Databehandleravtale

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

mellom

Os kommune
.....
(behandlingsansvarlig)

og

Navn på tjenesteleverandøren
Compilo AS
(995781778)
.....

Innhold

1. Avtalens hensikt

Avtalens hensikt er å regulere rettigheter og plikter i henhold til gjeldende norsk personopplysningslovgivning 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, samt om oppheving av direktiv 95/46/EF (GDPR).

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 forvaltning av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse, i forbindelse med bruk av Kvalitetsstyringssystem (KSS).

Ved motstrid skal vilkårene i denne avtalen gå foran vilkår i andre avtaler inngått mellom behandlingsansvarlig og databehandler i forbindelse med bruk av KSS.

2. Definisjoner

Følgende definisjoner, som gjøres gjeldende i denne avtalen, fremgår av GDPR 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. 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 å levere og administrere KSS.

Personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig kan ikke brukes til andre formål enn levering og administrasjon av KSS uten at dette på forhånd er godkjent av behandlingsansvarlig.

4. Instrukser

a) Databehandler

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

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

Databehandlers bistand i forbindelse med særskilte rutiner og instrukser pålagt av behandlingsansvarlig, skal kompenseres av behandlingsansvarlig i samsvar med databehandlers ordinære betingelser og timesatser.

b) Behandlingsansvarlig

Behandlingsansvarlig forplikter seg til å overholde alle plikter i henhold til gjeldende norsk personopplysningslovgivning som gjelder ved bruk av/behandling i (KSS) til behandling av personopplysninger.

Behandlingsansvarlig bekrefter at:

i. Det foreligger tilstrekkelig behandlingsgrunnlag for behandling av personopplysninger;
ii. Behandlingsansvarlig har rett til og ansvaret for lovligheten av overføring av personopplysninger til databehandler;
iii. Behandlingsansvarlig har ansvaret for nøyaktigheten, integriteten, innholdet, påliteligheten og lovligheten av personopplysningene som behandles; og
iv. Behandlingsansvarlig har informert de registrerte i henhold til de til enhver tid gjeldende lovkrav.

Behandlingsansvarlig skal sørge for at personopplysninger behandles i henhold til GDPR, svare på henvendelser fra de registrerte og sørge for å implementere tilstrekkelige tekniske og organisatoriske tiltak for å sikre personopplysningene som behandles, jfr. GDPR artikkel 32.

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 forvalter følgende personopplysninger på vegne av behandlingsansvarlig i forbindelse med levering og administrasjon av KSS:

- Fullt navn
- E-post
- Telefonnummer
- IP-Adresse
- Rolle i organisasjonen
- Organisatorisk tilhørighet

Personopplysningene gjelder følgende registrerte:

- Alle ansatte/personer med tilgang til KSS.

6. De registrertes rettigheter

Databehandler plikter å bistå behandlingsansvarlig ved ivaretakelse av den registrertes rettigheter i henhold til gjeldende norsk personopplysningslovgivning og GDPR.

Den registrertes rettigheter kan inkludere retten til informasjon om:

- hvordan hans eller hennes personopplysninger behandles,
- retten til å kreve innsyn i egne personopplysninger,
- retten til å kreve retting eller sletting av egne personopplysninger og
- retten til å kreve at behandlingen av egne personopplysninger begrenses.

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

Databehandlers bistand i henhold til dette punkt, skal kompenseres av behandlingsansvarlig i samsvar med databehandlers ordinære betingelser og timesatser.

7. Tilfredsstillende informasjonssikkerhet

Databehandler skal iverksette tilfredsstillende tekniske, fysiske og organisatoriske sikringstiltak for å beskytte personopplysninger som omfattes av denne avtalen mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet.

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.

Databehandler skal etablere kontinuitets- og beredskapsplaner for effektiv håndtering av alvorlige sikkerhetshendelser.

Dokumentasjonen skal kunne tilgjengeligjøres for behandlingsansvarlig på forespørsel.

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 på forespørsel dokumentere opplæringen av egne ansatte i informasjonssikkerhet.

8. Taushetsplikt

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

Ansatte hos databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til i henhold til denne avtalen. Denne bestemmelsen gjelder også etter avtalens opphør.

Norsk lov vil kunne begrense omfanget av taushetsplikten for ansatte hos databehandler og tredjeparter.

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 gjeldende norsk personopplysningslovgivning og GDPR.

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

Ansatte hos behandlingsansvarlig har taushetsplikt for konfidensiell sikkerhetsdokumentasjon som databehandler gjør tilgjengelig for behandlingsansvarlig.

10. Varslingsplikt ved sikkerhetsbrudd

Databehandler skal uten ugrunnet opphold varsle behandlingsansvarlig dersom personopplysninger som forvaltes på vegne av behandlingsansvarlig utsettes for sikkerhetsbrudd som innebærer risiko for krenkelser av de registrertes personvern.

Varslet til behandlingsansvarlig skal som minimum inneholde informasjon som:

- beskriver sikkerhetsbruddet,
- hvilke registrerte som er berørt av sikkerhetsbruddet,
- hvilke 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.

Behandlingsansvarlig er ansvarlig for at varsler om sikkerhetsbrudd fra databehandler blir videreformidlet til Datatilsynet eller de registrerte i den grad det er påkrevet at disse blir varslet i henhold til gjeldende personopplysningslovgivning.

11. Underleverandører

Databehandleren gis en generell rett av behandlingsansvarlig til å benytte underleverandører for å gjennomføre databehandlerens behandling av personopplysninger i henhold til avtalen. Databehandleren skal underrette den behandlingsansvarlige om eventuelle planer om å benytte nye databehandlere eller skifte ut databehandlere, slik at den behandlingsansvarlige gis mulighet til å motsette seg slike endringer.

Ved inngåelse av avtalen, engasjerer databehandler følgende underleverandører i forbindelse med levering og administrasjon av KSS:

- Fjordane IT
- Amazon Web Services

Databehandler plikter å inngå egne avtaler med underleverandører til KSS som regulerer underleverandørenes forvaltning av personopplysninger i forbindelse med levering og administrasjon av KSS.

I avtaler mellom databehandler og underleverandører skal underleverandørene pålegges å ivareta alle plikter som databehandleren selv er underlagt i henhold til denne avtalen.

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

Databehandler er ansvarlig overfor den behandlingsansvarlige for underleverandørenes handlinger og unnlatelser på samme måte som om dette hadde vært databehandlers egne handlinger og unnlatelser.

12. Overføring til land utenfor EU/EØS

Ikke aktuelt.

13. Sikkerhetsrevisjoner og konsekvensutredninger

Behandlingsansvarlig kan selv eller benytte uavhengig tredjepart til å gjennomføre sikkerhetsrevisjoner av databehandler. Behandlingsansvarlig dekker alle kostnader i forbindelse med en slik sikkerhetsrevisjon.

Databehandler skal bistå behandlingsansvarlig med å sikre overholdelse av forpliktelsene til behandlingsansvarlig i henhold til artikkel 32–36, herunder dersom bruk av KSS medfører at behandlingsansvarlig har plikt til å utrede personvernkonsekvenser. Databehandler kan bistå behandlingsansvarlig ved iverksetting av personvernfremmende tiltak dersom konsekvensutredningen viser at dette er nødvendig.

Databehandlers bistand i henhold til dette punkt, skal kompenseres av behandlingsansvarlig i samsvar med databehandlers ordinære betingelser og timesatser.

14. Tilbakelevering og sletting

Ved opphør av denne avtalen plikter databehandler å slette og tilbakelevere alle personopplysninger som forvaltes på vegne av behandlingsansvarlig i forbindelse med levering og administrasjon av KSS. Behandlingsansvarlig spesifiserer 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 på vegne av behandlingsansvarlig. Sletting skal skje ved at databehandler skriver over personopplysninger innen 31 dager etter avtalens opphør. Dette gjelder også for sikkerhetskopier av personopplysningene.

Databehandler skal dokumentere at sletting av personopplysninger er foretatt i henhold til denne avtalen. Dokumentasjonen skal gjøres tilgjengelig for behandlingsansvarlig.

Behandlingsansvarlig dekker alle kostnader og medgått arbeidstid fra databehandlers side i forbindelse med tilbakelevering og sletting av de personopplysninger som omfattes av denne avtalen.

15. Ansvar

Hver av Partene er ansvarlig for at denne Partens Behandling av Personopplysninger er i henhold til GDPR.

Behandlingsansvarlig kan under enhver omstendighet kun kreve dekket direkte tap forårsaket av databehandler oppad begrenset til 30% av årlig vedlikeholdskostnad. Tap av data, kunder, omsetning, omdømme e.l, skal anses som indirekte tap.

Behandlingsansvarlig skal holde databehandler skadesløs, for alle tap (herunder administrative gebyrer fra tilsynsmyndighet og erstatningsansvar ovenfor de registrerte) som skyldes brudd på behandlingsansvarliges forpliktelser under denne avtalen og personvernlovgivningen.

16. Avtalens varighet

Denne avtalen gjelder så lenge databehandler forvalter personopplysninger på vegne av behandlingsansvarlig.

Avtalen kan sies opp av begge parter med en gjensidig frist på 30 dager.

17. Kontaktinformasjon

Alle henvendelser vedrørende denne avtalen rettes til:

Hos behandlingsansvarlig:	Hos databehandler:
	John Tonheim
	928 00 060
	john@compilo.no

18. 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:

Oslo 18/9-18

John Tonheim, 20.07.2018

Avtalen undertegnes i to eksemplarer, ett til hver part.