Vestfold

FYLKESKOMMUNE

Åpen anbudskonkurranse

Transporttjenester Minibuss

Vestfold 2025

Kontrakt

Vedlegg 4B

Databehandleravtale Bilag A - D

Vestfold
FYLKESKOMMUNE

BILAG TIL DATABEHANDLERAVTALEN

DETTE DOKUMENT BESTÅR AV FØLGENDE BILAG:

A. OPPLYSNINGER OM BEHANDLINGEN

A.1 Hovedavtalen og formålet med behandlingen av personopplysninger

Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige er knyttet til å levere tjenester som beskrevet i Hovedavtalen.

Med Hovedavtalen menes følgende avtale(r) inngått mellom partene:

Transporttjenester Minibuss Vestfold 2025 - signert xx.xx.2024.

Behandlingen har følgende formål:

Databehandler behandler opplysninger på vegne av Behandlingsansvarlig i forbindelse med skoleskyss i Vestfold gjennom avtalen: «Transporttjenester Minibuss Vestfold 2025».

Databehandler skal kun behandle personopplysningene for følgende formål:

- Å utøve hensiktsmessig transport av skoleelever i henhold til Opplæringsloven kap 7.

A.2 Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige

Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige omhandler (karakteren av behandlingen):

Utkjøring av transportlister for å kunne utføre hensiktsmessig transport til den enkelte elev ut fra de behov eleven har for å bli transportert til og fra skole, eller annet reisemål.

A.3 Typer av personopplysninger

Behandlingen omfatter følgende typer av personopplysninger om de registrerte (flere valg mulig):

☒	*Særlige kategorier av personopplysninger i henhold til GDPR artikkel 9 (1):* *helseopplysninger*
☐	*Andre opplysninger med særlig behov for beskyttelse:*
☒	*Andre personopplysninger:* *f.eks. navn, adresse, skolenavn, type hjelpemiddel, elevkoder, skysskoder, transportkommentar, hente- og leveringstid, informasjon kundekontakt*

A.4 Kategorier av registrerte

Behandlingen omfatter følgende kategorier av registrerte:

- Elever med behov for Tilrettelagt transport

A.5 Varighet av behandlingen

Databehandlers behandling av personopplysninger under Hovedavtalen kan påbegynne når Databehandleravtalen har trådt i kraft. Behandlingen har følgende varighet (velg ett alternativ):

☒	Behandlingen er ikke tidsbegrenset, og varer frem til opphør av Hovedavtalen.
☐	Behandlingen er tidsbegrenset, og gjelder frem til *<angi dato eller kriterium for avslutning >.*

Ved opphør (av avtalen eller en behandling) skal personopplysninger tilbakeleveres og slettes i samsvar med Databehandleravtalen punkt 12 og instruksjonene i Bilag C.
databehandlerens bruk av underdatabehandlere

B. BETINGELSER FOR DATABEHANDLERENS BRUK OG ENDRING AV EVENTUELLE UNDERDATABEHANDLERE

B.1 Behandlingsansvarliges godkjennelse av bruk av Underdatabehandlere

Ved inngåelse av Databehandleravtalen godkjenner Behandlingsansvarlig bruk av de Underdatabehandlere som er oppført i punkt B.2. Merk at også mor-, søster- og

datterselskaper til Databehandleren regnes som Underdatabehandlere hvis de bidrar til leveransen og behandler personopplysninger.

For endringer i bruk av Underdatabehandlere er det i tillegg avtalt følgende:

☒	Databehandleren kan benytte Underdatabehandler som i samme konsern (mor-søster- eller datterselskap) som er etablert i et land innenfor EØS-området. Databehandleren skal på forhånd informere Behandlingsansvarlige om bruken av slik Underdatabehandler. (Dette alternativet kan kombineres med et av de andre alternativene.)
☐	Databehandler kan gjennomføre endringer i bruken av Underdatabehandlere forutsatt at den Behandlingsansvarlige underrettes og gis mulighet til å motsette seg endringene. En slik underretning skal være mottatt av Behandlingsansvarlig senest 1 måned før endringen trer i kraft, med mindre annet er avtalt skriftlig mellom partene. Merk at endringer som medfører overføring av personopplysninger til land utenfor EØS-området (Tredjestater) uansett krever skriftlig godkjenning etter Databehandleravtalens punkt 10. Hvis Behandlingsansvarlig motsetter seg endringen skal Databehandler underrettes så snart som mulig. Den behandlingsansvarlige kan ikke motsette seg endringen uten saklig grunn.
☒	Databehandler kan kun gjennomføre endringer i bruken av Underdatabehandlere etter spesifikk og forutgående skriftlig godkjennelse fra Behandlingsansvarlig. Underdatabehandleren kan ikke behandle personopplysninger under Hovedavtalen før slik godkjennelse er gitt. Godkjennelse kan ikke nektes uten saklig grunn.

Vestfold
FYLKESKOMMUNE

B.2 Godkjente Underdatabehandlere

Den Behandlingsansvarlige har godkjent bruk av følgende Underdatabehandlere:

Navn	Org.nr.	Adresse	Beskrivelse av behandling	Behandlingssted	Kontaktinformasjon	Særlige kategorier personopplysninger
[Navn]	*[Org.nr.]*	*[Adresse]*	*[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]*	*[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]*	*[Kontaktinformasjon]*	*[Angi om det behandles særlige kategorier av personopplysninger]*
[Navn]	*[Org.nr.]*	*[Adresse]*	*[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]*	*[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]*	*[Kontaktinformasjon]*	
[Navn]	*[Org.nr.]*	*[Adresse]*	*[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]*	*[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]*	*[Kontaktinformasjon]*	
[Navn]	*[Org.nr.]*	*[Adresse]*	*[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]*	*[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]*	*[Kontaktinformasjon]*	

Databehandleren kan ikke bruke den enkelte Underdatabehandleren til en annen behandling enn avtalt eller la en annen Underdatabehandler utføre den beskrevne behandlingen i andre tilfeller enn det som følger av Bilag B, punkt B.1 om skifte av Underdatabehandler.

C. INSTRUKS VEDRØRENDE BEHANDLING AV PERSONOPPLYSNINGER

C.1 Behandlingens omfang og formål

Personopplysningene skal utelukkende behandles i det omfang og for de formål som er beskrevet i

- Hovedavtalen
- Databehandleravtalen med bilag

Databehandler har ikke råderett over personopplysningene utover det som er nødvendig for å oppfylle sine plikter etter Databehandleravtalen, og kan ikke behandle disse til egne formål.

C.2 Sikkerhet ved behandlingen

C.2.1 Angivelse av sikkerhetsnivå

Ut fra en vurdering av omfanget av personopplysninger som blir behandlet, typen opplysninger og karakteren av behandlingen er det basert på en konkret risikovurdering fastsatt at behandlingen (velg ett alternativ):

☐ Krever et høyt sikkerhetsnivå. Begrunnelse:

☒ Ikke krever et høyt sikkerhetsnivå. Begrunnelse:

Behandlingen omfatter ikke opplysninger av typen «særlige kategorier av personopplysninger».

C.2.2 Styringssystem for informasjonssikkerhet

Databehandleren skal ha et egnet styringssystem for informasjonssikkerhet. Databehandleren skal etablere og forvalte tilstrekkelige sikkerhetstiltak for å ivareta informasjonssikkerheten for behandling av personopplysningene, herunder (flere valg mulig):

☐	Sikkerhetskrav som beskrevet i Hovedavtalen:

☒	Sikkerhetskrav som beskrevet nedenfor: **Krav til opplæring og informasjon til databehandlers ansatte** • Ansatte hos databehandleren skal ha informasjon om databehandleravtalen. **Internkontroll** • Databehandleren skal ha et dokumentert internkontrollsystem for å ivareta informasjonssikkerheten. • Databehandler skal sikre at rutiner for å håndtere uønskede hendelser er tatt i bruk. • Databehandleren plikter å ha kontrolltiltak for å forebygge og forhindre at databehandlerens medarbeidere, tredjeparter eller systemer, bevisst eller ubevisst, medvirker til uønskede sikkerhetshendelser i databehandlerens egen virksomhet eller hos andre virksomheter eller privatpersoner som etter avtale med databehandleren bidrar til å oppfylle leveranseavtalen. **Akutte endringer av informasjonssikkerhetstiltak** • Dersom databehandleren må endre informasjonssikkerhetstiltakene sine som følge av akutte endringer i trusselbildet, skal den behandlingsansvarlige varsles om dette skriftlig, med informasjon om endringene som er foretatt, og hvordan risiko/trusselbildet er endret. Dette skal skje så snart som mulig. **Risikovurdering** • Databehandleren skal varsle den behandlingsansvarlige om alle forhold som medfører endring i risikobildet for behandling av personopplysningene. **Vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet** • Personopplysninger som omfattes av denne databehandleravtalen, holdes logisk atskilt fra egne og andres opplysninger og tjenester. Logisk atskilt betyr her at nødvendige tekniske tiltak som sikrer data mot uønsket endring og innsyn, er iverksatt og opprettholdt. • Lagringsmedier og/eller datautstyr som benyttes ved behandling av personopplysninger, er beskyttet mot ødeleggelse og mot at uvedkommende får tilgang. Databehandleren skal ha systemer for sikkerhetskopiering og gjenoppretting. • Det er etablert tiltak mot ødeleggende programvare på de av databehandlerens systemer som benyttes til å behandle personopplysningene på vegne av den behandlingsansvarlige. Databehandleren skal blant annet benytte brannmur og programvare for viruskontroll. • Det er satt i verk tiltak som er nødvendige for å forhindre tilfeldig eller ulovlig ødeleggelse av data, tap av data, ikke-autorisert tilgang til data, spredning eller endring av data og urettmessig innsyn og enhver annen bruk av personopplysninger som ikke er i overensstemmelse med denne databehandleravtalen.

	• Løsningen har tilstrekkelig kapasitet, uavhengig av den totale lasten databehandleren har fra andre kunder. • Databehandleren har beredskapsplaner for bortfall av løsningen. • Databehandleren har forsvarlige sikkerhetskopi- og gjenopprettingsrutiner som testes regelmessig. • Databehandleren har evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse • Databehandleren gjennomfører tekniske eller organisatoriske tiltak mot hacking. • Databehandleren krypterer data ved fysisk overføring. • Ved bruk av IoT-enheter har databehandleren et godt regime for bruk av sterke passord og regelmessig endring av dem. **Fjerning av tilganger** Når personer hos Databehandleren som behandler eller har tilgang på personopplysninger på vegne av Behandlingsansvarlig ikke lenger har behov for tilgang på opplysningene, skal Databehandler umiddelbart gi beskjed til Behandlingsansvarlig slik at tilganger kan fjernes.

C.3 Dokumentasjon

Databehandler skal dokumentere de rutiner og tiltak som er iverksatt for å oppfylle kravene som fremkommer av Gjeldende personvernregler og Databehandleravtalen, herunder kravene til informasjonssikkerhet. Slik dokumentasjon skal oppbevares og ajourholdes så lenge Databehandleravtalen består, og gjøres tilgjengelig for Behandlingsansvarlig eller tilsynsmyndigheter på forespørsel.

C.4 Overføring av personopplysninger - Lokasjon for behandling og tilgang

Behandling av de personopplysninger som avtalen omfatter kan ikke uten den Behandlingsansvarliges forutgående skriftlige godkjennelse utføres på eller med tilgang fra andre lokasjoner enn de som er angitt i Bilag B.2. Med lokasjon menes:

- Sted det er mulig å få tilgang til personopplysningene fra (aksessering)
- Sted hvor personopplysningene bearbeides (prosesseres)
- Sted hvor personopplysningene lagres

Begrensningen ovenfor gjelder ikke Databehandlerens mor-, søster- og datterselskaper som er etablert innenfor EØS-området. Databehandleren skal imidlertid på forespørsel fra den Behandlingsansvarlige redegjøre for hvor personopplysningene til enhver tid behandles.

C.5 Rutiner for revisjon og tilsyn

For å kontrollere etterlevelse av Gjeldende personvernregler og Databehandleravtalen er det avtalt følgende (flere valg mulig):

☒	Behandlingsansvarlig har rett til å utføre revisjon på Databehandlers forretningssted for å verifisere Databehandlers etterlevelse av sine plikter i henhold til denne Databehandleravtalen eller Gjeldende personvernregler. Slike revisjoner skal: • Gjennomføres etter rimelig forhåndsvarsel og maksimalt én gang i året, med mindre sikkerhetsbrudd hos Databehandler eller andre særlige forhold gir grunn for hyppigere revisjoner; • Foregå innenfor normal arbeidstid og ikke forstyrre Databehandlers virksomhet unødvendig; • Utføres av ansatte hos Behandlingsansvarlig eller av tredjepart som er godkjent av Partene og underlagt taushetsplikt. Databehandler plikter å stille til rådighet de ressurser som med rimelighet kan kreves for å gjennomføre revisjonen. Behandlingsansvarlig skal dekke kostnader for eventuelle tredjeparter som benyttes til å gjennomføre revisjonen. For øvrig dekker Partene sine egne kostnader ved gjennomføring av revisjonen. Dersom revisjonen avdekker vesentlige brudd på forpliktelsene etter Gjeldende personvernregler eller Databehandleravtalen, skal Databehandler likevel dekke Behandlingsansvarliges rimelige kostnader ved revisjonen.
☐	Databehandleren skal benytte ekstern revisor til å attestere at sikkerhetstiltak er etablert og virker etter hensikten. Slik revisjon skal: i. gjennomføres én gang årlig, ii. utføres i henhold til anerkjente attestasjonsstandarder, for eksempel ISAE 3402. iii. utføres av en uavhengig tredjepart med tilstrekkelig kunnskap og erfaring Rapportene skal fremlegges for Behandlingsansvarlig på forespørsel. Databehandler skal i tillegg gi slik informasjon og bistand som er nødvendig for at Behandlingsansvarlig kan etterleve sine forpliktelser etter Gjeldende personvernregelverk.

☒	For standardiserte tredjepartstjenester som leveres av Underdatabehandler kan det fremlegges tredjepartsrevisjon forutsatt at revisjonen er gjennomført etter alminnelig anerkjente prinsipper og av sertifisert revisor.

C.6 Sletting og tilbakelevering av personopplysninger ved avtalens opphør

Partene har avtalt følgende om sletting/tilbakelevering av personopplysninger (velg ett alternativ):

☐	Alle personopplysninger som behandles under denne Databehandleravtale skal slettes uten ugrunnet opphold og senest innen 90 kalenderdager etter opphør av Hovedavtalen. Dette samme gjelder eventuell annen relevant informasjon som forvaltes på vegne av Behandlingsansvarlig.
☐	Alle personopplysninger som behandles under denne Databehandleravtale, samt eventuell annen relevant informasjon som forvaltes på vegne av Behandlingsansvarlig, skal tilbakeleveres ved opphør av Hovedavtalen. Etter tilbakelevering er skjedd, plikter Databehandler å slette alle personopplysninger og annen relevant informasjon som forvaltes på vegne av Behandlingsansvarlig innen 30 kalenderdager. Tilbakelevering skal skje på følgende måte: *<Angi hvordan og hvilket format som skal benyttes for tilbakelevering>*
☒	Personopplysninger omfattet av denne databehandleravtalen skal senest slettes på det tidspunktet da behandling av personopplysningene ikke lenger er nødvendig for å utføre de oppgavene og/eller tjenestene som følger av leveranseavtalen, med mindre annet følger av ufravikelig lovgivning, dokumentert instruks eller skriftlig avtale med behandlingsansvarlig.

C.7 Sektorspesifikke bestemmelser om behandling av personopplysninger

Ikke aktuelt for denne avtalen.

C.8 Kontaktinformasjon

Ved henvendelser i henhold til denne avtalen, eksempelvis ved varsling om brudd på personopplysningssikkerheten eller endring i bruk av underdatabehandlere, skal følgende kanaler benyttes:

Hos Behandlingsansvarlig	**Hos Leverandøren**
Sikkerhetsbrudd:	Sikkerhetsbrudd:
Telefon: 90 01 80 96	Telefon:
E-post: lars.sandnes@vestfoldfylke.no	E-post:
Andre henvendelser:	Andre henvendelser:
Navn: Lars Sandnes	Navn:
Stilling: Teamleder	Stilling:
Telefon: 90 01 80 96	Telefon:
E-post: lars.sandnes@vestfoldfylke.no	E-post:

D. ENDRINGER TIL DATABEHANDLERAVTALENS STANDARDTEKST OG ENDRINGER ETTER AVTALEINNGÅELSEN

Erstatningsansvar
Partenes erstatningsansvar for skade som rammer den registrerte eller andre fysiske personer, og som skyldes brudd på personvernforordningen, personopplysningsloven med forskrifter eller annet regelverk som gjennomfører personvernforordningen, følger av bestemmelsene i personvernforordningen artikkel 82.

Det er ikke erstatningsbegrensning for ansvar som følger av personvernforordningen artikkel 82.

Partene er hver for seg ansvarlige for overtredelsesgebyr som er ilagt i henhold til personvernforordningen artikkel 83.

Lovvalg
Partenes rettigheter og plikter etter denne databehandleravtalen bestemmes i sin helhet av norsk rett.

Dersom en tvist ikke blir løst ved forhandlinger eller mekling, kan hver av partene forlange tvisten avgjort med endelig virkning ved norske domstoler.

Partene vedtar ved denne databehandleravtalen Telemark tingrett som verneting. Dette gjelder også etter opphør av databehandleravtalen.

Dekning av kostnader
Ved revisjon og tilsyn skal hver avtalepart dekke sine egne kostnader. Dette gjelder med mindre et tilsyn avdekker avvik fra forpliktelsene etter denne databehandleravtale. I dette tilfellet skal alle kostnadene forbundet med tilsynet dekkes av databehandleren, inkludert den behandlingsansvarliges og eksterne revisorers relevante kostnader.