Vedlegg 4

08.07.2022

Versjon: 0.1

UTKAST Databehandleravtale

Minibuss- og personbiltjenester Romerike 2024

Databehandleravtale

Mellom

Ruter As
Behandlingsansvarlig

Og

……[Leverandør]……
Databehandler

Innhold

Avtalens hensikt:

Avtalens hensikt er å sørge for at databehandler behandler personopplysninger basert på den behandlingsansvarliges instrukser i henhold til denne avtalen og gjeldende personopplysningslov og personvernforordning (GDPR), særlig GPDR artikkel 28. Avtalen skal sikre at Personopplysninger om den registrerte ikke brukes urettmessig eller kommer uberettigede i hende.

Avtalen regulerer Databehandlers behandling av Personopplysninger på vegne av den Behandlingsansvarlige – herunder innsamling, registrering, sammenstilling, lagring, videreformidling, utlevering eller kombinasjoner av disse.

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

1 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.

Behandlingsformål:
Angir hensikten med behandlingen av Personopplysninger. Databehandler skal utføre konkrete oppgaver (driftsformål) for å oppfylle behandlingsformålet.

Rettslig grunnlag (behandlingsgrunnlag):
Grunnlag som gjør behandlingen av Personopplysninger lovlig.

2 Behandlingsformål og Rettslig grunnlag

Databehandler skal kun behandle Personopplysninger som er i samsvar med formålet og for øvrig i samsvar med kontrakten inngått mellom partene om kontrakt om Minibuss- og personbiltjenester Romerike 2023.

Formålet med behandlingen er:

[Må fylles inn]

Personopplysningene kan ikke benyttes for Databehandlers formål, dersom ikke noe annet følger av denne avtale.

Beskrivelse av behandlingens art som Databehandler skal behandle på vegne av den Behandlingsansvarliges instrukser:

[Må fylles inn]

Rettslig grunnlag for behandlingen:

Behandlingsansvarlige bekrefter at Behandlingsansvarlig har tilstrekkelig hjemmelsgrunnlag for Behandling av Personopplysninger, og har rett til, og ansvaret for lovligheten av, overføring av personopplysningene til Databehandler.

[Må fylles inn]

Personopplysningskategorier:
Databehandler vil kunne få tilgang og behandle følgende personopplysningskategorier:

[Må fylles inn]

Kategorier av registrerte:

[Må fylles inn]

Tidsavgrenset behandling og sletteprosedyrer:

Sletting av personopplysningene skal skje i samsvar med Behandlingsansvarliges sletterutiner, eller etter Behandlingsansvarliges instruks, og i samsvar med gjeldende lovverk.

[Hvis man kan spesifisere behandlingstiden for personopplysningene må det fylles inn. Dette inkluderer behandlingstid for ulike personopplysningskategorier. Man kan tenke seg at det er nødvendig å behandle noen typer opplysninger lenge, mens andre kan slettes etter kort tid.]

[Fyll også inn: Varighet av selve databehandleravtalen fra start til slutt (sammenfaller normalt med kontrakten inngått mellom partene)]

Hvordan Databehandler skal oppfylle kravet til informasjonssikkerhet etter denne avtale:

[Må fylles inn]

3 Den Behandlingsansvarliges rolle

Behandlingsansvarlig bestemmer over behandlingen av Personopplysninger som omfattes av denne avtale.

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.

4 Databehandlerens plikter

Databehandler skal følge de rutiner og instrukser for behandlingen som den Behandlingsansvarlige til enhver tid har bestemt skal gjelde.

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

Databehandler er ansvarlig for å oppfylle følgende pliktene i EU forordning 2016/679 for Behandling av Personopplysninger (men ikke avgrenset til):

- Varsle Behandlingsansvarlig om avvik uten unødvendig forsinkelse, slik at Behandlingsansvarlig kan oppfylle fristen til å varsle Datatilsynet innen 72 timer, jf. artikkel 33.
- Yte nødvendig bistand ved avvik, slik at Behandlingsansvarlig kan overholde fristen til å varsle innen 72 timer, jf. GDPR artikkel 33.
- Bistå Behandlingsansvarlig med å underrette den registrerte i henhold til GDPR artikkel 34, dersom Behandlingsansvarlig ber om dette.
- 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.
- Underrette den Behandlingsansvarlige dersom man mener at instruksjonene man mottar er i strid med forordningen eller andre personvernregler.
- Ivareta forsvarlig informasjonssikkerhet ved egen behandling, jf. GDPR art 32, se under punkt 9.

I tillegg skal Databehandler bistå Behandlingsansvarlig i utarbeidelsen av DPIA etter GDPR art 35.

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

Dersom Behandlingsansvarlig blir erstatningsansvarlig overfor den registrerte, eller blir ilagt bøter, er Databehandler ansvarlig for tap som er forårsaket av at Databehandler ikke har oppfylt forpliktelser i denne forordningen - eller har handlet i strid med Behandlingsansvarliges instruks for behandlingen.

5 Taushetsplikt

Databehandler, hans ansatte og godkjente leverandører har taushetsplikt om dokumentasjon og Personopplysninger som vedkommende får tilgang til iht. denne avtalen. Dette gjelder også etter avtalens eller ansettelsesforholdets eller tjenesteforholdets opphør.

Behandlingsansvarlig skal beskytte fortrolig sikkerhets-, forretnings- og/eller kundeinformasjon som behandlingsansvarlig mottar fra databehandler og underleverandører eller som behandlingsansvarlig blir kjent med i forbindelse med gjennomføring av hovedavtalen. Behandlingsansvarlig skal ikke uberettiget utnytte, dele eller videreformidle slik taushetsbelagt informasjon.

6 Forbud mot overføring av personopplysninger til land utenfor EU/EØS

Databehandler eller Databehandlers underleverandører, skal ikke benytte skytjenester eller andre systemer som 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.

Dersom Behandlingsansvarlig gir slik godkjenning skal Databehandler sikre og dokumentere at det finnes gyldig Rettslig grunnlag for Behandling av Personopplysninger utenfor EU/EØS. Databehandler skal på forhånd sørge for nødvendig risikovurdering, som skal forelegges Behandlingsansvarlig til godkjennelse.

Sensitive Personopplysninger kan uansett ikke behandles utenfor EU/EØS uten kryptering.

Spørsmål om behandling av Personopplysninger i land utenfor EU/EØS skal uansett tas opp med Behandlingsansvarlig senest tre måneder før oppstart av Behandling av personopplysninger.

7 Bruk av underleverandør

Behandlingsansvarlig skal godkjenne Databehandlers eventuelle bruk av underleverandører før behandlingen av Personopplysninger starter. Underleverandører som er godkjent ved oppstart av avtalen skal vedlegges. Databehandler skal ikke engasjere en annen databehandler uten at det på forhånd er hentet inn skriftlig godkjennelse av Behandlingsansvarlig.

Underleverandøren skal være kjent med Databehandlers avtalemessige og lovmessige forpliktelser, og oppfylle disse på lik linje med Databehandler. Dette inkluderer at underleverandør pålegges de samme vilkårene som databehandleren har akseptert i denne databehandleravtalen gjennom en egen avtale.

En oversikt over underleverandører som ved avtaleinngåelsen - eller på et senere tidspunkt - skal behandle Personopplysninger vedlegges databehandleravtalen, jf. bilag 1 Oversikt over godkjente underleverandører.

Databehandler er ansvarlig overfor Behandlingsansvarlig for avtalebrudd som eventuelle underleverandører til tjenesten gjør seg skyldig i. Dersom en underleverandør ikke lenger kan benyttes, skal Databehandler sørge for at tjenesten fortsatt kan tilbys ved at man skaffer en ny underleverandør, eller alternativt utfører tjenesten selv.

8 Informasjonssikkerhet

Databehandler skal gjennom egnede organisatoriske og tekniske tiltak sørge for forsvarlig informasjonssikkerhet i sine systemer for Behandling av Personopplysninger og annen informasjon knyttet til oppdraget for Ruter. Behandlingsansvarlig kan kreve å få fremlagt gjennomførte risikovurderinger.

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

Databehandler skal ha dokumenterte autorisasjonsordninger for ansatte som skal få tilgang til å behandle Personopplysninger. Databehandler 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.

For å oppfylle disse kravene, har Databehandler plikt til å dokumentere sine sikkerhetsrutiner. Dokumentasjonen skal gjøres tilgjengelig for Behandlingsansvarlig.

Databehandler skal ha et styringssystem. Systemet skal omfatte, men skal 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.
- Gjennomføring av årlige revisjoner av virksomheten.

Avviksmelding skal skje ved at Databehandler uten unødvendig opphold melder avviket til Behandlingsansvarlig. Den Behandlingsansvarlige har ansvaret for at avviksmelding sendes Datatilsynet, dersom dette er påkrevet.

Databehandler skal bistå Behandlingsansvarlig slik at han kan ivareta sitt eget ansvar etter lov og forskrift bla ved:

- Varsling av avvik, jf. punkt 5
- 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.

Databehandler skal oppfylle øvrige krav til sikkerhetstiltak som stilles etter gjeldende personopplysningslov og GDPR art 32 og 33.

9 Sikkerhetsrevisjoner

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

Databehandler plikter å bistå Behandlingsansvarlig med slike revisjoner og gjøre nødvendig dokumentasjon tilgjengelig for å påvise at forpliktelsene etter GDPR er ivaretatt.

10 Avtalens varighet og endringer

Avtalen gjelder så lenge Databehandler behandler Personopplysninger på vegne av Behandlingsansvarlig.

Ved brudd på avtalen eller gjeldende personopplysningslov, kan den Behandlingsansvarlige pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning. Brudd på denne avtalen er å regne som mislighold av kontrakt om minibuss- og personbiltjenester Romerike 2023.

Eventuelle endringer til denne avtalen skal beskrives i bilag 2 - Endringer.

11 Tilbakeføring og sletting av personopplysninger ved opphør av databehandleravtalen

Ved opphør av denne avtale plikter databehandler å tilbakelevere alle Personopplysninger som er mottatt på vegne av Behandlingsansvarlig, og som omfattes av denne avtalen.

Ved opphør av avtalen skal Databehandler 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. Databehandler skal skriftlig dokumentere at sletting og eller destruksjon er foretatt i henhold til avtalen innen rimelig tid etter avtalens opphør.

Databehandler skal uansatt lagre dokumentasjon på sikkerhetsrutiner i minst 5 år fra det tidspunkt dokumentet ble erstattet med ny gjeldende utgave, og må i lagringstiden bistå Behandlingsansvarlig med å fremskaffe slik dokumentasjon.

12 Lovvalg og verneting

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

Bilag 1 Oversikt over godkjente underleverandører:

Navn	Kontaktopplysninger	Behandles Personopplysninger innenfor/ utenfor EU

Bilag 2 Endringer i databehandleravtalen

Dato	Endringer gjelder punkt	Beskrivelse