplysninger i strid med regler og de iverksatte sikkerhetstiltak behandles som eller avvik. Et avvik kan for eksempel være at uautoriserte interne brukere har fått tilgang til personopplysninger.

9.5 Informasjonssikkerhet

9.5.1 Grunnleggende krav

Informasjonssikkerhet i henhold til personopplysningsloven handler om å sikre Personopplysningenes konfidensialitet, integritet og tilgjengelighet.

Ansvaret påhviler øverste leder i Virksomheten, som kan delegere utførelsen av ansvaret. Det skal angis definerte sikkerhetsmål og vurderinger av hva som er et akseptabelt sikkerhetsnivå gjennom styrende og gjennomførende dokumenter i Virksomhetens internkontrollsystem. Iverksatte kontrollrutiner og tiltak skal, basert på en risikovurdering, sikre Personopplysninger mot misbruk internt og eksternt.

[10] Typisk vil tilfeller der man vet at personopplysninger er kommet uvedkommende i hende, måtte meldes både til Datatilsynet og til den registrerte, uavhengig av om man vet om personopplysningene har blitt brukt av uvedkommende eller ikke. I tilfelles der man oppdager en svikt i behandlingen av personopplysninger, men man ikke har indikasjoner på at denne er utnyttet av uvedkommende, vil det normalt ikke være meldeplikt til Datatilsynet eller den registrerte, såfremt svikten rettes.

9.5.2 Risikovurderinger

Risikovurderinger er et verktøy for å sikre god informasjonssikkerhet. Risikovurderinger skal utføres både før endringer i eksisterende løsninger, og før etablering av nye løsninger. Risikovurderingen skal vurdere sannsynlighet for, og konsekvensen av, uønskede hendelser for Virksomheten og for Kunden. Risikovurderingen skal angi avhjelpende tiltak for identifiserte risikoer og disse tiltakene er et element i øvrige personvernmessige konsekvensvurderinger.

Risikovurderinger skal som minimum sikre at de personvernprinsipper og sikkerhetskrav som fremkommer av denne atferdsnormen er ivaretatt.

9.5.3 Sikkerhetskopier, back-up

Virksomheten er pliktig til å ha sikkerhetskopi. Virksomheten må vurdere hvor lenge sikkerhetskopien skal beholdes, og ha dokumentasjon internt på denne vurderingen[11]. Det foreligger ingen forpliktelse til å utlevere, rette eller slette personopplysninger i sikkerhetskopiene.

9.5.4 Tilgang til personopplysninger

Kun ansatte hos Virksomhetene som har tjenstlig behov for tilgang til Kundeopplysninger og/eller Reiseopplysninger skal få tilgang til de deler av det elektroniske billettsystemet hvor slike opplysninger ligger lagret.

Behandlingsansvarliges medarbeidere skal pålegges taushetsplikt for Personopplysninger og annen informasjon med betydning for informasjonssikkerheten. Det skal føres logger som viser hvem som har gjort oppslag i opplysninger. I tillegg skal det føres en oversikt over hvem som er autoriserte brukere av applikasjoner som gir tilganger til Personopplysninger.

9.6 Personvernombud

Offentlige Virksomhetene er pålagt å opprette Personvernombud som blant annet skal bistå Virksomheten og Kundene med spørsmål om personvern, samt oppfølging av internkontroll. For private Virksomheter anbefales å oppnevne en Personvernombud selv om dette ikke alltid er pålagt.

EU har utgitt retningslinjer for hvordan Personvernombudene skal utøve sin rolle og denne bør legges til grunn når virksomhetene lager stillingsinstruks for rollen. Retningslinjene understreker at Personvernombudet har en uavhengig rolle hvor vedkommende skal kunne ta stilling til om virksomheten følger lovverket eller ikke, noe som bla medfører at roller som CIO, CTO, HR-direktør ikke kan ha posisjonen fordi disse rollene ikke er tilstrekkelig uavhengige og dersom virksomheten har en compliance- eller internrevisjonsavdeling er det et naturlig sted å plassere rollen. Personvernombudet skal ha god kjennskap til både personvern og til bedriftens systemer og behandling av Personopplysninger. Flere virksomheter kan dele Personvernombud.

Eksempler på oppgaver for Personvernombud er:

a. Utarbeide og revidere interne rutiner
b. Foreta løpende vurdering av behandling av personopplysninger i Behandlingsansvarliges systemer, inklusive forhåndsvurdering av ny/ endret behandling av personopplysninger
c. Bistå ved utarbeidelsen av utredninger for personvernkonsekvenser ("Data Protection Impact Assessments (DPIA)"
d. Gi råd og veiledning til ansatte og ledelse, og bistå med opplæring
e. Bistå med egenkontroll av behandlingen av personopplysninger

[11] Undersøkelser viser at det gjennomsnittlig tar opptil et år før angrep avdekkes, og det er derfor behov for å kunne gå tilbake i tid for å sikre integritet i data og identifisere personer som er berørt av angrepet.

f. Bidra til at bedriften har tilstrekkelig internkontrollsystem og dokumentasjon, bistå og ivareta de registrertes interesser og følge opp brudd på personvernlovgivningen i enkeltsaker
g. Motta meldinger om avvik og delta i arbeid med avviksbehandling
h. Gjennomføre revisjon av etterlevelse av personvernregelverket

9.7 Etterlevelse og kontroll

Den enkelte Virksomhet er selv ansvarlig for å oppfylle personvernregelverkets krav og normens bestemmelser.

Datatilsynet legger normen til grunn ved tilsyn, etterlevelse og kontroll med Virksomheter som skal følge normen.

10 Oppdatering og endring av atferdsnormen

10.1 Rutiner for endringer

Normen vil måtte oppdateres i tråd med relevante endringer i lovverk, ny teknologi, etc.

Oppdateringer skal vedtas av en styringsgruppe basert på forslag fra en arbeidsgruppe. Styringsgruppens vedtak oversendes så Datatilsynet for behandling og vedtak der.

10.2 Styringsgruppen

Som styringsgruppe benyttes Strategisk samhandlingsforum, som beskrevet i Jernbanedirektoratets dokument «Retningslinjer for gebyrordning».

Etter behov kan Strategisk samhandlingsforum selv utnevne andre deltakere til å delta.

Avgjørelser skal tilstrebes å treffes enstemmig.

10.3 Arbeidsgruppen

Det opprettes en egen arbeidsgruppe på Taktisk samhandlingsnivå for vedlikehold av atferdsnormen. Arbeidsgruppen består av deltakere fra Jernbanedirektoratet Entur AS og representanter fra samferdselssektoren.

Etter behov kan også andre deltakere utnevnes til å delta i arbeidsgruppen, typisk personvernombud fra sentrale aktører.

Avgjørelser i arbeidsgruppen skal tilstrebes å treffes enstemmig.

10.4 Møter

Arbeidsgruppen møtes minimum én gang i året for å diskutere oppfølgningen av atferdsnormen og behovet for oppdateringer. Jernbanedirektoratet innkaller til slike møter.

Ved behov skal styringsgruppen få utarbeidet prosjektplan for revisjoner og endringer av normen etter innspill fra arbeidsgruppen.

11 Definisjoner

11.1 Juridisk

Juridiske begrep i normen som også brukes og er definert i personvernregelverket skal ha samme betydning som der. Under er likevel tatt inn noen kortfattede forklaringer på sentrale begrep.

Anonyme opplysninger: Opplysninger der navn, fødselsnummer og andre kjennetegn er fjernet eller ikke registrert, slik at opplysningene ikke lenger kan knyttes til en enkeltperson.

Anonymt (reise)kort: Kort som Virksomheten ikke kan knytte til en person.

Begrensning av behandling: Merking av lagrede personopplysninger med det som mål å begrense behandlingen av disse i framtiden.

Behandling: Enhver bruk av Personopplysninger, for eksempel innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

Behandlingsgrunnlag: Rettslig grunnlag, også kalt hjemmel, for å behandle Personopplysninger, for eksempel Kundens samtykke, hjemmel i lov - eller offentlig myndighetsutøvelse.

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.

Databehandleravtale: Avtale som regulerer rettigheter og plikter mellom den Behandlingsansvarlige og Databehandleren.

Kundeopplysninger: Kundeopplysninger er kontaktdata om den Registrerte som for eksempel navn, adresse og Kortnummer. Alle Kundeopplysninger vil være Personopplysninger.

Den Registrerte: Den som en Personopplysning kan knyttes til.

Personopplysninger: Opplysninger og vurderinger som kan knyttes til en enkeltperson.

Profilering: Enhver form for automatisert behandling av personopplysninger som innebærer å bruke personopplysninger for å vurdere visse personlige aspekter knyttet til en fysisk person, særlig for å analysere eller forutsi aspekter som gjelder nevnte fysiske persons arbeidsprestasjoner, økonomiske situasjon, helse, personlige preferanser, interesser, pålitelighet, atferd, plassering eller bevegelser.

Pseudonymisering: Behandling av Personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt Registrert uten bruk av tilleggsopplysninger, forutsatt at slike tilleggsopplysninger lagres atskilt og omfattes av tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar fysisk person. av

Reiseopplysninger: Opplysninger fra en transaksjon på billettbærer som registreres ved bruken av en Billett.

Salgsopplysninger: Opplysninger om oppladning av reisepenger på billettbærer eller bruk av reisepenger begrenset til dato, tid, beløp og sone.

Håndbok 821: Veileder/standard for elektronisk billettering som alle som har fått konsesjon for å drive offentlig transport etter yrkestransportloven er pliktig til å følge

11.2 Roller

Betalingsformidler: Den som tilgjengeliggjør en betalingstjeneste.

Formidler: Formidler av grenseflate mot kunde/bruker for levering av tjeneste, f.eks. billettsalg, eier av app, utstedelse av reisekort, konto, informasjonsformidling eller kundeservice.

Identitetstilbyder: Lager og fremskaffer en pålitelig mekanisme/token for autentisering av en kunde eller passasjer. Lagres gjerne på et medium.

Kontoeier: Ansvarlig overfor kunde/passasjer for kontoen som lagrer produkt, verdi eller annen avtale om reise og/eller betaling ved kontobasert billettering. Kan utføre salg.

Kunde: En person som inngår/trer inn i avtale med en Produkteier og/eller Tjenesteyter og som normalt selv vil benytte seg av en kollektiv transporttjeneste, m.a.o. den som kjøper tjenester.

Passasjer/reisende: Den som benytter transporttjenesten.

Kortutsteder: Virksomheten som har utstedt reisekort.

Produkteier: Et selskap eller institusjon som definerer alle produkter som Produkteier skal tilby Kundene. Dette skjer etter avtale med takstmyndighet.

Produktforhandler: Den som forestår selve salget og mottar betaling fra kunden. Gjennomfører salgstransaksjon og refusjon.

Takstmyndighet: Det organ som fastsetter og godkjenner tilbud og priser, som regel en fylkeskommune.

Tjenesteyter/operatør: Det selskapet som transporterer Kunden

Transportør: Transportør er den juridisk ansvarlige for transportarbeidet, og er Kundens avtalepart. Transportør er også ansvarlig for Tjenesteytere som har akseptert Produkteiers reisebevis som et dokument som gir rett til en transporttjeneste for Kunden.

Utsteder av mediet: Den som utsteder og er ansvarlig for mediet, det være seg medium for produkter, verdi eller identitet.

Virksomhet: Organ i fylkeskommunen eller et selskap som er medlem av Kollektivtrafikkforeningen og som planlegger, samordner, bestiller og markedsfører kollektivtransporten i et fylke eller i et nærmere avgrenset område.

11.3 Billetter og kort

Aktivere billetten: Igangsette en Billett som ligger i Kortet.

Anonym billett/produkt: En Billett som kan benyttes av ihendehaver uten at det må avgis Personopplysninger til Virksomheten så lenge Kunden sørger for å ha Gyldig billett.

App-id: ID tildelt den enkelte app-installasjon på en telefon.

Automatisk påfylling: Regelmessig oppfylling av Reisepenger på Kortet etter avtale med Kunden.

Billett: Dokumentasjon av reisehjemmelen/transportavtalen om kollektivtransport med Kunden lagret på en billettbærer.

Billettmaskin: En maskin hvor Kunden kan kjøpe eller fornye Billetter eller lese av en igangsatt Billett.

Capping: Se pristak.

Fornye Billett: Kjøpe ny Billett av samme type.

Gyldig billett: Aktivert Billett som gir Kunden rett til å reise den aktuelle strekningen. Kriteriene for hva som anses som gyldig billett fastsettes nærmere i transportørens reisevilkår.

Kortnummer: Entydig identifikator av Kort, lagret både i Kortet og i baksystemene.

Kontobasert billettering: Billettering med lagring av billetter i baksystem i stedet for på offline billettbærere som reisekort. Kunden tilkjennegir sin knytning til reisehjemmelen med en forhåndsdefinert identifikator.

Identifikator: Bevis for kundens knytning til en reisehjemmel eller konto. Eksempler på identifikatorer er dagens reisekort, QR-koder, betalingskort, nasjonale id-kort og biometri. En identifikator må alltid ha et visst nivå av sikkerhet for hindre misbruk.

Konto: Lagringsområde for kontobasert billettering. Kan lagre billetter, kundeprofil, registrerte identifikatorer for knytning til billett, betalingsavtaler m.m. Trenger ikke å lagre kundens identitet.

Kortleser: Utstyr ombord i buss, trikk, tog eller båt som kan lese av Kortet.

Lese av billettbærer/kort (avlese) Holde billettbærer inntil Kortleser for å:

1. Vise informasjon: lese av Kort uten å endre innhold (uten å etterlate spor
2. Utføre forhåndsbestemte handlinger mot Kortet som å sperre det eller laste ned automatisk fornyelse.
3. Starte/fortsette en kollktivreise ved kommunikasjon med Kortleser som å utstede eller å Aktivere en billett.
4. Registrere bruk av Billetten som ikke er aktivering av Billett (for eksempel ny reise eller overgang).

Handlinger omfattet av nr. 3 og 4) ble tidligere benevnt å validere.

Pay as you go: Løsning hvor reisen registreres og riktig beløp for betaling fastsettes i etterkant, basert på registrerte data.

Periodebillett: En Billett som gjør det mulig for Kunden å reise mellom bestemte soner/områder eller strekninger i en bestemt tidsperiode, for eksempel 30 dager etter at den er aktivert.

Personlig billett: En Billett som kun kan benyttes av den Billetten er utstedt til.

Personlig kort: Kort som er registrert på eller er utstedt til én person.

Pristak: Garantert makspris ved bruk av «pay as you go» eller kjøp av flere frittstående billetter over en avgrenset periode, hvor det settes maksimalpris når fastsatte grenser nås. Slike grenser kan være på reiselengde, reisetid eller totalpris for flere reiser over en lengre periode, som dag, uke eller måned.

Refundere/Refusjon: Tilbakebetale restverdi på et Kort (refusjon av Billetter og/eller Reisepenger).

Registrert kort: Kort hvor opplysninger om eieren er registrert i et kunderegister.

Reisehjemmel: Billett eller annen avtale som gir rett til å benytte en transporttjeneste.

Reiserett: De reiserettigheter som følger av en gyldig Reisehjemmel.

Reisekonto: En betalingskonto som lagres sentralt hos Virksomheten hvor reisekontoen belastes iht. avtale hver gang en Kunde bruker reisekontoen til å betale for en Billett. Må ikke forveksles med konto for kontobasert billettering.

Reisekort: En billettbærer som kan inneholde Billetter og Reisepenger.

Reisemønsterkartlegging: Registrering av de reisendes bevegelsesmønster på tvers av transportmidler for å skaffe datagrunnlag til ruteplanlegging.

Reisepenger: Verdi på Kortet som kan brukes til å betale for en reise eller kjøpe en Billett.

Rekonstruere/Rekonstruksjon: Gjenskape/rekonstruere kortinnholdet slik det var siste gang Kortet ble brukt.

Tellesystemer: Teknologiske løsninger for automatisk telling av reisende på transportmidler.

Tilleggstjenester: Tjeneste som ikke er knyttet til selv reiseretten, for eksempel rekonstruksjon.

Uregistrert kort: Kort hvor opplysninger om eieren ikke er registrert i et kunderegister

11.4 Annet

Reiseplanlegging: Kundens prosess for å finne reisealternativer og planlegge sin reise.

Ruteplanlegging: Kollektivselskapets prosess for å planlegge det totale rutetilbudet til publikum.

Symmetrisk/asymmetrisk kryptering: Symmetrisk kryptering er når samme nøkkel benyttes for både kryptering og dekryptering. Asymmetrisk kryptering er når forskjellig nøkkel brukes til kryptering/dekryptering eller signering/verifikasjon.

Synkron/asynkron dataoverføring: Synkron dataoverføringer når informasjon overføres i sanntid, og bekreftelse/svar kommer umiddelbart. Ved asynkron dataoverføring sender avsender en melding som først blir mottatt på et senere tidspunkt.

12 Vedlegg

Vedlegg 1: Krav til identifikasjon

Vedlegg 2: Lagring og sletting av personopplysninger for bokførings- og arkivformål (Produseres senere)

Vedlegg 1 - Krav til identifikasjon

Handlinger med konsekvens for den registrerte, slik som blant annet å sperre et reisekort, å korrigere eller slette personopplysninger eller å gi ut personopplysninger, skal kun skje dersom man er sikker på at en anmodning kommer fra riktig person.

Hvordan man kan konstatere at riktig person fremmer en henvendelse vil avhenge av hvilken salgskanal og på hvilket medium en reiserett er registrert. Normalt vil det være tilstrekkelig å be den registrerte om opplysninger som transportøren allerede har om vedkommende. Unntaksvis kan det være relevant å be vedkommende om tilleggsinformasjon. Man skal ikke be om flere opplysninger enn nødvendig. For eksempel vil det sjeldent være påkrevet å be om kopi av pass. Under er noen typetilfeller.

Foreldre kan be om informasjon for egne barn inntil fylte 15 år.

Dersom en kunde ber om informasjon på vegne av noen andre, må man be om fullmakt, eller be rette vedkommende om å ta kontakt selv.

Hvordan verifisere at den som retter en henvendelse er rette vedkommende

Avhengig av hvilken type begjæring og hva den knytter seg til, kan det være aktuelt med litt forskjellig metodikk for å sikre at det er rette vedkommende, men under står noen generelle retningslinjer.

Ved telefonisk kontakt fra kunde, må saksbehandler forsikre seg om at kunden er den han utgir seg for. Når kunden er identifisert, skal saksbehandler opplyse om hvilke opplysninger Ruter har registrert, og at sak er opprettet. Saksbehandler bør spørre etter minst tre av følgende opplysninger:

- Reisekortnummer/app-id/ordrenummer
- Navn
- Adresse
- Kundenummer
- Fødselsdato, evt fødselsnummer i saker om skoleskyss
- Billettkjøp
- E-postadresse/telefonnummer
- I billettkontrollsaker: hvor og når billettkontrollen fant sted og på hvilken linje

Hvordan saksbehandle ulike henvendelser

Henvendelse til kundebehandlere

Innsyn i reiseopplysninger må etterspørres skriftlig, ved personlig oppmøte. Man skal be om legitimasjon dersom man er usikker på at det er rette vedkommende som ber om innsyn (merk at man må ha fullmakt for egne barn over 15 år når man ønsker reiseopplysninger).

Ved gjenskaping av kort, overføring av mobilapper eller sperring skal man alltid be om legitimasjon dersom dette skjer i skranke. Det bør gis mulighet til å utvise skjønn ved gjenskaping i spesielle tilfeller, som f.eks. barn eller eldre. Saldo kan oppgis ved å lese av kortet uten mer informasjon.

Dersom henvendelser skjer pr e-post (eventuelt post) må stille tilstrekkelig kontrollspørsmål for å sikre at det er rette vedkommende. Ved fortsatt tvil må man be om legitimasjon.

Dersom legitimasjon fremvises skal kontrollnummer skrives som notat. Man kan oppgi reiseopplysninger til andre ved kopi av fullmakt fra korteier.

Innsyn i opplysninger knyttet til uregistrert reisekort

Det skal ikke utleveres reiseopplysninger på uregistrerte reisekort over skranke eller telefon.

Kunden kan likevel få innsyn i reiseopplysninger dersom han sender inn en skriftlig anmodning hvor han, i tillegg til å oppgi reisekortnummer/ app ID, K må sannsynliggjøre at vedkommende er rette eier ved å vedlegge bankutskrift som bekrefter minst to av billettkjøpene.

Min side-løsninger

Ved min side løsninger skal kunden ved å oppgi tilstrekkelig autentifiseringsopplysninger for å påvise at han/hun er rette vedkommende. Første gangs innlogging må skje med to-faktor identifisering.

Noe av min side informasjonen skal tilbys anonymt, uten registering av navn og adresse. Dette gjelder for eksempel opplysninger om reise og kjøp.