KOLLEKTIVTRAFIKK-
FORENINGEN

Jernbanedirektoratet
post@jernbanedirektoratet.no

REF: OVS
Dato: 01.02.2019

HØRINGSSVAR ATFERDSNORM FOR PERSONVERN OG INFORMASJONSSIKKERHET I KOLLEKTIVTRAFIKKEN

Kollektivtrafikk og mobilitetstjenester tilbys i stadig større grad gjennom digitale tjenester, og ved hjelp av flere aktører. Det gir store muligheter til å utvikle bedre, og mer kundetilpassede tjenester, men det gir også utfordringer knyttet til personvern og informasjonssikkerhet. Kollektivtrafikkforeningen setter derfor stor pris på arbeidet som har blitt gjort for å utvikle en atferdsnorm for personvern. Det vil gjøre det lettere å tilby gode tjenester for aktørene i bransjen – på en måte som ivaretar kundenes data på en trygg måte.

En overordnet problemstilling gjelder hensynet til anonyme reisende og deres rett til å ettergå reise- og kjøpsinformasjon. Anonyme reisende har ikke like rettigheter som registrerte i gjeldende regelverk, og aktørene har således ingen plikt til å gi innsyn i opplysninger, rette eller slette opplysninger eller begrense behandlingen av opplysningene. Unntaket er når det er mulig å gjøre en sikker kobling mellom opplysningene og individet som gjør henvendelsen. For å sikre at den som får utlevert opplysninger faktisk er eier av opplysningene – bør det anbefales å ta i bruk flere faktorer for å identifisere riktig person (f.eks kvittering – bankutskrift – ID). På den måten vil man ivareta informasjonssikkerheten til anonyme reisende, samtidig som man kan yte samme tjenester ovenfor uregistrerte kunde som for registrerte (se mer om denne problemstillingen i vedlagt notat fra Atb AS).

Videre har Kollektivtrafikkforeningen har følgende innspill til utkastet – sortert etter kapittelnummer.

1. Det henvises til gammel personopplysningslov. Ny henvisning skal være: "lov om behandling av personopplysninger av 15.6.2018 nr. 38 (pol.)"

4.1 Dette ikke er en uttømmende liste over behandlingsgrunnlag. En bør enten gjøre listen uttømmende eller spesifisere at den ikke er det.

4.1.1 Bør omformuleres for å være mer spesifikk for det behandlingsgrunnlaget som omtales. Forslag: "...nødvendig for å oppfylle avtalen".

4.1.2 Setningen «*Eksempelvis kan ikke et samtykke til å få bedre kundeservice*» bør omformuleres,

GDPR art. 7 (1) sier at den Behandlingsansvarlige skal kunne «påvise» at den registrerte har samtykket. Dette peker dithen at samtykke bør gis skriftlig. Et samtykke er bare gyldig hvis det kan dokumenteres.

4.1.5.1 Her bør det anbefales at kunden må gi positivt samtykke. Dette medfører at et forhåndsavkrysset felt eller et vilkår i en kontrakt ikke er tilstrekkelig til at det skal kunne sies å foreligge et gyldig samtykke.

Det er i tråd med både Forbrukertilsynets anbefaling, og GDPR fortale, premiss 32: «Taushet, forhåndsavkryssede bokser eller inaktivitet bør derfor ikke utgjøre et samtykke.»

4.2.1 Stryk ordet registrert i første avsnitt. Det holder å si «Et kort som ikke er registrert…»

4.2.2 Her bør det vurderes å bruke «produkt» i stedet for «Billett» i andre linje.

Videre er det kanskje mer presist å si at det er kontobasert betaling som skal tilbys anonymt, og ikke nødvendigvis etterskuddsberegnet betaling.

4.2.5 F.eks. på grunn av elever som bor på hemmelig adresse, bør det åpnes opp for unntak fra dette punktet. En alternativ formulering kan derfor være: «*…kan som hovedregel ikke gjennomføres anonymt.*»

6.1 Setningen «At Kunden kan klage til Datatilsynet» kan f.eks. erstattes med «Informasjon om klageadgang til Datatilsynet» for å gjøres mer presis og fullstendig

6.2.1 (Under punkt «Virksomheter som er underlagt Offentleglova…») Her bør det også nevnes unntaket fra innsynsretten i POL §16 bokstav d som et praktisk eksempel: «I lov eller med hjemmel i lov er underlagt taushetsplikt».

Det er problematisk at det vises til at sladding kun er et alternativ og at det dermed åpner for at man utelukker/sletter tekst som kan unntas innsyn fra et dokument.
Det fremgår av offl § 13 første ledd at det kun er «opplysninger» og ikke hele dokumentet som kan unntas offentlighet. Det er heller ikke tillatt å fjerne linjer fra et dokument – og sladding der derfor eneste alternativ. I setningen «…annen informasjon kan f.eks. sladdes..» bør derfor ordet «f.eks.» fjernes.

Identifisering av anonyme kunder ved hjelp av QR-kode eller reisekort ivaretar ikke informasjonssikkerheten til anonyme reisende. Her bør det foreslås å i bruk flere faktorer for å identifisere riktig person (f.eks kvittering – bankutskrift – ID)

6.2.2 Forslag: «… skal sendes i henhold til gjeldende regulering og med hensyn til prinsipper for god informasjonssikkerhet».

6.2.4.1 («*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*».)

I følge GDPR art. 17 har den behandlingsansvarlige «*plikt til å slette personopplysninger uten ugrunnet opphold*» når et av forholdene i bokstav a) til f) gjør seg gjeldende. All forsinkelse må være saklig begrunnet. Kan det da være problematisk å operere med en frist på 14 dager? En kan også vurdere å benytte begrepet «uten ugrunnet opphold» gjennomgående, i stedet for «så raskt som mulig» eller andre tilsvarende begrep. Forslag: «… slettes/anonymiseres uten ugrunnet opphold fra det tidspunktet kundeforholdet er ferdig avsluttet».

Hva vil det si at kundeforholdet er avsluttet? Tar man her høyde for «sovende» kunder?

6.2.4.3 Det er kanskje unødvendig å ha med setningen «typisk lovgrunnlag», da det er andre grunner som kan være like typiske, og dette uansett må vurderes i hvert enkelt tilfelle.

DRONNINGENS GATE 40, POSTBOKS 1030 SENTRUM, N-0104 OSLO, ORG.NR: 891 502 052

6.2.6 Retten til begrensning av behandling er regulert i GDPR art. 18.

6.2.8.1 (Tredje avsnitt)
Nåværende formulering er noe upresis. Forslag til omformulering: "*I de tilfellene hvor det skal kreves inn et krav i forbindelse med billettkontroll vil behandlingsgrunnlaget oftest være berettiget interesse. I slike tilfeller vil en innsigelse mot at det foreligger en berettiget interesse sjelden føre frem til tross for innsigelser fra den registrerte.*"

(Fjerde avsnitt)
En presisering kan være: *"... for eksempel at det nevnes i et eget avsnitt i informasjonen gitt til den registrerte ved innsamling av opplysningene."*

6.2.8.2 (Siste avsnitt)
I GDPR art. 22 nr. 4. har vilkåret «...og det er innført egnede tiltak for å verne den registrertes rettigheter, friheter og berettigede interesser» en kumulativ sammenheng med de to vilkårene for unntak som nevnes i punkt 6.2.8.2. Dette vilkåret bør også inkluderes i den endelige atferdsnormen.

8.1 Også dynamiske IP-adresser har blitt regnet som personopplysninger i EU-domstolen. Setningen i tredje avsnitt bør derfor nyanseres noe. Forslag: Kortvarig logging av IP-adresser anses som akseptabelt.

Kollektivtrafikkforeningen håper disse innspillene blir tatt hensyn til i den endelige atferdsnormen for personvern og informasjonssikkerhet.

Med vennlig hilsen
Kollektivtrafikkforeningen

Ola Viken Stalund (sign.)

Rådgiver

DRONNINGENS GATE 40, POSTBOKS 1030 SENTRUM, N-0104 OSLO, ORG.NR: 891 502 052