Busstjenester Drammen og Lier 2024

Vedlegg 8
Databehandleravtale

Databehandleravtale

Basert på Vedlegg 3 til Bransjenorm for behandling av personopplysninger i elektronisk billettering (Bransjenormen)

Oppdatert av Brakar as i forhold til endringer etter EU forordning 2016/679 for behandling av personopplysninger (i kraft 25.5.2018) og i samsvar med gjeldende personvernlovgivning

Mellom

---

behandlingsansvarlig

Og

---

databehandler

Blå tekst i dokumentet er veiledende retningslinjer for hvordan den enkelte Virksomhet skal implementere denne delen av Bransjenormen og inngå Databehandleravtale med tredjepart.

Rød markerer felter hvor man skal beskrive mer.

1 AVTALENS HENSIKT

Avtalens regulerer rettigheter og plikter etter gjeldende personopplysningslov. Avtalen skal sikre at personopplysninger om den registrerte ikke brukes urettmessig eller kommer uberettigede i hende.

Avtalen regulerer databehandlerens bruk av personopplysninger på vegne av den behandlingsansvarlige – herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse.

Meddelelser etter denne avtalen skal sendes skriftlig til e-postadresse [e-postadresse].

2 DEFINISJONER

Det vises til definisjonene i hovedavtalen. I tillegg gjelder følgende definisjoner:

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.
Personopplysninger	Opplysninger og vurderinger som kan knyttes til en enkeltperson.
Behandling av personopplysninger	Enhver bruk av Personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

3 FORMÅL OG RETTSLIG GRUNNLAG

Databehandler skal kun behandle opplysninger som er i samsvar med formålet og for øvrig i samsvar med hovedavtalen.

Rettslig grunnlag for behandling av personopplysninger er kundens samtykke og/ eller at behandlingen er nødvendig følge opp en avtale med en kunde.

Følgende opplysninger kan behandles for å ivareta formålet:

Reisekort

Reiseopplysninger som billettype, sone og gyldighetsperiode.

Billetterings-«apper»

Billettyper og reisepenger, saldo/gjenstående periode, kjøpstidspunkt, hvilken sone billetten er gyldig.

I tillegg behandles relevante kundeopplysninger som navn, e-post og telefonnummer.

Behandling skal forøvrig være i samsvar med Behandlingsansvarliges interne rutiner og relevant instruks.

4 DEN BEHANDLINGSANSVARLIGES ROLLE

[Oppdragsgiver] er behandlingsansvarlig og bestemmer over bruken av opplysningene som omfattes av denne avtale i henhold til det som er avtalt med den enkelte kunde.

[Oppdragssgiver] er som behandlingsansvarlig bl.a. ansvarlig for at det foreligger et lovlig behandlingsgrunnlag for personopplysningene, og at den aktuelle behandling er i overensstemmelse med gjeldende lovgivning.

Med mindre annet følger av lov, har den behandlingsansvarlige rett til tilgang til og innsyn i både personopplysningene som behandles og i systemene som benyttes til dette formål. Databehandler plikter å gi nødvendig bistand til dette.

Den behandlingsansvarlige har også taushetsplikt om eventuelle virksomhetskritiske opplysninger han får tilgang til gjennom innsyn.

5 DATABEHANDLERENS PLIKTER

Databehandleren skal følge de skriftlige rutiner og instrukser for behandlingen som den behandlingsansvarlige til enhver tid har bestemt skal gjelde. Personopplysningene skal ikke benyttes på annen måte eller til annet formål enn det som er avtalt med den behandlingsansvarlige. Databehandler kan imidlertid behandle personopplysninger i samsvar på plikter nedfelt i lov eller forskrift.

Databehandleren er i tillegg ansvarlig for at egen behandling av personopplysninger er i samsvar med personvernlovgivningen, se nærmere under avsnitt 7.

Ny EU forordning om behandling av personopplysninger EU 2016/679 («GDPR» eller «forordningen») er gjort til norsk lov, se personopplysningsloven § 1. Etter forordningens artikkel 28 skal databehandler:

- Sørge for informasjonssikkerhet, herunder egnede tiltak, for egen behandling, jf. artikkel 32
- Varsle den behandlingsansvarlige om avvik uten unødvendig forsinkelse og bistå den behandlingsansvarlige, slik at den behandlingsansvarlige kan oppfylle sine plikter etter GDPR, jf. artikkel 33.
- Opprette personvernombud dersom man behandler personopplysninger i stor målestokk, eller dersom man behandler sensitive personopplysninger i stort omfang eller er offentlig virksomhet. jf. art 38.
- Yte nødvendig bistand til behandlingsansvarlig i oppfyllelsen av den registrertes rettigheter slik de er beskrevet i GDPR kapitel 3, herunder retten å kreve sletting, retting og innsyn i personopplysningene, retten til å kreve begrensning av en behandling og dataportabilitet mm.
- Underrette den behandlingsansvarlige dersom databehandler mener at instruksjonene de mottar er i strid med forordningen eller personvernrett for øvrig.

Databehandler har i tillegg ansvar for forsvarlig informasjonssikkerhet ved egen behandling og skal i tillegg bistå Behandlingsansvarlig med å sikre overholdelse av forpliktelsene i GDPR artiklene 32-36. Den behandlingsansvarlige har likevel hovedansvaret for behandlingen av personopplysninger

Brudd på disse pliktene kan føre til sanksjoner fra Datatilsynet, jf. GDPR artikkel 58 og fortalepunkt nr. 146.

Dersom brudd på reglene medfører tap for den registrerte, er databehandleren erstatningsansvarlig (solidaransvar) for skade som er forårsaket av at han ikke har oppfylt forpliktelser i denne forordningen, eller hvis han har handlet i strid med behandlingsansvarliges instruks for behandlingen.

Øvrige plikter for databehandler vil bli kartlagt i forbindelse med implementering av forordningen.

6 TAUSHETSPLIKT

Databehandleren og ansatte hos databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til iht. denne avtalen. Dette gjelder også etter avtalens eller ansettelsesforholdets opphør.

7 BRUK AV SKYTJENESTER

Databehandleren eller hans underleverandører kan ikke benytte «sky- tjenester» dersom dette kan medføre at personopplysninger behandles utenfor EU/EØS, uten at dette er særskilt godkjent av Behandlingsansvarlig.

Dette inkluderer lagring av personopplysninger på server utenfor EU/EØS og at noen av leverandørens eller underleverandørens ansatte kan få tilgang til system hvor det behandles personopplysninger. Tilsvarende gjelder for innlogging via skytjenester.

Spørsmål om behandling av personopplysninger i forbindelse med skytjenester skal tas opp med Behandlingsansvarlig senest tre måneder før oppstart av behandlingen og skal baseres på EUs modellavtale for behandling av personopplysninger utenfor EU/EØS. Særlige kategorier av personopplysninger kan uansett ikke behandles utenfor EU/EØS.

Databehandler skal legge frem en risikovurdering som er tilpasset den tjenesten som tilbys Behandlingsansvarlig.

8 BRUK AV UNDERLEVERANDØRER

Behandlingsansvarlig skal skriftlig godkjenne Databehandlers eventuelle bruk og bytte av underleverandører før behandlingen av personopplysninger starter. Underleverandører som er godkjent ved oppstart av avtalen skal beskrives i vedlegg.

Underleverandøren skal være kjent med databehandlerens avtalemessige og lovmessige forpliktelser, og oppfylle disse på lik linje med databehandleren. Databehandler skal sørge for at underleverandører pålegges de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i denne databehandleravtalen. Dette skal gjøres ved hjelp av en egen avtale, der det særlig gis tilstrekkelige garantier for at det vil bli gjennomført egnede tiltak som sikrer at behandlingen oppfyller kravene i GDPR.

En oversikt over underleverandører som ved avtaleinngåelsen - eller på et senere tidspunkt - skal behandle personopplysninger vedlegges databehandleravtalen.

9 INFORMASJONSSIKKERHET

Databehandleren skal oppfylle de krav til sikkerhetstiltak som stilles i henhold til personopplysningsloven, herunder GDPR, og annen relevant lovgivning.

Databehandler skal ha en dokumentert autorisasjonsordninger for ansatte hos Databehandleren som skal få tilgang til å behandle personopplysninger.

For å oppfylle disse kravene, har Databehandleren en plikt til å dokumentere sine sikkerhetsrutiner. Dokumentasjonen skal gjøres tilgjengelig for den behandlings-ansvarlige.

Databehandleren må sørge for å ha forsvarlig sikring av servere, databaser og annet tilsvarende utstyr slik at ingen uvedkommende kan få tilgang til personopplysninger. Det samme gjelder utskrifter og utfylte skjemaer.

Databehandleren skal videre ha et styringssystem for sikkerhet. Systemet skal omfatte – men ikke avgrenses til rutiner for:

- Avviksbehandling som omfatter varsling ved feil bruk av informasjonssystemet, herunder sikkerhetsbrudd;
- Sikkerhetsrevisjon, herunder jevnlig oversendelse av rapporter fra sikkerhetsrevisjoner;
- Ledelsens gjennomgang av sikkerhetsarbeidet, samt
- Gjennomføring av årlige revisjoner av virksomheten;

Databehandleren skal etablere og holde en oversikt over sikkerhetstiltak som risikovurderinger har avdekket behov for.

Databehandleren skal også bistå behandlingsansvarlig slik at han kan ivareta sitt eget ansvar etter lov og forskrift bl.a. ved;

- Informasjon om nye momenter som har betydning for å vurdere personvernrisikoen for tjenesten.
- Bistå behandlingsansvarlig med bl.a. tekniske data og fakta om tjenesten ved utarbeidelse av nødvendig konsekvensanalyse og risikovurdering.
- Informasjonsutveksling med Behandlingsansvarlig om nye lover og regler, praksis og annet som kan ha betydning for å oppfylle krav til god informasjonssikkerhet.

Avviksmelding skal skje ved at databehandleren uten unødvendig opphold melder avviket til den behandlingsansvarlige. Den behandlingsansvarlige har ansvaret for at avviksmelding sendes Datatilsynet.

10 SIKKERHETSREVISJONER

Den behandlingsansvarlige skal jevnlig gjennomføre sikkerhetsrevisjoner av databehandleren. Revisjonen kan bl.a. omfatte gjennomgang av rutiner, stikkprøvekontroller, mer omfattende stedlige kontroller og andre egnede kontrolltiltak. Behandlingsansvarlig kan også benytte revisorer på fullmakt fra den behandlingsansvarlige.

Databehandler plikter å muliggjøre, bidra til, og bistå den behandlingsansvarlig ved slike revisjoner, og gjøre nødvendig informasjon tilgjengelig for å påvise at GDPR etterleves.

11 AVTALENS VARIGHET

Avtalen gjelder så lenge databehandleren behandler personopplysninger på vegne av den behandlingsansvarlige.

Ved brudd på denne avtale eller gjeldende personopplysningslov, kan den behandlingsansvarlige pålegge databehandleren å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning. Brudd på denne avtalen er å regne som mislighold av hovedavtalen.

12 TILBAKEFØRING VED OPPHØR

Ved opphør av denne avtalen plikter databehandleren å tilbakelevere alle personopplysninger som er mottatt på vegne av den behandlingsansvarlige, og som omfattes av denne avtalen.

Ved opphør av avtalen skal databehandleren også slette eller forsvarlig destruere alle kopier av personopplysninger, herunder dokumenter, data, disketter, cd-er, minnepinner/ USB sticks og annet som inneholder opplysninger som omfattes av avtalen. Dette gjelder også for eventuelle sikkerhetskopier. Databehandleren skal skriftlig dokumentere at sletting og eller destruksjon er foretatt i henhold til avtalen innen rimelig tid etter avtalens opphør.

Databehandleren skal uansett lagre dokumentasjon på sikkerhetsrutiner i minst 5 år fra det tidspunkt dokumentet ble erstattet med ny gjeldende utgave, og databehandleren må i lagringstiden bistå den behandlingsansvarlige med å fremskaffe slik dokumentasjon.

13 LOVVALG OG VERNETING

Avtalen er underlagt norsk rett og partene vedtar Drammen tingrett som verneting. Dette gjelder også etter opphør av avtalen.

14 SIGNERING

Sted/dato: _____

For behandlingsansvarlig

_____
xx
adm.dir.

Sted/dato: _____

For databehandler

_____
xx
adm.dir.