**Databehandleravtale**

I henhold til gjeldende norsk personopplysningslovgivning og EUs Personvernforordning 2016/679 inngås følgende avtale

mellom

**Eigersund kommune**

(behandlingsansvarlig)

og

**xxx**

(databehandler)

**Innhold**

[1. Om avtalen 3](#_Toc522779599)

[2. Definisjoner 3](#_Toc522779600)

[3. Avtalens bakgrunn og formål 3](#_Toc522779601)

[4. Omfanget av behandlingen 3](#_Toc522779602)

[5. Rådighet over data 5](#_Toc522779603)

[6. Partenes plikter og rettigheter 5](#_Toc522779604)

[7. De registrertes rettigheter 6](#_Toc522779605)

[8. Tilfredsstillende informasjonssikkerhet 6](#_Toc522779606)

[9. Taushetsplikt 6](#_Toc522779607)

[10. Tilgang til sikkerhetsdokumentasjon 7](#_Toc522779608)

[11. Varslingsplikt ved sikkerhetsbrudd 7](#_Toc522779609)

[12. Underleverandører 7](#_Toc522779610)

[13. Overføring til land utenfor EU/EØS 8](#_Toc522779611)

[14. Sikkerhetsrevisjoner og konsekvensutredninger 8](#_Toc522779612)

[15. Tilbakelevering og sletting 8](#_Toc522779613)

[16. Endring av avtale 8](#_Toc522779614)

[17. Mislighold 9](#_Toc522779615)

[18. Avtalens varighet 9](#_Toc522779616)

[19. Kontaktinformasjon 9](#_Toc522779617)

[20. Lovvalg og verneting 9](#_Toc522779618)

Bilag 1 - Underleverandører

# Om avtalen

Denne databehandleravtalen (heretter kalt avtalen) regulerer rettigheter og plikter mellom behandlingsansvarlig og databehandler i henhold til gjeldende norsk personopplysningslovgivning og EUs forordning 2016/679/EC av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utvekling av slike opplysninger (General Data Protection Regulation), heretter omtalt som personvernforordningen.

Ved motstrid mellom denne avtalens regulering og de rammer som følger av personvernforordningen eller annen relevant lovgivning, viker denne avtalens regulering.

# Definisjoner

I denne avtalen gjelder de definisjoner som fremkommer i personvernforordningen, artikkel 4.

# Avtalens bakgrunn og formål

Denne avtalen kommer til anvendelse på all behandling av personopplysninger og annen taushetsbelagt informasjon som databehandler foretar for behandlingsansvarlig i henhold til «avtale/formål».

Avtalen regulerer databehandlers forvaltning av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse

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.

Databehandler kan ikke overføre personopplysninger som omfattes av denne avtalen til samarbeidspartnere eller andre tredjeparter uten at dette på forhånd er godkjent av behandlingsansvarlig, jf. [punkt 12. Underleverandører](#_Underleverandører) og [13. Overføring til land utenfor EU/EØS](#_Overføring_til_land) i denne avtalen.

# Omfanget av behandlingen

Formålet med databehandlers behandling av personopplysninger er på vegne av behandslingsansvarlig er å xxx.

Behandlingen er hjemlet i xxx §x.

Følgende personopplysninger behandles:

* Xxx
* Xxx

Følgende kategorier av personer (registrerte) behandles det opplysninger om:

* Innbyggere
* Virksomheter
* Ansatte
* Elever
* Politikere

Følgende behandlinger omfattes av avtalen:

|  |  |
| --- | --- |
| **Behandling** | **Behandlingsaktiviteter** |
| Innsamling |  |
| Registrering |  |
| Lagring |  |
| Strukturering |  |
| Organisering |  |
| Tilpasning eller endring |  |
| Gjenfinning |  |
| Sammenstilling |  |
| Sletting eller tillintetgjøring |  |
| Utlevering/overføring |  |
| Fjernhjelp |  |

# Rådighet over data

Databehandler har ikke råderett over dataene som behandles, og kan dermed heller ikke behandle disse til egne formål.

Dataene skal utelukkende behandles for å ivareta de formål som er beskrevet i denne avtalen eller som fremkommer av senere skriftlige instrukser fra behandlingsansvarlig. Utarbeides slike instrukser skal disse inngå som endringsbilag til denne avtalen.

Behandlingsansvarlig har til enhver tid full rådighet over de personopplysninger som databehandler behandler etter denne avtalen.

Behandlingsansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i personopplysninger som behandles hos databehandleren.

# Partenes plikter og rettigheter

1. **Databehandler**

Databehandler skal følge de skriftlige rutiner og instrukser for behandlingen som behandlingsansvarlig til enhver tid 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 personvernopplysningslovgivning.

Databehandler plikter å påse at kun de personer som har tjenstlig behov for tilgang til personopplysninger som omfattes av denne avtalen, gis slik tilgang. Dette gjelder både egne ansatte og evt. andre som opptrer på vegne av databehandler. Databehandler plikter videre å påse at disse er kjent med og underlagt denne avtalens bestemmelser.

Databehandler plikter å dokumentere retningslinjer og rutiner for tilgangsstyring. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig.

1. **Behandlingsansvarlig**

Behandlingsansvarlig skal etterleve de forpliktelser som fremkommer av norsk personopplysningslovgivning og annen særlovgivning samt denne avtalen.

Behandlingsansvarlig skal uten ugrunnet opphold varsle databehandler om forhold behandlingsansvarlig forstår eller bør forstå kan få betydning for databehandlers oppfyllelse av denne avtalen.

Behandlingsansvarlig har rett til innsyn i alle opplysninger som omfattes av databehandleravtalen, med mindre annet er avtalt eller følger av lov, direkte eller gjennom bruk av uavhengig tredjepartsrevisor, herunder:

* *Den behandling av personopplysninger og taushetsbelagt informasjon som databehandler foretar.*
* *De systemer som benyttes til denne behandlingen.*

Databehandler plikter å gi nødvendig bistand til slik tilgang/innsyn innen rimelig tid.

Retten gjelder tilsvarende for aktuelle tilsynsmyndigheter.

# De registrertes rettigheter

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

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,
* retten til å kreve at behandlingen av egne personopplysninger begrenses,
* retten til å protestere mot behandlingen og
* retten til å klage til en tilsynsmyndighet.

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.

# 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. 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.

# Taushetsplikt

Databehandler har taushetsplikt om opplysninger og all annen relevant dokumentasjon som databehandler får tilgang til iht denne avtalen.

Ansatte og andre som opptrer på vegne av databehandler i forbindelse med behandling av personopplysninger skal ha undertegnet taushetserklæring. Bestemmelsen gjelder tilsvarende for underleverandører.

Taushetsplikten gjelder også etter avtalens opphør.

# 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 personvernforordningen.

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.

# Varslingsplikt ved sikkerhetsbrudd

Databehandler skal uten ubegrunnet opphold skriftlig 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 lignende hendelser i fremtiden.

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

# Underleverandører

Dersom databehandler benytter seg av underleverandør for oppfyllelse av forpliktelsene under denne avtalen, skal databehandler sikre at underleverandør ivaretar alle plikter som databehandler selv er underlagt i henhold til denne avtalen.

På forespørsel fra behandlingsansvarlig, plikter databehandler å legge frem kopi av avtaler(e) som er inngått med underleverandørene. Slik avtaler skal senest være inngått før underleverandørene starter med behandling av personopplysninger.

Databehandler benytter underleverandører som angitt i Bilag 1 for behandlinger omfattet av denne avtalen.

Databehandler skal ikke engasjere andre underleverandører enn de som er nevnt i Bilag 1 uten at dette på forhånd er skriftlig godkjent av behandlingsansvarlig.

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

# Overføring til land utenfor EU/EØS

Personopplysninger som databehandler forvalter i henhold til denne avtalen, vil ikke bli overført til mottakerland utenfor EU/EØS.

# Sikkerhetsrevisjoner og konsekvensutredninger

Databehandler skal jevnlig gjennomføre sikkerhetsrevisjoner av informasjonssikkerheten knyttet til behandlingen denne avtalen gjelder.

Sikkerhetsrevisjoner skal omfatte databehandlers sikkerhetsmål og sikkerhetsstrategi, sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, etablerte tekniske, fysiske og organiserte sikringstiltak og arbeidet med informasjonssikkerhet hos eventuelle underleverandører. Det skal i tillegg omfatte rutiner for varsling av behandlingsansvarlig ved sikkerhetsbrudd og rutiner for testing av beredskaps- og kontinuitetsplaner.

Databehandler skal dokumentere sikkerhetsrevisjonene. Behandlingsansvarlig skal gis tilgang til revisjonsrapportene.

Dersom en uavhengig tredjepart gjennomfører sikkerhetsrevisjoner hos databehandler, skal behandlingsansvarlig informeres om hvilken revisor som benyttes og gis tilgang til oppsummering av revisjonsrapportene.

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

# Tilbakelevering og sletting

Ved opphør av denne avtalen plikter databehandler å slette og tilbakelevere alle opplysninger som databehandler har mottatt og behandlet på vegne av behandlingsansvarlig. Partene avtaler nærmere hvordan overføring konkret skal skje.

Etter at alle opplysninger er overført til behandlingsansvarlig og bekreftet mottatt av denne, skal databehandler irreversibelt slette eller forsvarlig destruere disse opplysningene fra alle lagringsmedier i sine systemer, med mindre ufravikelige rettsregler krever at personopplysningene fortsatt lagres.

Databehandler skal gi behandlingsansvarlig skriftlig bekreftelse på at opplysningene er overført og slettet som angitt overfor.

# Endring av avtale

I tilfelle endringer i gjeldende lovverk, endelig dom som gir en annen tolkning av gjeldende lov, eller endringer i tilknyttet xxx (jf. pkt. 3) som krever endringer av denne avtale, skal partene samarbeide om å oppdatere denne avtalen tilsvarende.

# 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 forpliktet til å tilbakelevere og slette personopplysninger som forvaltes på vegne av behandlingsansvarlig i henhold til bestemmelsene i punkt 14.

# 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 3 måneder.

# Kontaktinformasjon

Alle henvendelser vedrørende denne avtalen skal sendes skriftlig til:

|  |  |
| --- | --- |
| Databehandler: | Behandlingsansvarlig: |
| Eigersund kommune | xxx |
| Avdeling/Enhet | Adresse |
| Postboks 580 | Adresse |
| 4379 Egersund | Postnummer og sted |
|  |  |
| v/XX | v/XX |
| xxx@eigersund.kommune.no | e-postadresse |
| Tlf: xx xx xx xx | Tlf: xx xx xx xx |

# Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar lokal tingrett, pt. Dalane tingrett, som verneting. Dette gjelder også etter opphør av avtalen.

\*\*\*

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

Egersund, den xxx (dato)

Behandlingsansvarlig Databehandler

………………………………………………….. ………………………………………………….. (underskrift) (underskrift)

**BILAG 1 – Underleverandører**

|  |  |  |
| --- | --- | --- |
| **Navn**  | **Virksomhetstype/** **Tjeneste som leveres** | **Stedlig plassering** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |