ÅLESUND KOMMUNE

Databehandleravtale

mellom

Behandlingsansvarlig:	**Ålesund kommune**
Organisasjonsnummer:	**929 911 709**
Etablert i:	Norge
Behandlingsansvarlig kontaktinformasjon for generelle henvendelser (navn, rolle, kontaktdetaljer):	*Kommunalsjef som er systemeier skal stå som behandlingsansvarlig.* *Systemeier eller innkjøpssjefen skal signere avtalen.*
Databehandler:	
Organisasjonsnummer:	
Etablert i :	
Databehandler kontaktinformasjon for generelle henvendelser (navn, rolle, kontaktdetaljer):	

heretter betegnet som henholdsvis
Behandlingsansvarlig, Databehandler eller part,
i fellesskap som partene.

ÅLESUND KOMMUNE

1. Innledning

Partene bekrefter herved at de har nødvendige fullmakter til å inngå denne databehandleravtalen (Databehandleravtalen). Databehandleravtalen vil utgjøre en del av og regulere all behandling av personopplysninger i tilknytning til [arkivsaksnummer/avtalenavn/signert dato] (Tjenesteavtale) mellom partene.

Kommentert [MCT1]: referer til hvilken tjenesteavtale inkl. arkivsaksnummer og dato signert, eks. *17/7450: Anskaffelse – Forvaltningsløsning for kart og plandata*, signert 29.06.18

2. Definisjoner

Definisjonene av personopplysning, sensitiv personopplysning, behandling av personopplysning, den registrerte, behandlingsansvarlig og databehandler skal forstås slik de brukes og tolkes i henhold til gjeldende personvernlovgivning, inkludert lov om behandling av personopplysninger av 15. juni 2018 nr. 38 og personvernforordningen Europaparlaments- og rådsforordning (EU) 2016/679 (GDPR) av 27. april 2016.

3. Formål

Databehandleravtalen regulerer Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige, og beskriver hvordan Databehandleren gjennom tekniske og organisatoriske virkemidler skal bidra til å sikre den registrertes rettigheter på vegne av den Behandlingsansvarlige.

Formålet med Databehandlerens behandling av personopplysninger er å oppfylle Tjenesteavtalen og Databehandleravtalen.

Avtalen skal sikre at personopplysninger ikke brukes urettmessig eller kommer uberettigede i hende.

Ved eventuell motstrid mellom bestemmelser om behandling av personopplysninger har Databehandleravtalen forrang over Tjenesteavtale eller andre tidligere avtaler som omhandler personvern inngått mellom partene.

Oversikt over typer personopplysninger og taushetsbelagt informasjon som behandles i henhold til denne databehandleravtalen:

	Angi hvilke opplysninger som vil behandles (angis med «x» og evt. tekst)
1. Personopplysninger:	
Sensitive personopplysninger (inkl. helseopplysninger)	
Dybdeopplysninger om person	
Ordinære personopplysning	
Opplysninger om ansatte	
Personnummer eller andre identifikatorer som kan knyttes direkte til fysisk person	

Annen informasjon av betydning for informasjonssikkerheten, f.eks. teknisk informasjon som muliggjør tilgang til skjermet informasjon	
2. Informasjon underlagt taushetsplikt:	
Lovbestemt taushetsplikt	
Informasjon som kan unntas offentlighet – Offentleglova kap. 3	
Avtalefestet taushetsplikt	
3. Sikkerhetsgradert informasjon	
4. Intern informasjon uten restriksjoner/uten innsynsrett	
5. Informasjon som skal lagres i nærmere angitte land (regnskapsmateriell)	
6. Informasjon som skal lagres i Norge (arkivmateriale)	

4. Databehandlerens plikter

Databehandler skal bare behandle personopplysninger på vegne av og i henhold til instruksjoner fra Behandlingsansvarlig. Type personopplysninger som behandles i henhold til denne databehandleravtalen er angitt i punkt 3. Ved å inngå denne Databehandleravtalen instruerer Behandlingsansvarlig Databehandler om å behandle personopplysninger på følgende måte:
i) bare i henhold til gjeldende lovgivning, ii) for å oppfylle alle plikter i henhold til Tjenesteavtale, iii) som instruert via Behandlingsansvarlig sin bruk av Databehandlers ordinære tjenester og iv) som spesifisert i denne Databehandleravtalen.

Databehandleren har ved avtaleinngåelsen ingen grunn til å anta at det foreligger regulatoriske hindringer mot å følge instruksjonene fra Behandlingsansvarlige. Dersom Databehandleren ved et senere tidspunkt blir klar over at Behandlingsansvarliges instruksjoner eller behandling av personopplysninger strider mot gjeldende personvernlovgivning, eller at behandling strider mot instruksjonene som angitt over, skal Databehandleren melde dette til Behandlingsansvarlige. Er Databehandler av den oppfatning at instruks fra Behandlingsansvarlig er i strid med GDPR, personopplysningsloven eller annen regulering av behandling av personopplysninger, skal Databehandler umiddelbart skriftlig underrette Behandlingsansvarlig om dette.

Databehandleren skal sikre konfidensialitet, integritet og tilgjengelighet til personopplysningene i henhold til de regulatoriske krav som gjelder for Databehandlere. Dette inkluderer å implementere systematiske, organisatoriske og tekniske virkemidler for å sikre et tilstrekkelig nivå for sikkerhet. Ved avgjørelsen av hva som er et tilstrekkelig nivå skal hensyn til den teknologiske utviklingen og kostnaden ved implementering av tiltak veies mot risikoen ved behandlingen og den typen personopplysninger som behandles.

ÅLESUND KOMMUNE

Databehandleren skal ved tekniske og organisatoriske virkemidler bistå Behandlingsansvarlig med å ivareta Behandlingsansvarliges plikter under Personopplysningsloven og GDPR artikkel 32 til 36, samt bistå i arbeidet med å behandle forespørsler fra registrerte i henhold til GDPR kapittel III. Pliktenes omfang avgrenses av formen for behandling av personopplysninger og hvilken informasjon som er tilgjengelig for Databehandler.

Behandlingsansvarlige kan kreve informasjon om sikkerhetstiltak, dokumentasjon og annen informasjon om hvordan Databehandleren behandler personopplysninger. Dersom Behandlingsansvarlige ber om mer informasjon enn det som Databehandler tilgjengelig gjør for å oppfylle kravene til rollen som Databehandler i henhold til gjeldende personvernlovgivning, kan Databehandleren kreve betaling for slike eventuelle tilleggstjenester i henhold til avtale mellom partene. Det vises for øvrig til pkt. 8.

Databehandler skal innhente taushetserklæring fra egne ansatte og andre som gis tilgang til Behandlingsansvarliges informasjon og annen relevant dokumentasjon i anledning oppdrag disse utfører for Behandlingsansvarlig, før tilgang til informasjonen gis. Taushetserklæringen må sikre at personer som er autorisert til å behandle personopplysningene, har forpliktet seg til behandle opplysningene konfidensielt eller er underlagt en egnet lovfestet taushetsplikt, og at dette også gjelder dersom arbeidsforholdet senere opphører. Taushetsplikten gjelder også etter at denne avtalen og Tjenesteavtalen opphører.

Taushetserklæringen skal gjøres tilgjengelig for Behandlingsansvarlig på forespørsel.

Databehandleren skal gjennom å varsle Behandlingsansvarlig skriftlig **uten ugrunnet opphold** om brudd på personopplysningssikkerheten, muliggjøre etterlevelse av gjeldende personvernlovgivning vedrørende varsling til tilsynsmyndigheter og registrerte om avvik.

Videre vil Databehandleren, i den utstrekning det er praktisk mulig og lovlig, varsle Behandlingsansvarlig om;

i) innsynsbegjæringer fra registrerte,

ii) innsynsbegjæringer fra offentlige myndigheter

Databehandleren vil kun besvare forespørsler fra registrerte i den grad Behandlingsansvarlig har gitt tillatelse til det. Databehandleren vil varsle Behandlingsansvarlig om innsynsbegjæringer fra offentlige myndigheter i den grad slikt varsel er lovlig, samt kun utlevere informasjon til offentlige myndigheter dersom rettslig pålegg foreligger. Henvendelser til Databehandler skal Databehandler videreformidle til Behandlingsansvarlig uten ugrunnet opphold.

Databehandleren har ikke eierskap til eller kontroll med hvorvidt og hvordan Behandlingsansvarlig velger å benytte seg av eventuelle tredjeparts integrasjoner via Databehandlers API, via direkte databasekobling eller lignende. Ansvaret for slike integrasjoner med tredjepart påhviler utelukkende Behandlingsansvarlig.

Databehandler skal sikre at opplysninger ikke sammenblandes med opplysninger som behandles på vegne av andre kunder. Databehandler plikter å rette opplysninger etter skriftlig pålegg fra Behandlingsansvarlig. Sletting av opplysninger skal utføres av Databehandler etter skriftlig avtale med Behandlingsansvarlig. Databehandler skal ta sikkerhetskopier av all informasjon som lagres. Databehandler skal lagre sikkerhetskopiene på en annen lokasjon enn originaldataene.

ÅLESUND KOMMUNE

Databehandler skal føre protokoll over behandlingsaktiviteter i samsvar med GDPR art. 30.

5. Behandlingsansvarliges plikter

Ved å signere Databehandleravtalen bekrefter Behandlingsansvarlig:

- Behandlingsansvarlig har rett til å behandle personopplysninger og til å gi Databehandleren og dennes underleverandører adgang til å behandle personopplysninger.
- Behandlingsansvarlig er ansvarlig for at personopplysningene som overlates til Databehandleren er lovlig innsamlet, korrekte og tilstrekkelige.
- At forpliktelsen til å formidle relevant informasjon til registrerte eller myndigheter vedrørende behandlingen av personopplysninger er oppfylt.
- At sensitive personopplysninger kun vil bli behandlet som en del av Tjenesteavtalen.

6. Bruk av underleverandører og overføring av personopplysninger

Dersom Databehandler benytter seg av underleverandør eller tredjeparter/samarbeidspartner har Databehandler plikt til å påse at disse påtar seg tilsvarende forpliktelser som det som følger av denne Databehandleravtalen. Ved bruk av underleverandør eller tredjepart blir også underleverandør / tredjepart/samarbeidspartnere å anse som Databehandler etter denne databehandleravtalen.

Oversikt over aktuelle underleverandører og tredjeparter/samarbeidspartnere ved avtalens oppstart, som er godkjent av Behandlingsansvarlig, ligger som bilag 1 til denne databehandleravtalen.

Databehandler kan ikke benytte nye underleverandører og/eller tredjeparter/samarbeidspartnere til oppfyllelse av avtaler med Behandlingsansvarlig uten skriftlig forhåndsgodkjennelse fra Behandlingsvarlig. Behandlingsansvarlig har rett til å underkjenne valg av nye underleverandører og tredjeparter/samarbeidspartnere på saklig grunnlag.

Den enkelte Databehandleren plikter fortløpende å føre en oversikt over alle underleverandører / tredjeparter/samarbeidspartnere som benyttes i Tjenesteavtalen og fremlegge denne for Behandlingsansvarlig på forespørsel.

Underleverandør/samarbeidspartner plikter å oppfylle alle krav i denne Databehandleravtale.

Bestemmelsen gjelder tilsvarende for den enkelte underleverandørs eller tredjeparters/samarbeidspartners underleverandører eller tredjeparter/samarbeidspartnere.

Informasjonen kan ikke uten skriftlig forhåndsgodkjenning fra behandlingsansvarlig overføres til land utenfor EU/EØS.

Behandlingsansvarlig vil kun godkjenne overføring til land under følgende kriterier:

1. Personopplysninger skal bare behandles innenfor EU/EØS (med mindre annet avtales skriftlig) og ikke i land som skårer under 70 på Transparency International sin «Corruption Perception Index» (iht. Tjenesteavtalen).

2. Dersom avtalen gjelder behandling av sensitive personopplysninger skal behandling av slike opplysninger skje i Norge. Behandlingsansvarlig kan tillate at behandling av sensitive personopplysninger skjer utenfor Norge. Slik behandling krever skriftlig forhåndsgodkjenning, og samtykke kan nektes på fritt grunnlag.

7. Sikkerhet

Databehandler skal sørge for et høyt sikkerhetsnivå i sine produkter og tjenester. Dette skal skje ved organisatoriske, tekniske og fysiske sikkerhetstiltak, i henhold kravene til informasjonssikkerhet som fremgår av GDPR artikkel 32.

Databehandler skal oppfylle de krav til sikkerhetstiltak som stilles etter personopplysningsloven med forskrifter. Databehandleren skal kunne dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjonen skal være tilgjengelig på den Behandlingsansvarliges forespørsel.

Ved sikkerhets- eller personvernbrudd, skal Databehandler skriftlig varsle den Behandlingsansvarlige uten ugrunnet opphold. Melding om brudd skal minimum inneholde

1. beskrivelse av arten av bruddet på personopplysningssikkerheten, herunder når det er mulig kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall personopplysningsposter som er berørt
2. navnet på og kontaktopplysningene til personvernrådgiver eller annet kontaktpunkt der mer informasjon kan innhentes
3. beskrivelse av de sannsynlige konsekvensene på bruddet på personopplysningssikkerheten,
4. beskrivelse av de tiltak som er truffet eller som skal treffes for å håndtere bruddet på personopplysningssikkerheten, herunder tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.

Dersom ikke alle opplysninger kan gis i første melding, skal opplysningene gis suksessivt så snart de foreligger.

8. Rett til tilsyn

Det vises til art. 28 i Personopplysningsloven vedrørende databehandler sin plikt til å gjennomføre sikkerhetsrevisjoner av f.eks. Hardware og Software, andre enheter, funksjoner, systemer og lignende som omfattes av denne databehandleravtalen. Testene skal omfatte så vel tekniske tester som gjennomgang av dokumentasjon etc. Dette skal vederlagsfritt legges frem for behandlingsansvarlig på forespørsel og uoppfordret ved tekniske eller organisatoriske endringer.

Sikkerhetsrevisjonen skal minimum omfatte gjennomgang av alle punkter i Databehandlers virksomhet som er relevant for å avdekke om Databehandler har et forsvarlig sikkerhetsnivå som oppfyller alle relevante krav i Rettsgrunnlaget/denne Databehandleravtale. Dette omfatter alle deler av Databehandlers virksomhet som kan være av betydning for Behandlingsansvarliges informasjonssikkerhet i de leveranser som Databehandler i henhold til Leveranseavtalen utfører på vegne av Behandlingsansvarlig.

Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som ikke oppfyller ovenstående krav, skal dette behandles som avvik/brudd på

personopplysningssikkerheten. Avdekker revisjonen at Databehandler ikke oppfyller kravene i denne databehandleravtalen, plikter Databehandleren å foreta nødvendige utbedringer umiddelbart.

Behandlingsansvarlig kan i tillegg utføre revisjon av databehandler ved behov. I slike tilfeller plikter databehandler vederlagsfritt å legge frem nødvendig dokumentasjon.

9. Varighet

Databehandleravtalen gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig i henhold til Tjenesteavtale,

Databehandleravtalen opphører i forbindelse med avslutning av Tjenesteavtale. Ved opphør av Databehandleravtalen, skal Databehandler returnere personopplysninger som er behandlet på vegne av Behandlingsansvarlig i tråd med Tjenesteavtale. Etter at Behandlingsansvarlig har bekreftet mottak av relevante opplysninger skal Databehandler foreta sikker sletting eller forsvarlig destruering av alle opplysninger inkludert eventuelle sikkerhetskopier. Med mindre annet er avtalt mellom partene, skal eventuell bistand fra Behandlingsansvarlig med dette arbeidet kompenseres basert på; i) kompleksiteten ved forespørselen og ii) betaling for medgått tid.

Databehandler kan beholde personopplysninger etter opphøret av Databehandleravtalen kun i henhold til gjeldende lovgivning, og alltid underlagt de samme typer tekniske og organisatoriske tiltak som skissert i denne Databehandleravtalen.

10. Endringer og ugyldighet

Eventuelle endringer i Databehandleravtalen skal inkluderes i et eget endringsvedlegg og signeres av begge parter for å være gyldig.

Hvis bestemmelser i Databehandleravtalen kjennes ugyldig, skal ikke dette påvirke de øvrige bestemmelsene i Databehandleravtalen. Partene skal erstatte den ugyldige bestemmelsen med en gyldig bestemmelse som reflekterer intensjonen til partene bak bestemmelsen.

11. Mislighold og pålegg om stans

Ved brudd på denne databehandleravtalen eller ved brudd på personvernregelverket, kan Behandlingsansvarlig og aktuelle tilsynsmyndigheter pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Hvis det foreligger mislighold av databehandleravtalen, kan Behandlingsansvarlig ved skriftlig varsel kreve at Databehandler utbedrer forholdet innen en rimelig frist satt av Behandlingsansvarlig.

Ved et vesentlig mislighold, kan Behandlingsansvarlig uansett heve Tjenesteavtalen med øyeblikkelig virkning.

12. Ansvar

Begge parter har et individuelt ansvar etter gjeldende personvernlovgivning i forhold til de personopplysningene de behandler og skal holdes selvstendig ansvarlig for å betale alle bøter og erstatning som ilegges den respektive part av myndigheter eller domstoler i henhold til GDPR.

Behandlingsansvarlig har imidlertid krav på erstatning for tap som følge av at Databehandler eller underleverandør ikke har overholdt sine plikter i henhold til denne avtalen. Dette omfatter også rett til å få tilbakebetalt eventuell utbetalt erstatning til den skadelidte ved et solidarisk ansvar og evt. overtredelsesgebyr e.l. som Behandlingsansvarlig blir pålagt av aktuelle tilsynsmyndigheter og som kan tilbakeføres til at Databehandler ikke har overholdt sine plikter i henhold til denne avtalen. Dette ansvaret mellom partene reguleres av ansvarsbegrensningene i Tjenesteavtalen.

13. Gjeldende rett og verneting

Databehandleravtalen er underlagt norsk rett ved norske domstoler med Møre og Romsdal tingrett som avtalt verneting.

****

ÅLESUND KOMMUNE

Bilag 1. Oversikt over Databehandlers underleverandører og tredjeparter/samarbeidspartnere.

Dersom Databehandler benytter seg av underleverandør eller tredjeparter/samarbeidspartner har Databehandler plikt til å påse at disse påtar seg tilsvarende forpliktelser som det som følger av denne Databehandleravtalen. Ved bruk av underleverandør eller tredjepart blir også underleverandør / tredjepart/samarbeidspartnere å anse som Databehandler etter denne databehandleravtalen, jf pkt 6

Selskap	Rolle	Org. nr.	Leveranseområde	Adresse	Kontaktperson	E-post kontaktperson
	Underleverandør/tredjepart/samarbeidspartner		**Behandling:** **Behandlingssted (navn på land):**			
	Underleverandør/tredjepart/samarbeidspartner		**Behandling:** **Behandlingssted (navn på land):**			
	Underleverandør/tredjepart/samarbeidspartner		**Behandling:** **Behandlingssted (navn på land):**			
	Underleverandør/tredjepart/samarbeidspartner		**Behandling:** **Behandlingssted (navn på land):**			

ÅLESUND KOMMUNE

	Underleverandør/tredjepart/samarbeidspartner		**Behandling:** **Behandlingssted (navn på land):**			