

Databehandleravtale

mellom

Brakar as
«Behandlingsansvarlig»

og

Leverandør
«Databehandler»

1. Avtalens parter

Avtalen gjelder mellom Brakar as (heretter «Behandlingsansvarlig» eller «Brakar») og *Leverandør* (heretter «Databehandler»). Behandlingsansvarlig og Databehandler samlet kalles heretter «partene».

Nøkkelpersonell hos partene og deres kontaktinformasjon er følgende:

For Behandlingsansvarlig:

Personvernombud / Jarle Ekelund

E-post-adresse: personvern@brakar.no eller jarle.ekelund@brakar.no

For Databehandler:

Stilling / Navn:

E-post-adresse:

Ved endringer i nøkkelpersonell skal ny kontaktinformasjon så raskt som mulig sendes den annen part. Ny kontaktinformasjon legges som vedlegg til denne avtale.

2. Bakgrunn

På vegne av Buskerud Fylkeskommune tilbyr Behandlingsansvarlig skoleskyss med taxi til elever ved grunnskole og videregående skole som har krav på dette etter opplæringsloven kapittel 7, og som ikke kan benytte seg av ordinær kollektivtransport, enten på grunn av deres helsetilstand eller fordi de bor utenfor ordinær kollektivrute. For å gi effektiv og trygg taxitransport til disse elevene, benytter Behandlingsansvarlig seg av ulike transportselskaper.

I forbindelse med gjennomføring av ovennevnte skoleskysstransport vil Databehandler behandle enkelte personopplysninger om elevene på vegne av Behandlingsansvarlig. Denne databehandleravtalen er inngått for å sikre at all behandling av personopplysninger som Databehandler foretar på vegne av Behandlingsansvarlig i forbindelse med gjennomføring av skoleskyssordningen, er i samsvar med norsk personvernlovgivning samt interne retningslinjer som gjelder i Brakar AS, og som Databehandler er gjort kjent med. Avtalen skal herunder sikre at personopplysninger om elevene (de registrerte) ikke brukes urettmessig eller kommer uberettigede i hende.

3. Avtalens formål og omfang

Databehandler skal bare behandle personopplysninger som er nødvendige for å gjennomføre sine transporttjenester i forbindelse med skoleskyssordningen. Personopplysningene som behandles er følgende:

- Kontaktinformasjon til eleven og dennes foresatte, herunder navn, adresse, og telefonnummer til eleven og elevens foresatte,
- Opplysninger om elevens skoletilhørighet
- Opplysninger om eleven benytter hjelpemidler, eksempelvis rullestol eller krykker - dersom dette har betydning for gjennomføringen av transporten. Slike opplysninger

regnes som sensitive personopplysninger i henhold til personopplysningsloven § 2 (8) bokstav c.

- Medisinske opplysninger om eleven. Slike opplysninger regnes som sensitive personopplysninger i henhold til personopplysningsloven § 2 (8) bokstav c.
- Opplysninger om eleven må ha med seg ledsager eller må fraktes i egen bil. I slike tilfeller oppgis ikke årsaken til behovet for disse tilpasningene av transporten.

Formålet med behandlingen av personopplysningene er å kunne legge til rette for en mest mulig spesialtilpasset og sikker skoleskysstjeneste for de elevene som Behandlingsansvarlig tilbyr skoleskysstjeneste med taxi.

Databehandler får overlevert, lagrer og sammenstiller ovennevnte kategorier av personopplysninger om elever som er innvilget spesialtilpasset skoleskysstjeneste.

Avtalen er underlagt personopplysningsloven og forordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (heretter omtalt som «personvernforordningen»). Ved motstrid mellom avtalens regulering og de rammer som følger av personopplysningsloven eller personvernforordningen, viker avtalens regulering.

4. Databehandlers plikter

Så lenge avtalen gjelder skal Databehandler:

- (i) sikre at Databehandlers behandling av personopplysninger er i overensstemmelse med all relevant regelverk/lovgivning om personopplysninger;
- (ii) bare behandle personopplysninger etter dokumenterte instruksjoner som den Behandlingsansvarlig til enhver tid har bestemt skal gjelde, og ikke behandle personopplysninger utover hva som er nødvendig for å oppfylle Databehandlers forpliktelser i sammenheng med avtalen;
- (iii) ikke utlevere eller overlate personopplysninger til andre, herunder til stater utenfor EU/EØS, med mindre Behandlingsansvarlig har godkjent dette skriftlig;
- (iv) etablere og etterkomme nødvendige tekniske og organisatoriske tiltak for å sikre tilfredsstillende informasjonssikkerhet i henhold til gjeldende regelverk, herunder kravene etter personvernforordningen artikkel 32. Tiltakene skal sørge for at hensynene til konfidensialitet, integritet og tilgjengelighet ivaretas ved behandling av personopplysninger. Dette omfatter blant annet, alt etter hva som er relevant, nødvendige tiltak for å forhindre tilfeldig eller ulovlig ødeleggelse eller tap av data, ikke-autorisert tilgang til eller spredning av data så vel som enhver annen bruk av personopplysninger som ikke er i overensstemmelse med denne avtalen. Det omfatter også tiltak for å gjenopprette tilgjengelighet og tilgang til personopplysninger ved uønskede hendelser;
- (v) gjennomføre årlig sikkerhetsrevisjon og vedlikehold av interne systemer for behandling av personopplysninger for å ivareta kravene til informasjonssikkerhet i henhold til gjeldende regelverk;

- (vi) ha rutiner for autorisasjon og styring som sikrer at bare de av Databehandlers medarbeidere som har reelt behov for tilgang til systemer og personopplysningene for å ivareta nødvendige oppgaver for drift av tjenestene, har slik tilgang. Tilgangsnivået skal være i henhold til reelt behov knyttet til å gjennomføre og administrere transporten, og tilgangen skal være basert på individuelle brukernavn og passord. Databehandler plikter å sørge for at tilgangen opphører dersom medarbeideren slutter eller misbruker personopplysningene;
- (vii) i henhold til Databehandlers rutiner avdekke, registrere, rapportere og lukke avvik knyttet til informasjonssikkerhet, herunder loggføre og dokumentere ethvert forsøk på ikke-autorisert tilgang og andre brudd på sikkerheten i datasystemet. Slik dokumentasjon skal oppbevares hos Databehandler;
- (viii) varsle Datatilsynet ved uautorisert utlevering av personopplysninger i henhold til personvernforordningen artikkel 33;
- (ix) registrere all autorisert og uautorisert tilgang til informasjon. Alle oppslag som gjøres i lagrede personopplysninger skal registreres slik at de kan spores til den enkelte bruker (dvs. ansatte hos Databehandler, eventuelle underleverandører og Behandlingsansvarlig). Loggene skal oppbevares til det ikke lenger antas å være bruk for dem, og slettes senest seks måneder etter at avtalen opphører;
- (x) bistå Behandlingsansvarlig med å sikre overholdelse av forpliktelsene knyttet til personvernforordningen artiklene 32–36, dvs.;
 - a. sikkerhet ved behandlingen;
 - b. melding til Datatilsynet om brudd på personopplysningssikkerheten
 - c. underretning av elevene (de registrerte) om brudd på personopplysningssikkerheten
 - d. vurdering av personvernkonsekvenser og forhåndsdrøftinger
- (xi) etablere rutiner for å slette informasjon når den ikke lenger er nødvendig ut fra formålet med behandlingen. Personopplysninger om elevene (de registrerte) skal slettes når transportbehovet for vedkommende elev opphører;
- (xii) samarbeide med, og assistere, Behandlingsansvarlig ved oppfyllelse av elevenes (de registrertes) rettigheter knyttet til tilgang til opplysninger, herunder å svare på anmodninger som elevene (de registrerte) inngir med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III.;
- (xiii) omgående underrette Behandlingsansvarlig dersom Databehandler mener at en instruks er i strid med forordningen eller andre bestemmelser om vern av personopplysninger.
- (xiv) holde Behandlingsansvarlig skadesløs for eventuelle utgifter relatert til erstatningskrav eller overtredelsesgebyrer som kan henføres til forhold hos Databehandler. Behandlingsansvarlig kan søke regress for slike utgifter og kostnader dersom Behandlingsansvarlig har lagt ut overfor den registrerte.

Ved brudd på denne avtalen kan behandlingsansvarlig pålegge databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Databehandler skal dokumentere sine rutiner og alle tiltak som er truffet for å oppfylle kravene angitt ovenfor. Denne dokumentasjonen skal på forespørsel gjøres tilgjengelig for

den Behandlingsansvarlige og Datatilsynet.

Databehandler plikter å påse at samtlige personer som gis tilgang til personopplysninger som behandles på vegne av Behandlingsansvarlig, er kjent med denne avtalen og underlagt avtalens bestemmelser.

Meddelelser, underretting, varsel eller annen kommunikasjon mellom behandlingsansvarlig og databehandler, skal sendes elektronisk til adressen som er oppgitt i punkt 1 over.

5. Behandlingsansvarliges plikter

Behandlingsansvarlig skal etterleve de forpliktelser som følger av personopplysningsloven, personvernforordningen og annen relevant lovgivning samt denne avtalen, herunder å gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med det foran nevnte.

6. Taushetsplikt

Databehandler behandler en rekke personopplysninger som må behandles konfidensielt. Dette gjelder særlige sensitive personopplysninger knyttet til skoleelevens helse, jf. punkt 3 over.

Databehandlers ansatte som behandler personopplysninger om elevene og andre som opptrer på Databehandlers vegne i forbindelse med behandling av personopplysninger i henhold til denne avtalen (heretter omtalt som «personer som er autorisert til å behandle personopplysningene»), skal være underlagt taushetsplikt. Personer som er autorisert til å behandle personopplysningene forplikter seg videre til å behandle opplysningene fortrolig. Databehandler skal påse at alle som behandler personopplysninger under avtalen er kjent med taushetsplikten, og undertegner taushetserklæring.

Bestemmelsen gjelder tilsvarende for eventuelle underleverandører, jf. pkt. 8.

Taushetsplikten gjelder også *etter* avtalens opphør. Partene plikter å ta de forholdsregler som er nødvendige for å sikre at materiale eller opplysninger ikke blir gjort kjent for andre i strid med dette punktet.

7. Innsyn og revisjoner mv.

Behandlingsansvarlig kan til enhver tid kreve innsyn i Databehandlers behandling av personopplysninger tilhørende Behandlingsansvarlig, samt i de systemene som benyttes til dette formål. Dette omfatter også dokumentasjon for oppfyllelse av kravene til informasjonssikkerhet og Databehandlers system for internkontroll. Retten til innsyn gjelder alle tekniske, organisatoriske og administrative forhold som er relevante for sikkerheten ved behandlingen av personopplysningene som utføres av Databehandler på vegne av Behandlingsansvarlig, og øvrige innsynsrettigheter nedfelt i lov.

Databehandler plikter å gi nødvendig bistand til Behandlingsansvarlig ved innsyn og revisjoner.

Databehandler skal gi Datatilsynet og annen relevant tilsynsmyndighet tilgang og innsyn i behandlingen av personopplysninger som følger av personopplysningsloven og personvernforordningen.

Databehandler skal uten ugrunnet opphold korrigere eventuelle avvik som oppdages i forbindelse med innsyn. Avvik som skyldes Databehandler eller dennes underleverandører skal korrigeres uten kostnad for Behandlingsansvarlig. Databehandler skal skriftlig redegjøre for korrektive tiltak og plan for gjennomføring.

8. Bruk av underleverandør

Dersom Databehandler ønsker å benytte andre underleverandører for oppfyllelse av forpliktelsene under avtalen krever dette skriftlig samtykke fra Behandlingsansvarlig før behandlingen/overføringen av personopplysninger starter. Behandlingsansvarlig forbeholder seg retten til å nekte bruk av underleverandør.

Dersom Behandlingsansvarlig samtykker til bruk av underleverandør, skal Databehandler sikre at underleverandøren påtar seg tilsvarende forpliktelser som Databehandler under denne avtalen. Databehandler er fullt ut ansvarlig overfor Behandlingsansvarlig for alt arbeid som utføres av egne underleverandører.

Databehandleren skal underrette den Behandlingsansvarlig om eventuelle planer skifte ut underleverandører. Endringer i bruk av underleverandører må kommuniseres tydelig skriftlig, slik at Behandlingsansvarlige gis mulighet til å motsette seg endringen.

Tilgang til personopplysninger for eksterne tredjeparter krever konkret avtale mellom partene utover denne avtalen for alle andre enn databehandlers underleverandører.

9. Avtalens varighet

Avtalen gjelder fra den er undertegnet og så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig.

Ved brudd på denne avtale, personopplysningsloven, personvernforordningen eller annet regelverk for behandling av personopplysninger kan Behandlingsansvarlig pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

10. Opphør av avtalen

Ved opphør av denne avtalen plikter Databehandler å slette/destruere alle personopplysninger som er mottatt på vegne av den Behandlingsansvarlige og som omfattes av denne avtalen.

Databehandler skal slette eller forsvarlig destruere alle fysiske dokumenter og elektroniske kopier som inneholder personopplysninger som omfattes av avtalen, inkludert all

informasjon lagret lokalt hos Databehandler eller lagret i ekstern informasjonsenhet, enten hos Databehandler eller hos Underleverandør som lagrer på vegne av Databehandler. Dette gjelder også for eventuelle sikkerhetskopier.

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

11. Signatur og tilgang til avtalen

Denne avtalen er signert av begge parter og skal arkiveres på egnet måte, slik at den er lett tilgjengelig for tilsynsmyndigheter.

12. Lovvalg og verneting

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

Denne avtale er i 2 – to eksemplarer, hvorav partene har hvert sitt.

Drammen xx.xx.2018

Behandlingsansvarlig

Databehandler

.....

.....

Brakar as

Leverandør

Terje Sundfjord

Navn

*Vedlegg 1: Endringer i kontaktinformasjonen (opprettes ved behov)