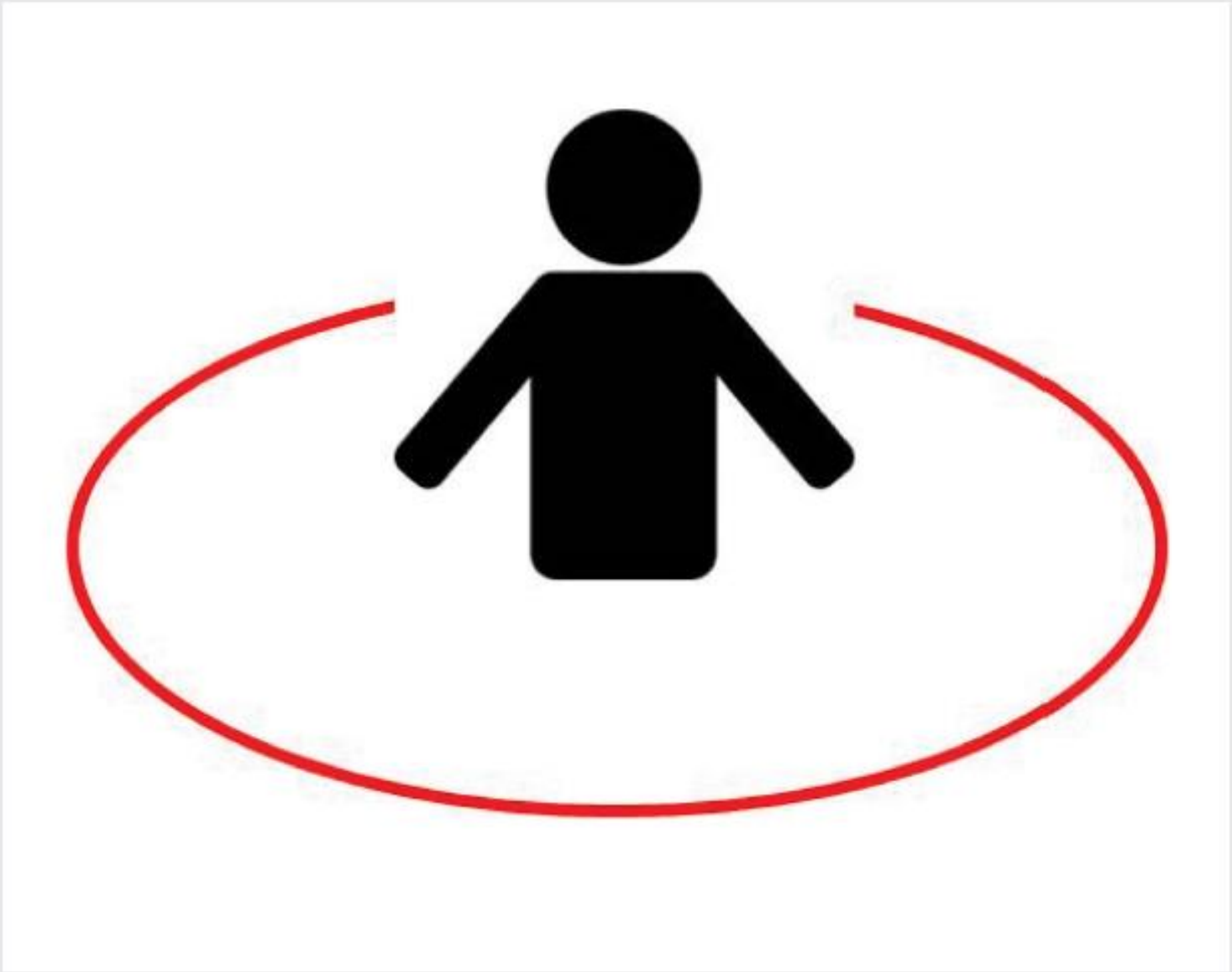
Vegdirektoratet
Veg- og transportavdelingen
Trafikkforvaltning
2014

Statens vegvesen

Bransjenorm

for personvern og informasjonssikkerhet i elektronisk billettering



Illustrasjon: Trond Foss

Revisjonshistorie

Versjon	Dato	Forfattere	Viktigste endringer
1	4. desember 2011	Eva Jarbekk, Svend Eric Wandaas, Mette Hendbukt	Første versjon av dokumentet
2	September 2014	Mette Hendbukt, Eva Jarbekk, Cathrine Ruud	Ny forside, presisering av privacy-by-design prinsippet, nytt avsnitt om mobilbillettering (kap 7.9.2)

Innhold

1 Bakgrunn og formål

Kollektivtrafikkbransjen i Norge implementerer løsninger for elektronisk billettering. Implementering av slike løsninger er en politisk målsetting. Noen virksomheter har allerede innført elektronisk billettering, mens andre virksomheter er på planleggingsstadiet. Det er en politisk målsetting at man skal kunne reise "sømløst" med elektronisk billett i Norge uavhengig av hvilke transportselskap som benyttes.

Innføring av elektronisk billettering reiser en rekke personvernrettslige spørsmål som må løses i henhold til bestemmelsene i lov om behandling av personopplysninger av 14.4.2000 nr. 31 (pol) med tilhørende forskrifter. Personopplysningsloven bygger på EU-Direktiv 95/46/EF, om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger.

For å etablere en felles forståelse av hvordan bestemmelsene skal tolkes, er denne bransjenormen utarbeidet av sentrale aktører i bransjen, transportmyndigheter og Datatilsynet i fellesskap. Formålet er dels å skape forutsigbarhet for aktørene i tolkningen av regelverket, dels å skape et tillitvekkende og godt personvern for de reisende. Kollektivtrafikkbransjen skal kunne utvikle gode tjenester for de reisende, samtidig som man utarbeider verktøy for å ivareta personvern og god informasjonssikkerhet.

2 Forholdet mellom bransjenormen og andre regler

Bransjenormen er hjemlet i pol § 42, tredje ledd nr. 6.

Alle Virksomheter som har løyve eller mottar tilskudd er forpliktet til å følge Håndbok 206 (HB 206). HB 206 henviser til denne bransjenormen, og bransjenormen er således bindende for aktørene.

Virksomheter som ikke er forpliktet til å følge HB 206 kan velge å tilslutte seg bransjenormen, og gir skriftlig melding om dette til Vegdirektoratet. Oversikt over Virksomheter som velger å tilslutte seg normen vedlikeholdes av Vegdirektoratet. Normen angir grunnleggende prinsipper for elektronisk billettering, 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.

Bransjenormen gjelder med unntak for eventuelle avvikende nasjonale og internasjonale rettslige forpliktelser.

3 Behandling av personopplysninger i kollektivtrafikken

Utformingen av elektroniske billetteringsløsninger bygger på HB 206 som er utarbeidet av Statens vegvesen Vegdirektoratet og aktører i bransjen.

De elektroniske billettsystemene er transaksjonsbasert, det vil si at systemenes oppbygging forutsetter at reiseopplysninger fra hver enkelt transaksjon samles inn for å ivareta visse formål med behandlingen, se nærmere i Vedlegg 1. HB 206 bygger på ISO/DIS 24014-1:2005.

Avtalen mellom reisende og transportør er lagret på det elektroniske reisekortet. Rettigheter for den reisende ligger i en "kontrakt" på kortet. Kontrakten vises frem for kortleseren, noe som normalt generer en transaksjon som samler inn de reise-opplysningene som er beskrevet i Vedlegg 1. Mange av systemene er offline, og det skjer en asynkron overføring av data.

Kortnummeret er, sammen med en transaksjonsteller på kortet, sentral i de elektroniske billettsystemene. Kortnummeret er nødvendig for å kunne verifisere at alle kortavlesninger er kommet inn og er korrekte. Kortnummeret er for eksempel avgjørende for å kunne feilsøke og for å verifisere at relevante transaksjoner (salg, valideringer, refusjoner m.m.) er med i avregningsgrunnlaget.

Dessuten vil kortnummeret være avgjørende for å kunne yte tilleggstjenester til kunden som for eksempel abonnement og rekonstruksjon.

Noen reisende har avtale om ulike varianter av reisekonto. I slike avtaler er det lagret en betalingsavtale på kortet – koordinert mot et betalingsinstrument i baksystemet. Reisekontonummer brukes bare når slik avtale er inngått på forhånd med kunden.

Ikke all aktivitet medfører innsamling eller lagring av reiseopplysninger ved avlesning på en billettautomat. Et eksempel vil være når kunden bare sjekker hvilket produkt som ligger på kortet, eller om det er gyldig.

4 Personvernombud

Det anbefales at Virksomhetene oppretter personvernombud som blant annet skal bistå Virksomheten og Kundene med spørsmål om personvern, samt oppfølging av internkontroll.

5 Samtykke og krav om anonyme alternativer

Kunden har en grunnleggende rett til å kunne bestemme over sine Personopplysninger og til å kunne velge å ferdes anonymt i samfunnet. Bruk av Personopplysninger i elektronisk billettering skal baseres på Kundens samtykke, jf. pol § 11, første ledd bokstav a) og § 8 første ledd.

Et samtykke skal være uttrykkelig, frivillig og informert. Frivilligheten anses først å være reell når det foreligger reelle anonyme alternativer til personlige reiseprodukter.

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 derfor tilby anonyme alternativer i tillegg til personifiserte Billetter og tjenester.

Under angis hvordan Virksomheten skal tilby anonyme alternativer, slik at det anonyme alternativ utgjør et valgbart alternativ for den reisende. Et Registrert kort som ikke er registrert på innehavers navn hos Kortutsteder er tilstrekkelig anonymt.[1]

5.1 Pris

Det skal tilbys lik pris for anonyme og personidentifiserbare reiser.

For sentrale personlige reiseprodukter skal det også tilbys tilsvarende Anonyme produkter. Det er likevel ikke nødvendig at man tilbyr samme produkttype så lenge det anonyme alternativ er minst like fordelaktig for Kunden som den personifiserte Billett. Dette innebærer at dersom rabattordninger tilbys, må det være likeverdige rabatt-ordninger for personlige og Anonyme produkter.

5.2 Salgskanaler

Som hovedregel skal produkter som gir rett til anonyme reiser kunne kjøpes gjennom samme salgskanaler som personifiserte produkter. Dette gjelder salgskanaler hvor det selges Billetter over disk/luke og på Billettmaskiner.

Dersom man tilbyr en internettløsning for kjøp av produkter, så skal den også tilby Anonyme produkter. Selve kjøpet skal kunne foretas anonymt.

[1] Dette innebærer at et kort med bilde og navn anses som anonymt så lenge det ikke kan identifiseres hos Kortutsteder.

Unntak fra dette kan gjøres dersom det ikke er praktisk mulig å tilby Anonyme produkter i alle salgskanaler, så lenge en kan tilby en alternativ salgskanal som er lett tilgjengelig.

5.3 Tilleggstjenester

Tilleggstjenester som ikke er knyttet til selve reiseretten, kan være personlige. Eksempler er SMS-varsling ved forsinkelser og etterskuddsvis betaling.

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

6 Innsynsrett

6.1 Generell innsynsrett

Alle har krav på å få innsyn i følgende opplysninger:

a) Navn og adresse på Behandlingsansvarlig, typisk Virksomhetens navn og adresse. Det skal også opplyses om hvem som har det daglige ansvaret for at loven etterleves i selskapet.

b) Virksomheten skal kunne redegjøre for hva som er formålet med Behandlingen av Personopplysninger og hvilke typer Personopplysninger som behandles, se nærmere i punkt 8.

c) Det skal informeres om hvor opplysningene er hentet fra, om de vil bli utlevert og eventuelt til hvem.

d) Innsynsrett etter offentleglova omfatter ikke innsyn i Reiseopplysninger, jf. offl §13 annet ledd, jf. fvl §13 første ledd nr. 1).

Uregistrerte Kunder skal så langt som mulig ha rett til innsyn i Reiseopplysninger for Kortet de disponerer for å sikre kontroll med funksjonalitet og transaksjoner, samt rett til å klage ved feil.[2]

6.2 Registrerte kunders rett til innsyn

Registrerte kunder har, i tillegg til opplistingen i punkt 6.1, krav på å få vite hvilke opplysninger som er registrert om seg selv.

Virksomheten skal utarbeide interne rutiner som sikrer at kun den som det er registrert opplysninger om, får utlevert disse. Følgende prinsipper skal legges til grunn:

[2] Eksempelvis kan dette gjøres ved at innsyn gis mot fremvising av kort.

- Betaler har kun innsyn i opplysninger som vedrører selve salget.[3]
- Den Registrerte som innehar et Kort har krav på alle opplysninger som behandles om vedkommende.
- Innsyn kan for enkelthets skyld etter avtale med den som ber om innsynet, avgrenses til de mest relevante opplysninger som hvilke Kundeopplysninger som er registrert og Reiseopplysninger som angir tid og sted for reisen.
- Den Registrerte har også innsynsrett i sikkerhetstiltakene knyttet til den aktuelle Behandling.

Sikkerhetstiltakene skal beskrives i et eget dokument av Virksomhetene, og være tilgjengelig for utsendelse. Dette gjelder kun så langt innsyn ikke svekker sikkerheten. Det er eksempelvis tilstrekkelig med en typebenevnelse av den aktuelle sikkerhets-løsning, typisk at man oppgir at Kortene er beskyttet med ”DESFire” teknologi uten å gjengi sikkerhetsløsningen på Kortet i detalj.

6.2.1 Hvordan innsyn skal gis

For å få utvidet 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 Registerte.

Svaret sendes per post til den adressen som er registrert i registeret, og skal ikke sender per e-post.

Innsyn kan alternativt skje via elektroniske hjelpemidler, for eksempel via en ”Min Side” løsning.

Det vil som hovedregel ikke bli gitt innsyn i saksrelaterte kommentarfelt. Dette anses for å være tekst som er utarbeidet for den interne saksforberedelse.

6.2.2 Frist for å besvare henvendelsen

Svar på henvendelser om innsyn 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.

[3] Dette medfører at tid og sted for reise ikke skal oppgis.

6.3 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.

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.

7 Grunnkrav til behandling av personopplysninger i billetteringssystemet

7.1 Samtykke og andre behandlingsgrunnlag

Det må foreligge et Behandlingsgrunnlag for hvert formål Personopplysningene skal benyttes til. Under gjennomgås sentrale Behandlingsgrunnlag.

7.1.1 Generelt om samtykke og informasjon til kunden – formkrav

Samtykke avgis av Kunden på basis av den informasjon Virksomheten har gitt. Samtykket skal være frivillig, jf. punkt 6 om anonyme alternativer.

Samtykke kan avgis muntlig, men av hensyn til etterprøvbarhet anbefales at det innhentes skriftlig eller ved avkryssing i elektronisk skjema.

Dersom betaler er en annen enn den som skal inneha/benytte Kortet, skal betaler påse at vedkommende person får tilstrekkelig informasjon.[4]

[4] Typisk vil dette gjelde for arbeidsgivere som betaler for ansattes bruk av reisekort i arbeidstiden. Arbeidstakeres bruk av Registrerte kort krever samtykke fra hver ansatt.

Samtykke og informasjon skal minimum inneholde følgende:

- Hvem som er ansvarlig for Behandlingen av Personopplysninger.
- Informasjon om at samtykket er frivillig, og at anonyme alternativer eksisterer.
- Formålet med Behandlingen skal angis, se Vedlegg 1; typisk:
    - Utstede Billetter, for eksempel ved automatisk fornyelse av Billett eller Reisepenger;
    - Yte kundeservice ved å tilby Tilleggstjenester som for eksempel:
        - Rekonstruksjon
        - Refusjon av større beløp
        - SMS-varsling;
    - Foreta feilsøking og internkontroll;
    - Avregne fakturagrunnlag mellom Virksomheter (det skal ikke gjøres koblinger mellom Reiseopplysninger og Kundeopplysninger).
- Om, og til hvem, Personopplysninger utleveres.
- 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.
- Informasjon om adgang til å kreve innsyn, retting og sletting av feil informasjon.

Vedlegg 2 angir en mal for hvordan utforming av samtykke og informasjon kan utformes. Malen er basert på de formål bransjen typisk har for de grunnleggende reiseprodukter og Tilleggstjenester.

Virksomheten skal veilede i hvordan man kan foreta en avlesning som ikke medfører innsamling eller lagring av Reiseopplysninger, eksempelvis når Kunden kun ønsker å sjekke innhold på Kortet.

7.1.2 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. Se vedlegg 2 for en mal på hvordan et slikt samtykke kan innhentes.

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

7.1.3 Direkte markedsføring i eksisterende kundeforhold

I henhold til markedsføringsloven § 15, tredje ledd, er det adgang til direkte markedsføring overfor registrerte Kunder, dersom ikke Kunden på forhånd eller ved mottagelse av tilbud og informasjon reserverer seg mot dette. Kunden skal ved innsamling og ved hver henvendelse gis en mulighet til enkelt å reservere seg.

7.1.4 Billettkontroll – ivareta en berettiget interesse

Kunder som ikke kan fremvise Gyldig billett, skal med hjemmel i yrkestransportloven § 33 og Virksomhetenes transportvedtekter betale tilleggsavgift.

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

7.1.5 Ivareta skoleskyss

Skoleskyss er en rettighet for skoleelever på vilkår som er omhandlet i opplæringsloven kapittel 7. Den enkelte fylkeskommune delegerer i noen tilfelle myndighet til sitt administrasjonsselskap noe som forutsetter inngåelse av en Databehandleravtale. Dersom slik avtale er inngått er Behandlingen av sensitive opplysninger om helseforhold unntatt konsesjonsplikt etter pol § 33, fjerde ledd, da Behandlingen har hjemmel i opplæringslovens kapittel 7.

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

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

7.1.6 Andre formål

Personopplysninger som samles inn til bruk for de ovennevnte formål kan ikke benyttes til andre formål uten særskilt hjemmel, jf. pol §11, første ledd.

7.2 Saklige formål

Behandling av Personopplysninger i kollektivbransjen kan kun iverksettes for å oppnå formål som etter pol §11, første ledd, bokstav b) anses som saklige i forhold til virksomheten som drives.

Alle formål som er angitt ovenfor, og i Vedlegg 1, anses som saklige i forhold til den virksomhet bransjen driver.

7.3 Relevante opplysninger

De opplysningstyper som benyttes i Behandlingen må være relevant for å oppnå det aktuelle formål, jf. pol §11, første ledd bokstav d.

De opplysningstypene som er beskrevet i tilknytting til det enkelte formål i Vedlegg 1, anses relevante for den aktuelle Behandlingen.

Behandling av Kortnummeret anses relevant for oppnåelse av de aller fleste formål som er angitt i bransjenormens punkt 7.1.1, fjerde avsnitt og i Vedlegg 1. For Behandling av Personopplysninger om Kunder som har inngått avtale om Reisekonto, anses også Behandling av Reisekonto som relevant for oppfølgning av bruken av en slik Reisekonto.

Behandling av fødselsnummer anses som relevant for å utøve offentlig myndighet etter beskrivelsen i bransjenormens punkt 7.1.5, jf. pol § 12. Av samme grunn anses helseopplysninger som relevante så langt disse er nødvendige for å innvilge skyss etter medisinske grunner etter opplæringslovens kapittel 7.

Virksomhetene som omfattes av denne normen er forpliktet til ikke å igangsette Behandling av andre opplysningstyper til andre formål uten at dette er på forhånd er vurdert og godkjent i henhold til endringsregimet i Bransjenormen, jf punkt 10.

7.4 Lagring og sletting av personopplysninger

Opplysninger som ikke lenger er nødvendig skal slettes. Sletting av Reiseopplysninger kan skje ved at alle Reiseopplysninger slettes fysisk, eller ved at Kortnummeret slettes/erstattes på en irreversibel måte. Reiseopplysninger skal uansett anonymiseres/slettes etter 104 dager.
Kundeopplysninger kan lagres så lenge Kunden har et kundeforhold til Virksomheten. Dersom Kunden trekker sitt samtykke tilbake, skal ikke Kortet sperres/leveres inn før Gyldig billett på Kortet er utgått/brukt opp. I tilfeller hvor Kunden trekker sitt samtykke tilbake og enten har levert inn Kortet eller får Kortet avpersonalisert, skal Kundeopplysningene deretter slettes senest 14 dager etter at avtaleforholdet er avsluttet. Kunden må få tydelig informasjon om hvordan dette kan gjøres.

Opplysninger som er nødvendige for fakturerings- eller arkivformål følger særlige regler, se Vedlegg 5. [Dette vedlegget opprettes etter at spørsmål om lagring iht. Bokføringslovgivningen er utredet.]

For å sikre at de nevnte slettefristene overholdes, skal alle Virksomheter ha rutiner for sletting av opplysninger i alle databaser og filer hvor Personopplysninger lagres. Dokumenter inneholdende Personopplysninger skal sikkerhetsmakuleres på forsvarlig måte.

Status med hensyn til sletting av unødvendige Personopplysninger skal være gjenstand for beskrivelse i en årlig gjennomgang av informasjonssikkerheten med sikte på ledelsesmessig vurdering av sikkerhetsmål og strategi, jf. personopplysnings-forskriften § 2-3.

7.5 Tilgang til personopplysninger

Kun ansatte hos Virksomhetene som har tjenestelig 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.

7.6 Avregning mellom virksomheter

Enkelte Virksomheter har etablert løsninger der den reisende kan benytte seg av et reiseprodukt utstedt av et 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 og tilhørende bruk, og at det blir inngått en Databehandleravtale med selskapet som gjennomfører avregningen.

7.7 Utlevering av personopplysninger til andre enn kunden

7.7.1 Hovedregel

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

7.7.2 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.

7.8 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.

Databehandleravtalen skal minimum angi formålet med - og grunnlaget for Behandlingen, beskrive hvordan opplysningene skal behandles, regulere bruk av underleverandører, sikre rettighetene til den opplysningene omhandler, samt pålegge leverandøren å ha tilfredsstillende informasjonssikkerhet. Vedlegg 3 beskriver hvordan Databehandleravtaler kan utformes og følges opp.

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

7.9 Bruk av nye løsninger og ny teknologi

Det kommer stadig nye løsninger og teknologi som kan bidra til å forbedre kollektivtrafikken. Bruk av ny teknologi eller nye løsninger skal vurderes opp mot prinsippene i normen både ut fra personvernkonsekvenser og informasjonssikkerhets-spørsmål. Vurderingene skal gjennomgås av Arbeidsgruppen som grunnlag for en revisjon av normen, jf punkt 10.

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 nedenstående krav og samtidig ta hensyn til personvern allerede i designfasen av nye produkter og tjenester slik at bruken av personopplysninger minimaliseres (privacy by design).

7.9.1 Særlig om internettløsninger

Internett er en stadig mer brukt kanal for å tilby ulike tjenester. Ved bruk av Internett, skal Virksomheten sikre at de løsninger som blir utviklet ivaretar kravet om anonymitet, se punkt 5.

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.

Kortvarig logging av IP-adresser av sikkerhetsårsaker anses ikke som en trussel mot anonymitet, jf. personopplysningsforskriften § 7-11 og § 2-16.

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

Kunder som ønsker anonymitet skal ikke uforvarende kunne skrive inn identifiserende opplysninger som for eksempel navn, telefonnummer eller e-postadresse i tekstfelt på ”Min Side” ved kjøp eller administrasjon av Anonyme produkter. Det skal legges til rette for at Kunder som ønsker anonymitet, ikke ved en feiltakelse selv undergraver sin anonymitet.

7.9.2 Særlig om mobilbillettering

Applikasjonsløsninger

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. Denne informasjonen skal både være tilgjengelig der applikasjonen lastes ned og i selve applikasjonen.

7.9.3 Betalingsløsninger

Ved bruk av betalingsløsninger over Internett, skal det legges til rette for at det ikke behandles Personopplysninger i de tilfeller anonymitet kreves, jf. punkt 5.

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

I de tilfeller hvor betalingen ikke er separert fra billetteringssystemet, skal Personopplysninger filtreres bort så fort transaksjonen er gjennomført.

7.9.4 Bruk av e-post og mobiltelefonnummer

E-postadresse kan benyttes som identifikator i anonyme løsninger, men Virksomheten bør 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 Informasjonssikkerhet

8.1 Grunnleggende krav

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

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.

8.2 Avvik

Avvik skal registreres og iverksatte tiltak skal dokumenteres.

Dersom avvik har medført uautorisert utlevering av Personopplysninger hvor konfidensialitet er nødvendig, skal Datatilsynet varsles.

8.3 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.

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

8.4 Internkontrollsystem

Videre utforming av dokumentasjon og system for internkontroll avhenger av de faktiske forhold i den enkelte Virksomhet. Regler om dette finnes i personopplysnings-forskriftens kapittel 2. Vedlegg 4 angir en veileder for hvordan internkontrollsystemet kan bygges opp. Virksomhetens personvernombud skal engasjeres i arbeidet med internkontrollsystem.

9 Etterlevelse og kontroll

Den enkelte Virksomhet er selv ansvarlig for å oppfylle normens bestemmelser. Datatilsynet legger normen til grunn ved tilsyn og kontroll med Virksomheter som skal følge normen.

10 Oppdatering og endring av bransjenormen

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 formaliseres deretter som endring til bransjenormen av Datatilsynet iht. reglene i pol § 42, tredje ledd nr. 6.

10.2 Styringsgruppen

Styringsgruppen består minimum av følgende deltakere: én deltaker fra Statens vegvesen Vegdirektoratet, én deltaker fra Datatilsynet, deltakere utpekt av Kollektivtrafikkforeningen, én representant fra samferdselssjefskollegiet, én deltaker fra Ruter, én deltaker fra NSB, én deltaker fra AtB, én deltaker fra Skyss og én deltaker fra Interoperabilitetstjenester AS.

Etter behov kan styringsgruppen selv utnevne andre deltakere til å delta i gruppen.

Avgjørelser i styringsgruppen skal tilstrebes å treffes enstemmig.

10.3 Arbeidsgruppen

Arbeidsgruppen består minimum av følgende deltakere: én deltaker fra Statens vegvesen Vegdirektoratet, én jurist og én ingeniør fra Datatilsynet, deltakere utpekt av Kollektivtrafikkforeningen, én deltaker fra Ruter, én deltaker fra NSB, én deltaker fra AtB, én deltaker fra Skyss, én deltaker fra Vestviken kollektivtrafikk AS, én deltaker fra Oppland fylkeskommune og én deltaker fra Interoperabilitetstjenester AS.

Dersom mange Virksomheter har personvernombud, skal Statens vegvesen Vegdirektoratet utpeke minst tre personvernombud som skal delta i arbeidsgruppen.

Etter behov kan også andre deltakere utnevnes til å delta i arbeidsgruppen.

Avgjørelser i arbeidsgruppen skal tilstrebes å treffes enstemmig.

10.4 Møter

Arbeidsgruppen møtes minimum én gang i året for å diskutere oppfølgningen av bransjenormen og behovet for oppdateringer. Statens vegvesen Vegdirektoratet innkaller til slike møter.

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

11 Ikrafttredelse og overgangsordninger

Bransjenormen trer i kraft 1. juni 2012.

Ved saklig behov i den enkelte Virksomhet for tekniske tilpasninger og/eller finansiering av nye løsninger for å overholde normen, kan Datatilsynet innvilge en overgangsperiode under følgende forutsetninger:

- det skal legges frem en fremdriftsplan som viser hvilke forhold Virksomheten arbeider aktivt med å utbedre, slik at bransjenormens krav overholdes – og

- fremdriftsplanen skal klart vise hvilken fremdrift og tiltak som er planlagt for å overholde bransjenormens krav, samt hvor lang overgangsperioden må være.

Noen Virksomheter tilbyr foreløpig kun Personlige billetter. Disse skal i sin eventuelle overgangsperiode tilby minst ett produkt som i størst mulig grad oppfyller kriteriet om anonymitet og lik pris, jf. punkt 5.

12 Definisjoner

12.1 Juridisk

Anonyme opplysninger: Opplysninger der navn, fødselsnummer og andre personentydige 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.

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

Behandlingsgrunnlag: Rettslig grunnlag 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.

Den Registrerte: Den som en Personopplysning kan knyttes til.

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

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

Håndbok 206: Veileder/standard for elektronisk billettering som alle som har fått konsesjon for å drive offentlig transport etter yrkestransportloven er pliktig til å følge.

12.2 Roller

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

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.

Kortutsteder: Virksomheten som har utstedt Kortet.

Produkteier: Et selskap eller institusjon som definerer alle produkter som Produkteier skal tilby Kundene. Produkteier er Kundens avtalepart, og også ansvarlig for Tjenesteytere som har akseptert Produkteiers reisebevis som et dokument som gir rett til en transporttjeneste for Kunden.

Tjenesteyter/transportør: Det selskapet som transporterer Kunden.

12.3 Billetter og kort

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.

Billett: Dokumentasjon av reiseretten/avtalen om kollektivtransport med Kunden lagret på en billettbærer.

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 den enkelte Virksomhets reisevilkår.

Kort: En billettbærer som kan inneholde Billetter og Reisepenger.

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

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 lagres på et Personlig kort og som kun kan benyttes av den Billetten er utstedt til.

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

Reisekonto: En konto som lagres sentralt hos Virksomheten hvor kontoen belastes iht. avtale hver gang en Kunde bruker kontoen til å betale for en Billett.

Reisekontonummer: Avtalenummer for en Reisekonto lagret på Kortet.

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

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

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

12.4 Handlinger med kortet/utstyr

Aktivere billetten: Igangsette en Billett som ligger i Kortet.

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

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

Fornye Billett: Kjøpe ny Billett av samme type.

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 kollektivreise 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.

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

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

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

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