Vedlegg 8 Avtale om behandling av personopplysninger

Avtale om behandling av personopplysninger

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

Oppdatert av Ruter etter krav i ny personopplysningslov og EU forordning 2016/679 for behandling av personopplysninger.

1. Avtalens hensikt

Avtalens hensikt er å regulere rettigheter og plikter etter gjeldende personopplysningslov og GDPR, innenfor rammen av kontrakten om transporttjenester Follo 2025 (hovedavtalen). Avtalen skal sikre at Personopplysninger om den registrerte ikke brukes urettmessig eller kommer uberettigede i hende.

Avtalen regulerer i hvilke tilfeller partene er henholdsvis Behandlingsansvarlig og Databehandler. I tillegg regulerer den Databehandlerens (Operatørens) bruk av Personopplysninger på vegne av den Behandlingsansvarlige (Ruter) – herunder innsamling, registrering, sammenstilling, lagring, videreformidling, utlevering eller kombinasjoner av disse.

Meddelelser etter denne Avtalen skal sendes skriftlig til:
personvernombud@ruter.no

Begreper i denne Avtale skal ha samme innhold som angitt i GDPR.

2. Definisjoner

I tillegg til definisjonene i hovedavtalen gjelder følgende definisjoner:

Begrep	Definisjon
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.
Behandlingsgrunnlag	Et grunnlag som gjør behandlingen av personopplysninger lovlig. Samtykke fra den registrerte (vedkommende personopplysningene handler om) er et praktisk behandlingsgrunnlag.

3. Roller

Ruter og Operatør har hver for seg selvstendig behandlingsansvar for oppfølgning av kundehenvendelser knyttet til personskader.

Operatøren er Behandlingsansvarlig for Personopplysninger om personskader som de får tilsendt enten fra kunden eller Ruter, mens Ruter er Behandlingsansvarlig for øvrige kundehenvendelser.

For Behandling av Personopplysninger på vegne av Ruter om andre kundehenvendelser enn skadetilfeller, er Operatøren Databehandler for Ruter. Der denne avtale bruker begrepet "Databehandler", siktes til Operatøren.

Den Behandlingsansvarlige bestemmer over behandlingen av opplysningene som omfattes av denne Avtale, i henhold til det som er avtalt med den enkelte kunde.

Den som er Behandlingsansvarlig er bl.a. ansvarlig for at det foreligger et lovlig Behandlingsgrunnlag, og at den aktuelle behandling er i overensstemmelse med gjeldende lovgivning.

Hver Behandlingsansvarlig skal sørge for tilstrekkelig interne rutiner og dokumentasjon om Behandlingen, nødvendig informasjon om behandling og gjennomfører eventuelle risikovurderinger og DPIA.

4. Formål og rettslig grunnlag

4.1 Innledning

Databehandler skal kun behandle Personopplysninger som er i samsvar med formålet med behandlingen, på den måten som er angitt i denne avtale, og for øvrig i samsvar med hovedavtalen.

4.2 Formålet med behandlingen

Formålet med behandlingen når partene er selvstendig behandlingsansvarlige, er:

Personopplysninger som nevnt i denne Avtale behandles for å kunne følge opp henvendelser og Behandling av Personopplysninger i forbindelse med skadesaker fra kunden.

For henvendelser og Behandling av Personopplysninger i forbindelse med skadesaker vil Operatør/forsikringsselskap og Ruter ha selvstendig Behandlingsansvar hver for seg.

For personskader er Operatøren Behandlingsansvarlig for egen behandling av saker som blir oversendt av Ruter, eller av kunden direkte, og skal selv sørge for overholdelse av kravene i personopplysnings - loven og GDPR.

Operatør skal likevel gi Ruter tilbakemelding om status i slike saker og rapportere på antall saker og hvordan de ble løst.

Formålet med behandlingen når Operatøren er databehandler:

Personopplysninger som nevnt i Avtalen behandles for å kunne følge opp henvendelser og Behandling av Personopplysninger i forbindelse med kundeklager og materiell skade.

Kameraovervåking

Kameraovervåking benyttes for at passasjer skal ha en så trygg og sikker reise som mulig. I tillegg skal overvåking gi fører sikkerhet ved utførelse av tjenesten.

Ruter er Behandlingsansvarlig, men Operatør skal som Databehandler være ansvarlig for at drift og installasjon er i samsvar med relevante lovkrav, herunder krav til informasjonssikkerhet, se krav i Vedlegg 2 punkt 5.4

4.3 Behandlingsmåter

Behandlingen kan foregå ved transportering, innsamling, registrering, lesing, oppslag, bearbeiding i form av nødvendig tillegg i en sak, lagring, sletting og utlevering til Behandlingsansvarlig, og hvis nødvendig også gjennom kobling av opplysninger og/eller data.

Opplysningene skal ikke lagres for fremtidig bruk i arkivinstans.

Personopplysningene kan ikke benyttes for Databehandlers formål.

4.4 Rettslig grunnlag for behandlingen

Behandlingsansvarlig bekrefter at Behandlingsansvarlig har tilstrekkelig hjemmelsgrunnlag for Behandling av Personopplysninger, og har rett til, og ansvaret for lovligheten av, overføring av personopplysningene til Databehandler. Rettslig grunnlag er beskrevet på ruter.no/personvern.

Aktuelt grunnlag for Behandling av Personopplysninger i denne avtale er kundens samtykke, eller at behandlingen er nødvendig for å følge opp transportavtalen med kunden.

Når Ruter overfører Personopplysninger til Operatør som selvstendig Behandlingsansvarlig i forbindelse med skadesaker, er det rettslige grunnlaget at dette er nødvendig for å fremme kundens rettskrav om erstatning/ oppfylle den Behandlingsansvarlige rettslige forpliktelser.

4.5 Kategorier av Personopplysninger som behandles

4.5.1 Kundeopplysninger

Kundeopplysninger er for eksempel navn, fødselsnummer, adresse, postadresse, telefonnummer, e-postadresse, kortnummer og status kort.

4.5.2 Reiseopplysninger

Reiseopplysninger er informasjon om tid og sted for transporten, inklusive informasjon om hentested og leveringssted.

4.5.3 Kameraovervåking

Opptak som viser passasjerer og/ eller sjåfør.

4.5.4 Særlige personopplysningskategorier

Det behandles særlige kategorier av Personopplysninger i skadesaker.

4.5.5 Tidsavgrenset behandling

Behandling av personopplysningene skal opphøre etter instruks fra Behandlingsansvarlig, og i samsvar med gjeldende lovverk.

4.5.6 Sletting eller anonymisering av data som kan knyttes til en person

Fortløpende sletting, eller anonymisering, av Personopplysninger skal gjennomføres dersom opplysningene ikke lenger er nødvendig for å oppfylle formålet, og såfremt det ikke foreligger en plikt til oppbevaring i lovgivningen. En eventuell oppbevaringsplikt skal i tilfelle dokumenteres overfor Behandlingsansvarlig.

Kameraovervåkingsbilder skal slettes når det ikke er nødvendig lenger og senest etter en uke. Hvis det er sannsynlig at opptaket vil bli utlevert til politiet i forbindelse med etterforskning av straffbare handlinger eller ulykker, kan opptakene oppbevares inntil 30 dager.

5. Den Behandlingsansvarliges rolle

Den Behandlingsansvarlige beslutter behandlingen av opplysningene som omfattes av denne avtale, i henhold til det som er avtalt med den enkelte kunde.

Behandlingsansvarlig bl.a. ansvarlig for at det foreligger et lovlig Behandlingsgrunnlag for personopplysningene, og at den aktuelle behandling er i overensstemmelse med gjeldende lovgivning.

Den Behandlingsansvarlige skal sørge for tilstrekkelig interne rutiner og dokumentasjon om behandlingen, nødvendig informasjon om behandlingen, og gjennomfører risikovurdering og DPIA.

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.

6. Databehandlerens plikter

Databehandleren skal følge de rutiner og instrukser for behandlingen som den Behandlingsansvarlige til enhver tid har besluttet at skal gjelde.

Det skal ikke behandles andre Personopplysninger enn det som er beskrevet i denne avtalen.

Dersom ikke annet er avtalt skal personopplysningene ikke benyttes til andre formål enn det som er beskrevet i denne avtalen.

Databehandleren er i tillegg ansvarlig for at egen Behandling av Personopplysninger er i samsvar med personvernlovgivningen.

Databehandler er ansvarlig for å oppfylle pliktene i EU forordning 2016/679 for Behandling av Personopplysninger. Dette innebærer, men er ikke avgrenset til:

- Varsle den Behandlingsansvarlige om avvik uten unødvendig forsinkelse slik at Behandlingsansvarlig kan oppfylle fristen til å varsle Datatilsynet innen 72 timer 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 37 og 38.
- Yte nødvendig bistand til Behandlingsansvarlig i oppfyllelsen av den registrertes rettigheter slik de er beskrevet i GDPR kapitel 3, herunder retten til å kreve sletting, retting og innsyn i personopplysningene, retten til å kreve begrensning av en behandling og dataportabilitet mm. Bistandstimeprisen som beskrevet i hovedavtalen skal benyttes.
- Underrette den Behandlingsansvarlige dersom de mener at instruksjonene de mottar er i strid med forordningen eller personvernretten for øvrig.
- Å ivareta forsvarlig informasjonssikkerhet ved egen behandling, jf. GDPR art 32.
- Brudd på pliktene kan føre til sanksjoner fra Datatilsynet, jf. artikkel 58 og fortalen nr.146.
- Dersom brudd på personopplysningsloven og GDPR 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.

7. Taushetsplikt

Databehandleren har taushetsplikt om dokumentasjon og Personopplysninger som vedkommende får tilgang til i henhold til denne avtalen. Dette gjelder også etter avtalens eller ansettelsesforholdets eller tjenesteforholdets opphør.

8. Bruk av skytjenester – overføring av opplysninger til land utenfor EUØ/EØS

Databehandleren eller hans underleverandører kan ikke benytte skytjenester dersom dette kan medføre at Personopplysninger behandles utenfor EU/EØS, uten at dette er særskilt godkjent av Behandlingsansvarlig. Tilsvarende gjelder annen Behandling av Personopplysninger som innebærer overføring av Personopplysninger til mottakerland utenfor EU/EØS.

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 uansett tas opp med Behandlingsansvarlig senest tre måneder før planlagt oppstart av behandlingen. Sensitive Personopplysninger kan uansett ikke behandles utenfor EU/EØS.

Behandling av Personopplysninger utenfor EU/EØS skal i alle tilfelle baseres på et gyldig utleveringsgrunnlag i samsvar med GDPR og praksis, og i tillegg nødvendig tiltak, vurdert utfra beskyttelsesnivået i lov og praksis i mottakerlandet. Vurderingen skal gjøres i samsvar med retningslinjer fra EDPB.

I tilfeller hvor Operatøren er Behandlingsansvarlig skal Ruter likevel informeres om slik behandling og hvilke tiltak som er gjennomført etter GDPR art 46.

9. Bruk av underleverandør

Behandlingsansvarlig skal godkjenne Databehandlers eventuelle bruk av underleverandører før behandlingen av Personopplysninger starter.

Underleverandøren skal være kjent med Databehandlerens avtalemessige og lovmessige forpliktelser, og oppfylle disse på lik linje med Databehandleren.

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

Databehandler er ansvarlig overfor Behandlingsansvarlig for avtalebrudd som eventuelle underleverandører til tjenesten gjør seg skyldig i.

10. Informasjonssikkerhet

Partene skal oppfylle de krav til sikkerhetstiltak som stilles etter gjeldende personopplysningslov og GDPR art 32.

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 Behandlingsansvarlige.

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 ha et styringssystem. Systemet skal omfatte, men ikke avgrenses til, rutiner for:

- Tilgangskontroll
- Avviksbehandling som omfatter varsling ved feil bruk av informasjonssystemet, herunder sikkerhetsbrudd.
- Sikkerhetsrevisjon, herunder jevnlig oversendelse av rapporter fra sikkerhetsrevisjoner.
- Ledelsens gjennomgang av sikkerhetsarbeidet.
- Gjennomføring av årlige revisjoner av virksomheten.
- Dokumentasjon av relevante hendelser

- 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 blant annet ved:
- Varsling av avvik, jf. Punkt 6.
- Informasjon om nye momenter som har betydning for å vurdere personvernrisikoen for tjenesten.
- Bistå Behandlingsansvarlig med blant 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.
- Den Behandlingsansvarlige har ansvaret for at avviksmelding sendes Datatilsynet.

11. Sikkerhetsrevisjoner

Den Behandlingsansvarlige skal kunne gjennomføre sikkerhetsrevisjoner av Databehandleren. Revisjonen kan omfatte gjennomgang av rutiner, stikkprøvekontroller, mer omfattende stedlige kontroller og andre egnede kontrolltiltak.

Databehandler plikter å bistå den Behandlingsansvarlig ved slike revisjoner og gjøre nødvendig dokumentasjon tilgjengelig. Bistandstimepris som beskrevet i hovedavtalen skal benyttes.

12. Avtalens varighet og endringer

Avtalen gjelder så lenge Databehandleren behandler Personopplysninger på vegne av den Behandlingsansvarlige. Dette tidspunktet vil i praksis være knyttet til hovedavtalens utløp.

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.

Eventuelle endringer til denne avtalen skal beskrives i bilag 3, Endringer.

13. Tilbakeføring ved opphør

Ved opphør av hovedavtalen 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 deretter endelig slette eller forsvarlig destruere alle dokumenter, data, disketter, lagringstape, cd'er, minnepinner/USB-sticks og annet som inneholder Personopplysninger 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 uansatt 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.

14. Lovvalg og verneting

Avtalen er underlagt norsk rett og følger vernetingsbestemmelsene i hovedavtalen.