

DATABEHANDLERAVTALE

Denne databehandleravtalen «**Databehandleravtalen**» gjelder der Databehandler Behandler Personopplysninger på vegne av Behandlingsansvarlig. Databehandleravtalen er inngått mellom:

org.nr. _____ og EMG Bay Tele og Data AS,
omtales som _____ org.nr. 980 369 617
«**Behandlingsansvarlig**» omtales som «**Databehandler**»;

Behandlingsansvarlig og Databehandler omtales samlet som «**Partene**», og hver for seg som «**Part**».

Partene har blitt enige om følgende for å oppnå tilstrekkelige garantier med hensyn til beskyttelse av personvern og andre grunnleggende rettigheter for de som får sine personopplysninger, som spesifisert i denne Avtalen, overført fra Behandlingsansvarlig til Databehandler.

1. Definisjoner

Databehandleravtalen skal forstås på bakgrunn av følgende definisjoner:

| | |
|-------------------------------|--|
| Personvernregelverket: | Med Personvernregelverket forstås: a) Personopplysningsloven av 2000; Gjennomføring og implementering av EUs personverndirektiv (95/46/EF) og kommunikasjonsverndirektiv (2002/58/EF) i norsk lov; b) GDPR (Generell Personvernsforordning); Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016. Med mindre annet er særskilt angitt skal enhver henvisning til GDPR forstås som en henvisning til gjennomføring og implementering av GDPR i norsk lov; c) Kommunikasjonsvernforordningen; forslag til Europaparlaments- og rådsforordning 2017/0003 (forordning om personvern og elektronisk kommunikasjon), dersom og fra den tid forordningen vedtas og gjennomføres i norsk lov; d) All annen gjeldende norsk lov og forskrift som regulerer Databehandlers Behandling av Personopplysninger, herunder lov som implementerer og gjennomfører GDPR, samt sektorlovgivning. |
| Personopplysning: | Enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»), jf. GDPR art. 4 (1). |
| 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, jf. GDPR art. 4 (2). |
| Brudd på Personopplysningssikkerheten: | Et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte Behandlet. Slikt Brudd på Personopplysningssikkerheten er ikke avhengig av at det har skjedd et brudd på Personvernregelverket, jf. GDPR art. 4 (12). |
| Behandlingsansvarlig: | Fysisk eller juridisk person som alene eller sammen med andre bestemmer formålet med Behandlingen av personopplysninger og hvilke midler som skal benyttes, jf. GDPR art. 4 (7). |
| Databehandler: | Fysisk eller juridisk person som Behandler personopplysninger på vegne av den behandlingsansvarlige, jf. GDPR art. 4 (8). |
| Underleverandør: | Fysisk eller juridisk person som Databehandler engasjerer, intensjonelt eller ikke, for å utføre behandlingsaktiviteter på vegne av Behandlingsansvarlig. |
| Tredjestat eller internasjonal organisasjon: | Overføring av personopplysninger som behandles eller skal behandles etter overføring til en tredjestat eller til en internasjonal organisasjon som ikke sikrer et tilstrekkelig beskyttelsesnivå uten at det foreligger et overføringsgrunnlag, for eksempel land utenfor EØS-området. |

2. Formål

Denne Databehandleravtalen har som formål å regulere Databehandlers Behandling av Personopplysninger på vegne av Behandlingsansvarlig i forbindelse med tjenester levert fra Emg Bay tele og data AS. Konsulenttenester og MS Office365 (omtales heretter som Drift og Supportavtalen). Databehandleravtalen skal sikre at Personopplysninger behandles i samsvar med kravene i til enhver tid gjeldende personvernlovgivning (Personvernregelverket, som definert ovenfor) og at Personopplysninger kun behandles i henhold til denne Databehandleravtalen og ved dokumenterte instruksjoner fra Behandlingsansvarlige.

Databehandlers behandling av Personopplysninger skal kun omfatte den Behandling som er nødvendig for at Databehandler skal kunne gjennomføre Drift og Supportavtalen med den Behandlingsansvarlige.

Databehandleravtalen kan revideres ved behov for tilpasninger til preseptorisk lovgivning, tolkninger av GDPR og Personvernregelverket (slik dette er definert over).

I tillegg til Behandling av Personopplysninger som følge av Drift og Supportavtalen er Partene kjent med at Databehandler også kan behandle Personopplysninger som behandlingsansvarlig, i forbindelse med (i) Etterlevelsen av gjeldende lover og regelverk, (ii) forespørsler/anmodninger og kommunikasjon fra myndigheter og (iii) av hensyn til administrasjon, bokføring og risikoevaluering.

3. Databehandlers Behandling av Personopplysninger

3.1 Behandlingens art

Databehandler vil Behandle og ha tilgang til Personopplysninger i forbindelse med IT support og Office365 i henhold til Drift og Supportavtalen for den Behandlingsansvarlige.

I forbindelse med oppfyllelsen av Drift og Supportavtalen vil Databehandler kunne foreta Behandlinger i form av tilgang, organisering, strukturering, tilpasning, gjenfinning, konvertering, lagring, flytting, konsultering og tilintetgjøring. Slik Behandling vil kun foregå i henhold til bestemmelsene i Databehandleravtalen og Drift og Supportavtalen, og kun etter instruksjoner fra Behandlingsansvarlig.

Databehandler skal ikke Behandle Personopplysninger i større omfang enn det som er nødvendig for å oppfylle Drift og Supportavtalen med den Behandlingsansvarlige. Annen Behandling kan kun skje unntaksvis og ved kortvarige tilfeller, og kun under instruksjon fra Behandlingsansvarlig.

Dersom Databehandler er i tvil om Behandlingen av enkelte Personopplysninger er nødvendig, eller innenfor Drift og Supportavtalen omfang, skal det straks, og før Personopplysninger behandles, konsulteres med Behandlingsansvarlig.

Under ingen omstendigheter er Databehandler berettiget til å Behandle Personopplysninger eller andre data som tilhører Behandlingsansvarlig for egne formål, og utover de formål som fremkommer av Databehandleravtalen eller Drift og Supportavtalen.

Dersom Databehandler er pålagt videre Behandling gjennom lov eller tilsvarende pålegg fra offentlig myndighet forplikter Databehandler seg til å varsle Behandlingsansvarlig, samt sikre videre konfidensialitet og sikkerhet som ilegges gjennom Databehandleravtalen. I slike tilfeller skal Databehandler i forkant gi varsel til Behandlingsansvarlig, med mindre gjeldende lovgivning forbyr slikt varsel.

3.2 Kategorier av Personopplysninger og datasubjekter

I forbindelse med oppfyllelse av Drift og Supportavtalen, og avhengig av Databehandlers leveranse, kan Databehandler komme i kontakt med Personopplysninger under den Behandlingsansvarliges ansvar. Dette omfatter blant annet opplysninger om navn, telefonnummer, epost-adresse, kommunikasjonsdata, dokumenter og tekst, sensitive opplysninger, etc.

Personopplysningene vil være gjelde ansatte hos den Behandlingsansvarlige/kunder av den Behandlingsansvarlige/klienter, ansatte hos bedriftskunder/leverandører og deres ansatte.

3.3 Området for Behandlingen

Databehandler skal hovedsakelig Behandle personopplysninger innenfor EØS-området.

Databehandler har ikke rett til å overføre Personopplysninger til et tredjeland eller internasjonal organisasjon, herunder ut av EØS-området, uten at det er nødvendig for å oppfylle Drift og Supportavtalen, kun etter spesifikt skriftlig samtykke fra Behandlingsansvarlig og under forsikring om at det foreligger tilstrekkelig overføringsgrunnlag i henhold til GDPR art. 44-49.

All slik eventuell overførsel skal møte de krav til sikkerhet og vern av de registrertes rettigheter som følger av Databehandleravtale og i henhold til Personvernregelverket.

3.4 Bruk av Underleverandører

Databehandler kan benytte Underleverandør i forbindelse med behandling av Personopplysninger dersom dette er nødvendig for å behandle Personopplysninger i henhold til Drift og Supportavtalen.

Behandlingsansvarlig gir Databehandler ved signering av denne Databehandleravtalen et generelt skriftlig samtykke til å benytte de Underleverandører som benyttes av Databehandler ved signering, samt foreta bytte av Underleverandører. Ved bytte eller engasjering av ny Underleverandør har Behandlingsansvarlig rett til to måneders varsel.

Behandlingsansvarlig har rett til å motsette seg Databehandlers bruk eller bytte av Underleverandør der det foreligger saklig grunn. Behandlingsansvarlig er forpliktet til å fremlegge skriftlig redegjørelse og dokumentasjon innen én måned etter varsel er mottatt, dersom det påstås saklig grunn til å motsette seg bytte av Underleverandør.

Databehandlers Underleverandører for behandling av Personopplysninger skal være bundet av de samme avtalemessige og lovmessige forpliktelser som Databehandler er underlagt i henhold til denne Databehandleravtalen, gjennom egne databehandleravtaler.

Behandlingsansvarlig har rett på opplysninger om Underleverandør, herunder innhold i databehandleravtale og informasjon om tekniske og organisatoriske tiltak Underleverandør har iverksatt for å etterleve Personvernregelverket. Utlevering av slike opplysninger og informasjon fra Databehandler forutsetter varsel fra Behandlingsansvarlig.

Behandlingsansvarlig har forhåndsgodkjent Underleverandører som opplistet i Bilag 1.

Databehandler kan, uten Behandlingsansvarliges godkjenning etter denne bestemmelsen, involvere, bytte eller engasjering ny Underleverandør eller andre tredjeparter som kun har midlertidig og begrenset tilgang til Personopplysninger i forbindelse med vedlikehold av systemer,

dersom disse ikke aktivt bidrar i Behandlingen av Personopplysninger eller Behandler Personopplysninger for eget formål.

4. Forpliktelser som Databehandler

4.1 Bistand til Behandlingsansvarlig

Databehandler forplikter seg til, og i hovedsak uten kompensasjon eller annet vederlag, til å:

- a. Behandle Personopplysninger kun etter instruks fra Behandlingsansvarlig og kun i henhold til det som er formålet med Drift og Supportavtalen
- b. Treffe alle tiltak som er nødvendig for å ivareta sikkerheten tatt i betraktning den Behandlingen som utføres på vegne av Behandlingsansvarlig, samt regelmessig og på eget tiltak foreta analyse og testing av slike forholdsmessige sikkerhetstiltak, herunder vurdere deres effektivitet;
- c. Bistå Behandlingsansvarlig med å sikre overholdelse av dennes forpliktelser til å ivareta Personopplysningssikkerhet og vurdere personvernkonsekvenser, idet det tas hensyn til Behandlingens art og den informasjonen som er tilgjengelig for Databehandleren;
- d. Bistå Behandlingsansvarlig, idet det tas hensyn til Behandlingens art og i den grad det er mulig, med å oppfylle dennes plikt til å oppfylle anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter. Kommer slik anmodning fra den registrerte direkte til Databehandler skal denne oversendes Behandlingsansvarlig som regulert i Databehandleravtalens varslingsbestemmelse;
- e. Bistå Behandlingsansvarlig med å løse avvikssituasjoner i samarbeid med Behandlingsansvarlig, såfremt avviket nødvendiggjør dette og i henhold til avvikhåndtering som regulert i Databehandleravtalen;
- f. Etter Behandlingsansvarliges instruks, slette eller tilbakelevere alle Personopplysninger og slette eventuelle eksisterende kopier, med mindre det foreligger en lovpålagt plikt til å fortsette lagringen;
- g. Umiddelbart varsle Behandlingsansvarlig hvis en instruksjon er i strid med Personvernregelverket;
- h. Sikre at alle som Behandler Personopplysninger har forpliktet seg til fortrolighet eller er underlagt en egnet lovfestet taushetsplikt, samt at kun slike autoriserte personer som har et nødvendig behov for å oppfylle Drift og Supportavtalen har eller får tilgang til Personopplysninger.

Databehandler er berettiget til å fakturere etter medgått tid for oppfyllelse av punktene d, e og f nevnt ovenfor. Timesats for konsulenter for dette arbeid p.t. NOK 1350.

4.2 Tekniske og organisatoriske tiltak

Databehandler skal sørge for at det foreligger tekniske og organisatoriske tiltak for å sikre og påvise at Behandlingen utføres i samsvar med Personvernregelverket, denne Databehandleravtalen og for å sikre bistand til oppfyllelsen av rettighetene til den registrerte.

Databehandler skal før oppstart, og deretter årlig, fremlegge dokumentasjon på Behandlingen som skjer på vegne av Behandlingsansvarlig. Denne dokumentasjonen skal inneholde:

- i. Kategorier av behandlingsaktiviteter;
- ii. Bruken av Underleverandører;
- iii. Overføringer ut av EØS-området;
- iv. En generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene;

Databehandler skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen ved Behandlingen. Disse egnede tekniske og organisatoriske tiltakene skal også sikre og påvise at Behandlingen utføres i samsvar med denne Databehandleravtalen. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov. Databehandler kan ta hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, men vurderingen skal gjøres i tråd med den vurderingen som skal gjennomføres etter GDPR art. 32.

Slike tekniske og organisatoriske tiltak skal som et minimum inkludere, men er ikke begrenset til, tiltak for å:

- a) Pseudonymisere og kryptere personopplysninger der det er relevant;
- b) Sikre evnen til vedvarende fortrolighet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene;
- c) Sikre evnen til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse;
- d) Ivareta en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er;
- e) Forhindre at datasystemer som Behandler Personopplysninger blir brukt eller gir tilgang til Personopplysninger til personer som ikke er autorisert, inkludert tilgang til å lese, kopiere, endre eller slette Personopplysninger uten autorisasjon.

Behandlingsansvarlig er forpliktet til å iverksette ovennevnte tiltak, og om nødvendig oppdatere tiltak, slik at de tekniske og organisatoriske tiltakene til enhver tid er i henhold til Personvernregelverket, herunder slik de er oppstilt i GDPR artikler 28 og 32.

4.3 Varsling

Databehandler skal varsle Behandlingsansvarlig uten ugrunnet opphold om:

- i. En instruksjon fra Behandlingsansvarlig strider mot Personvernregelverket;
- ii. Et pålegg om utlevering av Personopplysninger fra offentlig myndighet, med unntak av der slik varsling er forbudt;

- iii. Et brudd eller mulig brudd på sikkerheten som kan føre til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte Behandlet, herunder som et minimum der det foreligger Brudd på Personopplysningssikkerheten;
- iv. Henvendelser fra en registrert slik at Behandlingsansvarlig kan respondere, og uten at Databehandler selv responderer uten å ha fått eksplisitt tillatelse til å håndtere henvendelsen selv.

Databehandler plikter å gi tilstrekkelig bistand til Behandlingsansvarlig i etterkant av eventuelt varsel til Datatilsynet om Brudd på Personopplysningssikkerheten eller til den registrerte ved henvendelser. Enhver varsling eller henvendelse til Datatilsynet skal skje gjennom Behandlingsansvarlig. Dersom det er nødvendig for å avklare omfanget av Brudd på Personopplysningssikkerheten, skal Databehandler bistå Behandlingsansvarlig i samarbeidet med Datatilsynet.

Umiddelbart etter å ha gitt varsel om et Brudd på Personopplysningssikkerheten skal Databehandler gi ytterligere beskrivelse til Behandlingsansvarlig om:

- i. Alle relevante forhold knyttet til bruddet som Databehandler har kjennskap til, herunder hva bruddet består av, kategorier og volum på Personopplysninger. Forhold knyttet til avviket som Databehandler først får kjennskap til etter slik varsling skal meddeles Behandlingsansvarlig straks Databehandler får slik kjennskap;
- ii. Hvilke tiltak som er iverksatt eller foreslått iverksatt for å hindre konsekvenser og begrense omfanget av Bruddet på Personopplysningssikkerheten.

Videre skal Databehandler bistå Behandlingsansvarlig med å vurdere personvernkonsekvenser ved slikt Brudd på Personopplysningssikkerheten.

Databehandler plikter å varsle Behandlingsansvarlig dersom det avdekkes at Databehandler ikke etterlever, eller ser at det blir vanskelig å etterleve, kravene som følger av Personvernregelverket og denne Databehandleravtalen, uavhengig av årsak. I et slikt tilfelle kan Behandlingsansvarlig suspendere overføring og videre Behandling av Personopplysninger hos Databehandler.

5. Ansvar for Behandlingen

Behandlingsansvarlig er ansvarlig for at Personopplysninger som Databehandler får tilgang til har blitt innhentet lovlig og har gyldig behandlingsgrunnlag.

Behandlingsansvarlig har hovedansvaret for behandling av Personopplysninger som en følge av Drift og Supportavtalen og skal varsle Databehandler dersom det oppstår behov for bistand i forbindelse med GDPR artikkel 28(3) bokstav e og f. Databehandler er berettiget til å fakturere etter medgått tid for oppfyllelse av punktene nevnt ovenfor. Timesats for konsulenter for dette arbeid pt. NOK 1350.

Behandlingsansvarlig skal holde Databehandler skadesløs for alle kostnader, utgifter (inkludert kostnader til juridisk bistand), skade, tap (inkludert indirekte tap), forpliktelser, krav, søksmål, handlinger eller rettslige prosesser som Databehandler kan stå ovenfor som følge av Behandlingsansvarliges brudd på Personvernregelverket, Brudd på Personopplysningsikkerheten, og instruks gitt til Databehandler i strid med Personvernregelverket.

Ansvar for materiell eller ikke-materiell skade på en eller flere registrerte skal reguleres i henhold til vilkår og føringer gitt i GDPR art. 82.

Hver Parts ansvar skal begrenses oppad, per kontraktsår, til et beløp tilsvarende NOK 50.000

Ingen ansvarsbegrensning skal gjelde dersom skadevoldende handling er foretatt ved forsettlig eller grov uaktsomhet av noen av Partene.

6. Sikkerhetsrevisjon

Databehandler er forpliktet til å gi Behandlingsansvarlig tilstrekkelig tilgang og dokumentasjon til all informasjon som er nødvendig for å påvise etterlevelse av forpliktelsene fastsatt i Databehandleravtalen, og for å kunne gjennomføre sikkerhetsrevisjoner. Slike sikkerhetsrevisjoner omfatter, men er ikke begrenset til, stedlig inspeksjon og evaluering av systemer, organisering og sikkerhetstiltak, samt bruk av Underleverandører.

Behandlingsansvarlig er berettiget til å oppnevne en uavhengig inspektør, utpekt av Databehandler, til å gjennomføre sikkerhetsrevisjoner av Databehandlers etterlevelse av denne Databehandleravtalen, Drift og Supportavtalen Personregelverket.

Denne bestemmelsen innebærer ikke at Behandlingsansvarlig eller inspektør er berettiget til innsyn i aktiviteter, protokoller, informasjon eller noe annet materiale uavhengig av format som:

- a) Som vedrører kunder av Databehandler;
- b) Ikke er relevant for Behandlingen av Personopplysninger;
- c) Anses som en forretnings- eller bedriftshemmeligheter, eller
- d) Er underlagt taushetsplikt eller konfidensialitetsplikt (lovbestemt eller kontraktfestet) som Databehandler har overfor en tredjepart.

Behandlingsansvarlig skal Behandle alt materiale, uansett format, som Behandlingsansvarlig får i sin besittelse eller tilgang til som følge av sikkerhetsrevisjonen som konfidensiell informasjon. Under ingen omstendighet skal slike materialer deles med tredjeparter, eller benyttes på annen måte enn det som er nødvendig i forbindelse med sikkerhetsrevisjonen.

Behandlingsansvarlig er ansvarlig for alle kostnader knyttet til sikkerhetsrevisjoner, inkludert kostnader som blir påført Databehandler i denne forbindelse.

7. Taushetsplikt

Informasjon som Partene blir kjent med i forbindelse med denne Databehandleravtalen og gjennomføringen av den skal behandles konfidensielt, og ikke gjøres tilgjengelig for utenforstående uten samtykke fra den annen Part. Taushetsplikten er ikke til hinder for at opplysningene brukes når de er alminnelig kjent eller alminnelig tilgjengelig andre steder.

Partene skal ta nødvendige forholdsregler for å sikre at uvedkommende ikke får innsyn i eller kan bli kjent med konfidensiell informasjon.

Taushetsplikten gjelder Partenes ansatte, Underleverandører som handler på Partenes vegne i forbindelse med gjennomføring av denne Databehandleravtalen og Drift og Supportavtalen. Partene kan bare overføre taushetsbelagt informasjon til slike Underleverandører og tredjeparter i den utstrekning dette er nødvendig for gjennomføring av denne Databehandleravtalen og Drift og Supportavtalen, forutsatt at disse pålegges plikt om konfidensialitet tilsvarende dette punkt.

Taushetsplikten gjelder også etter at denne Databehandleravtalen og Drift og Supportavtalen er opphørt. Ansatte eller andre som fratrer sin tjeneste hos en av Partene, skal pålegges taushetsplikt også etter fratredelsen om forhold som nevnt ovenfor. Taushetsplikten opphører 10 (ti) år etter opphøret av denne Databehandleravtalen og Drift og Supportavtalen, med mindre annet følger av lov eller forskrift.

8. Varighet og avslutning av Behandlingen

Databehandleravtalen gjelder så lenge Databehandler Behandler eller har tilgang til Personopplysninger på vegne av Behandlingsansvarlig, og Behandlingsansvarlig er å anse som Behandlingsansvarlig for Personopplysningene.

Databehandlerens Behandling av Personopplysninger for Behandlingsansvarlig skal avsluttes ved opphør av Drift og Supportavtalen. Ved avslutning av Behandlingen av Personopplysninger skal Databehandler enten tilbakelevere eller slette alle eventuelle Personopplysninger, etter den Behandlingsansvarliges instruks, så fremt videre Behandling ikke er lovpålagt. Slik lovpålagt videre Behandling må varsles om til Behandlingsansvarlig.

Databehandler er berettiget til å fakturere etter medgått tid for oppfyllelse av denne bestemmelsen. Timesats for konsulenter for dette arbeid p.t. NOK 1350.

All tilgang til Behandlingsansvarliges systemer skal ved avslutning av Behandlingen stenges for Databehandler og dennes personell. Databehandler er forpliktet til å bistå Behandlingsansvarlig med gjennomføringen av dette.

Dette punktet medfører ikke at Databehandler skal slette Personopplysninger som Databehandler innehar som behandlingsansvarlig.

9. Lovvalg og verneting

Denne Databehandleravtalen er underlagt norsk rett og Partene aksepterer Behandlingsansvarliges hjemting som verneting. Dette gjelder også etter avslutning av Drift og Supportavtalen.

* * *