Databehandleravtale inngått i forbindelse med Avtale om plasser i privat barneverninstitusjon

I henhold til personopplysningsloven, personopplysningsforskriften og forordning (EU) 2016/679 av 27. april 2016 (GDPR), artikkel 28, jf. artikkel 29 og 32-36, inngås følgende avtale mellom

Bufdir

Org.nr. 986 128 433

(behandlingsansvarlig)

og

Leverandør

Org.nr.

(databehandler)

Innhold

1. Avtalens hensikt

Hensikten med denne avtalen (heretter omtalt som «**Avtalen**») er å regulere rettigheter og plikter etter personopplysningsloven av 15. juni 2018 nr. 38 med tilhørende forskrift som inkorporerer EUs personvernforordning av 27. april 2016 (GDPR) samt øvrig relevant regelverk (heretter samlet omtalt som «**personvernregelverket**»).

Avtalen skal sikre at personopplysninger ikke brukes ulovlig, urettmessig eller at opplysningene behandles på måter som fører til uautorisert tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Avtalen regulerer databehandlers behandling og forvaltning av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse, i forbindelse med kjøp av institusjonstjenester.

Ved motstrid skal vilkårene i Avtalen gå foran databehandlers personvernerklæring og/eller vilkår i andre avtaler inngått mellom behandlingsansvarlig og databehandler.

2. Definisjoner

Følgende definisjoner, som gjøres gjeldende i Avtalen, fremgår av personvernforordningen artikkel 4:

> Nr. 1: «**personopplysninger**» enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en online-identifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet,
>
> Nr. 2 «**behandling**» enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring,
>
> Nr. 7: «**behandlingsansvarlig**» en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett,
>
> Nr. 8: «**databehandler**» en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.

3. Formålsbegrensning

Formålet med databehandlers forvaltning av personopplysninger på vegne av behandlingsansvarlig, er under behandling av barn og ungdom i privat barneverninstitusjon, med følgende behandlinger; å samle inn, registrere og lagre informasjon mv.

Personopplysninger som databehandler forvalter og behandler på vegne av behandlingsansvarlig kan ikke brukes til andre formål enn ovennevnte uten at dette på forhånd er godkjent skriftlig av behandlingsansvarlig.

Databehandler kan ikke overføre personopplysninger som omfattes av Avtalen til samarbeidspartnere eller andre tredjeparter eller engasjere en annen databehandler uten at dette på forhånd er godkjent skriftlig av behandlingsansvarlig, jf. punkt **11 Underleverandører** og punkt **12 Overføring av personopplysninger til stater utenfor EU/EØS**, i Avtalen.

4. Instrukser

Databehandler

Databehandler skal følge de skriftlige og dokumenterte instrukser for forvaltning og behandling av personopplysninger som behandlingsansvarlig har bestemt skal gjelde.

Databehandler forplikter seg til omgående å varsle behandlingsansvarlig dersom databehandler mottar instrukser fra behandlingsansvarlig som er i strid med bestemmelsene i gjeldende norsk personopplysningslovgivning.

Behandlingsansvarlig

Bufdir som behandlingsansvarlig forplikter seg til å overholde alle plikter i henhold til personvernregelverket som gjelder ved bruk av/behandling i Jobbpulz fagsystem til behandling av personopplysninger.

Behandlingsansvarlig skal uten ugrunnet opphold varsle databehandler om forhold behandlingsansvarlig forstår eller bør forstå kan få betydning for oppdragets/tjenestens gjennomføring.

5. Opplysningstyper og registrerte

Databehandleren behandler følgende personopplysninger på vegne av behandlingsansvarlig:

All informasjon som er nødvendig under oppholdet ved institusjonen. For eksempel telefonnummer, fødselsnummer, epostadresse, helseopplysninger med videre.

Personopplysningene gjelder følgende registrerte:

Primært barn og ungdom, men også ansatte i virksomheten som bruker systemene til institusjonen.

6. De registrertes rettigheter

Databehandler plikter å bistå behandlingsansvarlig med ivaretakelse av de registrertes rettigheter i henhold til personvernregelverket, særlig etter personvernforordningen kapittel III.

Den registrertes rettigheter kan omfatte rett til informasjon om behandlingen, innsyn, retting, sletting, begrensning av behandling, rett til å protestere og vern i forhold til profilering.

I den grad det er relevant, skal databehandler også bistå behandlingsansvarlig med å ivareta de registrertes rett til dataportabilitet og retten til å motsette seg automatiske avgjørelser, inkludert profilering.

Databehandler skal ikke gi innsyn i personopplysninger til den registrerte eller oppfylle eventuelle øvrige rettigheter uten at dette er skriftlig avtalt i det enkelte tilfelle med behandlingsansvarlig.

Databehandler skal videresende eventuelle forespørsler fra registrerte til behandlingsansvarlig snarest.

7. Tilfredsstillende informasjonssikkerhet

Databehandler skal iverksette tilfredsstillende tekniske, fysiske og organisatoriske sikringstiltak for å beskytte personopplysninger som omfattes av Avtalen mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet i henhold til personvernregelverket, herunder personvernforordningen artikkel 32.

Databehandler skal dokumentere egen sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, risikovurderinger og etablerte tekniske, fysiske eller organisatoriske sikringstiltak, herunder taushetserklæringer for egne ansatte, se punkt 8 Taushetsplikt. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig.

Databehandler skal etablere kontinuitets- og beredskapsplaner for effektiv håndtering av alvorlige sikkerhetshendelser. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig.

Databehandler skal gi egne ansatte tilstrekkelig informasjon om og opplæring i informasjonssikkerhet slik at sikkerheten til personopplysninger som behandles på vegne av behandlingsansvarlig blir ivaretatt.

Databehandler skal dokumentere opplæringen av egne ansatte i informasjonssikkerhet. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig.

Jobpulz fagsystem

Jobpulz fagsystem krypterer all trafikk til og fra server, inklusive passord ved pålogging. Hostingtjeneste er ISO sertifisert på høyeste sikkerhetsnivå og datalagring skjer utelukkende på sertifiserte datasentre i Norge, inklusive data backup, redundans og failover. Pålogging identifiserer hver bruker unikt med sterk autentisering (to-faktor). Det benyttes utelukkende SSL protokoller med klare føringer for sikkerhet og innstillinger i lokal nettleser. Jobpulz fagsystem har videre svært omfattende tilgangsstyring, hvor i realiteten alle funksjoner i journaldelen av løsningen er tilgangsstyrt. Alle operasjoner i løsningen loggføres i sanntid med unik identifisering av bruker og tidspunkt for utførelse av operasjoner. Jobpulz AS er fo røvrig nylig godkjent ASP leverandør i Norsk Helsenett med ditto godkjenning av styringssystem og sikkerhetsoppsett, både hva angår fagsystem og infrastruktur for hostingtjenester. Endelig nevnes at Jobpuls fagsystem også inkluderer moduler for planlegging, gjennomføring og dokumentasjon av virksomheters internkontroll og risikostyring.

8. Taushetsplikt

Taushetspliktbestemmelsene i lov om behandlingsmåten i forvaltningssaker 10. februar 1967 (forvaltningsloven) og/eller lov om barneverntjenester 17. juli 1992 (barnevernloven) kommer til anvendelse for databehandler og eventuelle underleverandører.

Kun ansatte hos databehandler som har tjenstlig behov for tilgang til personopplysninger som forvaltes på vegne av behandlingsansvarlig, skal gis slik tilgang. Databehandler plikter å dokumentere retningslinjer og rutiner for tilgangsstyring, herunder sørge for at egne ansatte undertegner en taushetserklæring. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig.

Ansatte hos databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til i henhold til Avtalen. Denne bestemmelsen gjelder også etter Avtalens

opphør. Taushetsplikten omfatter ansatte hos tredjeparter som utfører vedlikehold (eller liknende oppgaver) av systemer, utstyr, nettverk eller bygninger som databehandler anvender for å levere eller administrere tjenesten eller utføre behandlingen.

Norsk lov vil kunne begrense omfanget av taushetsplikten for ansatte hos databehandler og tredjeparter. Databehandler plikter å dokumentere eventuelle begrensninger i taushetsplikten som finner sted.

9. Tilgang til sikkerhetsdokumentasjon

Databehandler plikter å gi behandlingsansvarlig tilgang til all sikkerhetsdokumentasjon som er nødvendig for at behandlingsansvarlig skal kunne ivareta sine forpliktelser i henhold til personvernregelverket.

Databehandler plikter å gi behandlingsansvarlig tilgang til annen relevant dokumentasjon som gjør det mulig for behandlingsansvarlig å vurdere om databehandler overholder vilkårene i Avtalen.

Ansatte hos behandlingsansvarlig har taushetsplikt om konfidensiell sikkerhetsdokumentasjon som databehandler gjør tilgjengelig for behandlingsansvarlig, med mindre det er rettslig grunnlag for å utlevere denne.

10. Varslingsplikt ved sikkerhetsbrudd

Databehandler skal umiddelbart, og senest innen 24 timer etter kunnskap om hendelsen, varsle behandlingsansvarlig dersom personopplysninger som forvaltes/behandles på vegne av behandlingsansvarlig er blitt utsatt eller mistenkes utsatt for sikkerhetsbrudd som innebærer risiko for krenkelser av de registrertes personvern og personopplysningssikkerhet.

Varslet til behandlingsansvarlig skal som minimum inneholde informasjon som fremgår av artikkel 33 nr. 3, herunder informasjon som:

- beskriver sikkerhetsbruddet, herunder de sannsynlige konsekvensene av sikkerhetsbruddet,
- hvilke og omtrentlig antall registrerte som er berørt av sikkerhetsbruddet,
- hvilke og omtrentlig antall registreringer av personopplysninger som er berørt av sikkerhetsbruddet,
- hvilke strakstiltak som er iverksatt for å håndtere sikkerhetsbruddet og
- hvilke forebyggende tiltak som eventuelt er etablert for å unngå liknende hendelser i fremtiden.

Databehandler skal straks etter forsikre seg om at varselet er kommet frem og er under håndtering hos behandlingsansvarlig.

Databehandler skal også bistå behandlingsansvarlig angående plikten som behandlingsansvarlig har til å underrette de/den registrerte om bruddet.

Behandlingsansvarlig er ansvarlig for at varsler om sikkerhetsbrudd fra databehandler blir videreformidlet til Datatilsynet og/eller de registrerte.

11. Underleverandører

Databehandler plikter å inngå egne skriftlige avtaler med underleverandører som blir engasjert i forbindelse med forvaltningen av tjenesten og behandlingen av personopplysningene.

I avtaler mellom databehandler og underleverandører skal underleverandørene som et minimum pålegges å ivareta de samme plikter som databehandleren selv er underlagt i henhold til Avtalen. Databehandler plikter å forelegge avtalene for behandlingsansvarlig etter forespørsel.

Databehandler skal kontrollere at underleverandører overholder sine avtalemessige plikter, blant annet at informasjonssikkerheten er tilfredsstillende og at ansatte hos underleverandører er kjent med sine forpliktelser og oppfyller disse.

Databehandler kan bare engasjere underleverandører som på forhånd er skriftlig godkjent av behandlingsansvarlig. Databehandleren skal be om slik godkjennelse minst en måned før den aktuelle underleverandøren engasjeres.

En liste over de underleverandører som databehandler til enhver tid har engasjert og den behandlingsansvarlige videre har godkjent, fremgår av vedlegg 1. Vedlegget skal oppdateres hver gang det skjer endringer i engasjerte underleverandører.

Dersom underleverandøren ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger, skal databehandleren være fullt ut ansvarlig overfor den behandlingsansvarlige for oppfyllelse av underleverandørens forpliktelser.

Databehandler er erstatningsansvarlig overfor behandlingsansvarlig for tap som påføres behandlingsansvarlig og som skyldes ulovlig eller urettmessig behandling av personopplysninger eller mangelfull informasjonssikkerhet hos underleverandører til behandlingen.

12. Overføring av personopplysninger til stater utenfor EU/EØS

Personopplysninger kan bare overføres til en stat utenfor EØS-området ("tredjestat") eller til en internasjonal organisasjon hvis behandlingsansvarlig skriftlig har godkjent eller gitt instruks om slik overføring. Uten slik tillatelse eller instruks, kan databehandleren derfor blant annet ikke:

a) Videregi, utlevere eller gi tilgang til personopplysningene til en behandlingsansvarlig i en tredjestat eller internasjonal organisasjon;
b) Overlate behandlingen av personopplysninger til en underdatabehandler i en tredjestat eller internasjonal organisasjon;
c) La personopplysningene bli behandlet i en annen av databehandleren sine avdelinger som er plassert i en tredjestat; eller
d) For øvrig behandle personopplysningene i en tredjestat.

På tidspunktet for inngåelsen av denne Avtalen har behandlingsansvarlig ikke godkjent overføring av personopplysninger til en tredjestat eller en internasjonal organisasjon.

Dersom overføring av personopplysninger til en tredjestat eller en internasjonal organisasjon, som databehandleren ikke er blitt instruert av den behandlingsansvarlige om å gjennomføre, kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt, skal databehandleren underrette den behandlingsansvarlige om nevnte rettslige krav før behandlingen, med mindre denne rett av hensyn til viktige allmenne interesser forbyr en slik underretning.

Enhver overføring til en tredjestat eller internasjonal organisasjon skal skje i samsvar med gjeldende regelverk, herunder kapittel 5 i personvernforordningen.

Ved overføring til utlandet skal databehandler gi behandlingsansvarlig nødvendig dokumentasjon om sikkerhet, risiko og etterlevelsesnivå slik at behandlingsansvarlig kan gjennomføre en særskilt risikovurdering.

13. Sikkerhetsrevisjoner og personvernkonsekvensvurderinger

Databehandler skal gjøre tilgjengelig for behandlingsansvarlig all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i personvernforordningen artikkel 28 er oppfylt. Databehandler skal også muliggjøre og bidra til revisjoner, herunder inspeksjoner, som gjennomføres av den behandlingsansvarlige eller en annen revisor på fullmakt fra den behandlingsansvarlige.

Utover dette skal databehandler jevnlig gjennomføre sikkerhetsrevisjoner av informasjonssikkerheten og personopplysningssikkerheten knyttet til behandlingen. Sikkerhetsrevisjoner skal omfatte databehandlers sikkerhetsmål og sikkerhetsstrategi, sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, etablerte tekniske, fysiske og organisatoriske sikringstiltak og arbeidet med informasjonssikkerhet hos underleverandører knyttet til behandlingen. Det skal i tillegg omfatte rutiner for varsling av behandlingsansvarlig ved sikkerhetsbrudd og rutiner for testing av beredskaps- og kontinuitetsplaner. Databehandler skal dokumentere sikkerhetsrevisjonene, og plikter å fremlegge og presentere disse i et årlig kontraktsoppfølgingsmøte med behandlingsansvarlig.

Databehandler skal bistå behandlingsansvarlig dersom behandlingsansvarlig har plikt til å utrede personvernkonsekvenser, jf. personvernforordningen artikkel 35 og 36. Databehandler kan bistå behandlingsansvarlig ved iverksetting av personvernfremmende tiltak dersom konsekvensutredningen viser at dette er nødvendig.

14. Tilbakelevering og sletting

Ved opphør av denne avtalen plikter databehandler å tilbakelevere og/eller slette alle personopplysninger som forvaltes og foreligger på vegne av behandlingsansvarlig i forbindelse med levering/administrasjon av tjenesten og behandlingen. Behandlingsansvarlig bestemmer hvordan tilbakelevering av personopplysningene skal skje, herunder hvilket format som skal benyttes.

Databehandler skal slette personopplysninger fra alle lagringsmedier som inneholder personopplysninger som databehandler forvalter, besitter og behandler på vegne av behandlingsansvarlig. Sletting skal skje ved at databehandler skriver over personopplysninger etter Avtalens opphør innen 30 dager. Dette gjelder også for eventuelle sikkerhetskopier av personopplysningene.

Databehandler skal dokumentere at sletting (hardsletting) av personopplysninger er foretatt i henhold til denne Avtalen. Dokumentasjonen skal gjøres tilgjengelig for behandlingsansvarlig.

Databehandler dekker alle kostnader i forbindelse med tilbakelevering og/eller sletting av de personopplysninger som omfattes av denne avtalen.

Mislighold

Ved mislighold av vilkårene i denne Avtalen som skyldes feil eller forsømmelser fra databehandlers side, kan behandlingsansvarlig si opp Avtalen med øyeblikkelig virkning. Databehandler vil fortsatt være pliktig til å tilbakelevere og/eller slette personopplysninger som forvaltes på vegne av behandlingsansvarlig i henhold til bestemmelsene i punkt 14 Tilbakelevering og sletting ovenfor.

Databehandler er erstatningsansvarlig overfor de registrerte dersom feil eller forsømmelser hos databehandler påfører de registrerte økonomiske eller ikke-økonomiske tap som følge av at deres rettigheter eller personvern er krenket. Behandlingsansvarlig kan kreve erstatning for økonomiske tap som feil eller forsømmelser fra databehandlers side, inkludert mislighold av vilkårene i denne Avtalen.

15. Avtalens varighet

Denne Avtalen gjelder så lenge databehandler behandler personopplysninger på vegne av behandlingsansvarlig.

16. Kontaktinformasjon

Alle henvendelser vedrørende denne Avtalen rettes til:

Hos behandlingsansvarlig:	**Hos databehandler:**
Navn:	Navn:
Telefon:	Telefon:
E-post:	E-post:

17. Lovvalg og verneting

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

***

Undertegning

For behandlingsansvarlig: For databehandler:

_____ _____

direktør

Avtalen undertegnes elektronisk

Vedlegg 1

Underleverandører

I henhold til punkt 11 i Avtalen over, godkjenner behandlingsansvarlig følgende underleverandører til behandling av personopplysninger omfattet av Avtalen. Vedlegget skal oppdateres hver gang det skjer endringer i engasjerte underleverandører.

Databehandler kan ikke, uten den behandlingsansvarliges skriftlige godkjennelse, benytte en underleverandør til en annen behandlingsaktivitet eller på en annen lokasjon, eller bruke en annen underleverandør til den angitte behandlingsaktiviteten, enn det som er avtalt.

Navn på underleverandør	**Org.nr.**	**Adresse/lokasjon**	**Beskrivelse av behandling**