

Databehandleravtale

mellom

Kunden (heretter kalt "Behandlingsansvarlig")

og

Vemento AS Organisasjonsnummer: 929 628 675 Bekkedalen 15, 4325 Sandnes E-post: kontakt@hmsveileder.no (heretter kalt "Databehandler")

1. Avtalens bakgrunn og formål

1.1 Bakgrunn

Denne databehandleravtalen ("Avtalen") er inngått i forbindelse med Behandlingsansvarligs bruk av Databehandlers HMS-plattform ("Tjenesten") tilgjengelig på hmsveileder.no.

1.2 Formål

Avtalen regulerer Databehandlers behandling av personopplysninger på vegne av Behandlingsansvarlig i henhold til personvernforordningen (GDPR) artikkel 28.

1.3 Avtaleinngåelse

Avtalen anses inngått når Behandlingsansvarlig oppretter en bedriftskonto i Tjenesten og aksepterer brukervilkårene.

2. Behandlingens art, formål og varighet

2.1 Art og formål

Databehandler skal behandle personopplysninger på vegne av Behandlingsansvarlig for følgende formål:

- Drift og vedlikehold av HMS-styringssystemet
- Lagring og administrasjon av HMS-dokumentasjon
- Håndtering av risikovurderinger og avviksmeldinger
- Brukeradministrasjon og tilgangskontroll
- Generering av rapporter og eksport av data
- Teknisk support og feilretting

2.2 Varighet

Behandlingen av personopplysninger pågår så lenge Behandlingsansvarlig har en aktiv konto i Tjenesten, samt i en oppbevaringsperiode på 90 dager etter avslutning for å muliggjøre dataeksport.

3. Kategorier av registrerte og personopplysninger

3.1 Kategorier av registrerte

Behandlingen omfatter følgende kategorier av registrerte:

- Ansatte hos Behandlingsansvarlig
- Ledere og HMS-ansvarlige
- Verneombud
- Eksterne konsulenter med tilgang til systemet

3.2 Typer personopplysninger

Følgende kategorier av personopplysninger kan behandles:

Kategori	Eksempler
Identitetsopplysninger	Navn, e-postadresse, telefonnummer, stillingstittel
Kontoinformasjon	Brukernavn, kryptert passord, innloggingshistorikk
Virksomhetsdata	Organisasjonsnummer, firmanavn, adresse, bransje
HMS-relaterte data	Risikovurderinger, avviksrapporter, handlingsplaner, HMS-dokumenter
Tekniske data	IP-adresse, enhetstype, nettlesertype, aktivitetslogger

3.3 Særlige kategorier

Avtalen omfatter ikke behandling av særlige kategorier av personopplysninger (sensitive personopplysninger) med mindre Behandlingsansvarlig uttrykkelig velger å registrere slike i Tjenesten. I så fall er Behandlingsansvarlig selv ansvarlig for å sikre lovlig behandlingsgrunnlag.

4. Behandlingsansvarliges plikter og rettigheter

4.1 Instruksjonsrett

Behandlingsansvarlig har rett til å gi dokumenterte instruksjoner om hvordan personopplysningene skal behandles. Databehandler skal kun behandle personopplysninger i samsvar med slike instruksjoner.

4.2 Ansvar for lovlighet

Behandlingsansvarlig er ansvarlig for at:

- Det foreligger gyldig behandlingsgrunnlag for personopplysningene
- De registrerte er informert om behandlingen
- Behandlingen er i samsvar med GDPR og annen relevant lovgivning

4.3 Kontrollrett

Behandlingsansvarlig har rett til å gjennomføre revisjoner og inspeksjoner for å verifisere at Databehandler overholder denne Avtalen, jf. punkt 10.

5. Databehandlers forpliktelser

5.1 Behandling etter instruks

Databehandler skal kun behandle personopplysninger etter dokumenterte instruksjoner fra Behandlingsansvarlig. Dersom Databehandler mener en instruks er i strid med GDPR eller annen personvernlovgivning, skal Databehandler umiddelbart varsle Behandlingsansvarlig.

5.2 Konfidensialitet

Databehandler skal sikre at personer som er autorisert til å behandle personopplysningene:

- Har forpliktet seg til konfidensialitet eller er underlagt lovbestemt taushetsplikt
- Kun behandler personopplysninger etter instruks fra Behandlingsansvarlig

5.3 Sikkerhetstiltak

Databehandler skal implementere følgende tekniske og organisatoriske tiltak for å sikre et passende sikkerhetsnivå (jf. GDPR artikkel 32):

Tekniske tiltak:

- SSL/TLS-kryptering for all dataoverføring
- AES-256-CBC kryptering for data i hvile (gjelder også sikkerhetskopier)
- Daglig sikkerhetskopiering med 30 dagers oppbevaring
- Tilgangskontroll med rollebasert autorisasjon
- Logging av sikkerhetshendelser

Organisatoriske tiltak:

- Tilgangsbegrensning etter minste privilegiums prinsipp
- Regelmessig sikkerhetsopplæring av personell
- Dokumenterte rutiner for hendelseshåndtering
- Regelmessig gjennomgang av sikkerhetstiltak

5.4 Bistand ved utøvelse av registrertes rettigheter

Databehandler skal bistå Behandlingsansvarlig med å oppfylle sine forpliktelser overfor registrerte, herunder:

- Innsyn i egne personopplysninger
- Retting av uriktige opplysninger
- Sletting ("retten til å bli glemt")
- Begrensning av behandling
- Dataportabilitet
- Innsigelse mot behandling

Bistand ytes gjennom Tjenestens innebygde funksjoner og ved henvendelse til support@vemento.no.

5.5 Bistand ved sikkerhetsbrudd og konsekvensutredninger

Databehandler skal:

- Bistå Behandlingsansvarlig med å oppfylle forpliktelsene i GDPR artikkel 32-36
- Bistå ved vurdering av personvernkonsekvenser (DPIA) når relevant
- Bistå ved forhåndsdrøftelser med Datatilsynet

6. Varsling ved brudd på personopplysningssikkerheten**6.1 Varslingsplikt**

Ved brudd på personopplysningssikkerheten skal Databehandler varsle Behandlingsansvarlig uten ugrunnet opphold, og senest innen 24 timer etter at bruddet ble oppdaget.

6.2 Innhold i varsel

Varselet skal minst inneholde:

- Beskrivelse av bruddets art
- Kategorier og omtrentlig antall berørte registrerte
- Kategorier og omtrentlig antall berørte personopplysningsregistre
- Navn og kontaktopplysninger til personvernkontakt
- Sannsynlige konsekvenser av bruddet
- Tiltak som er iverksatt eller foreslås for å håndtere bruddet

6.3 Dokumentasjon

Databehandler skal dokumentere alle brudd på personopplysningssikkerheten, herunder fakta om bruddet, dets virkninger og tiltak som er iverksatt.

7. Bruk av underleverandører (underdatabehandlere)

7.1 Godkjente underleverandører

Behandlingsansvarlig gir herved en generell forhåndsgodkjenning til bruk av følgende underleverandører:

Underleverandør	Tjeneste	Lokasjon
Microsoft Azure	Skyinfrastruktur og hosting	EU (West Europe)
Microsoft 365	E-postutsendelse	EU
Sanity.io	Innholdshåndtering (CMS)	EU
ServeTheWorld	Webhosting og CDN	EU

7.2 Nye underleverandører

Ved endringer i bruk av underleverandører skal Databehandler varsle Behandlingsansvarlig minst 30 dager før endringen trer i kraft. Behandlingsansvarlig kan protestere mot endringen innen denne fristen.

7.3 Underleverandørers forpliktelser

Databehandler skal sikre at alle underleverandører er bundet av tilsvarende forpliktelser som følger av denne Avtalen. Databehandler er fullt ansvarlig overfor Behandlingsansvarlig for underleverandørers oppfyllelse av forpliktelsene.

8. Overføring til tredjeland

8.1 Hovedregel

Personopplysninger skal som hovedregel behandles og lagres innenfor EU/EØS.

8.2 Overføring utenfor EU/EØS

Dersom det er nødvendig å overføre personopplysninger til land utenfor EU/EØS, skal Databehandler sikre at:

- Det foreligger gyldig overføringsgrunnlag (adequacy decision, SCCs, eller annet)
- Behandlingsansvarlig informeres om overføringen
- Nødvendige tilleggstiltak er implementert

9. Sletting og tilbakelevering av data

9.1 Ved avtalens opphør

Ved opphør av avtaleforholdet skal Databehandler, etter Behandlingsansvarligs valg:

- Slette alle personopplysninger, eller
- Tilbakelevere alle personopplysninger til Behandlingsansvarlig

9.2 Oppbevaringsperiode

Behandlingsansvarlig har 90 dager etter avtalens opphør til å eksportere sine data fra Tjenesten. Etter utløpet av denne perioden vil alle personopplysninger bli slettet.

9.3 Lovpålagt oppbevaring

Databehandler kan beholde personopplysninger i den grad det er påkrevd etter gjeldende lovgivning (f.eks. regnskapsloven). Slik oppbevaring skal dokumenteres.

9.4 Bekreftelse

Databehandler skal på forespørsel bekrefte skriftlig at sletting er gjennomført.

10. Revisjon og kontroll

10.1 Tilgjengeliggjøring av informasjon

Databehandler skal gjøre tilgjengelig for Behandlingsansvarlig all informasjon som er nødvendig for å påvise at forpliktelsene i GDPR artikkel 28 er oppfylt.

10.2 Revisjonsrett

Behandlingsansvarlig, eller en uavhengig tredjepart utpekt av Behandlingsansvarlig, har rett til å gjennomføre revisjoner og inspeksjoner. Slik revisjon skal:

- Varsles minst 14 dager i forveien
- Gjennomføres i normal arbeidstid
- Ikke urimelig forstyrre Databehandlers virksomhet

10.3 Kostnader

Behandlingsansvarlig bærer egne kostnader ved revisjon. Databehandler kan kreve rimelig kompensasjon for tidsbruk ved omfattende revisjoner ut over én årlig revisjon.

11. Ansvar og erstatning

11.1 Ansvarsbegrensning

Databehandlers erstatningsansvar er begrenset til direkte tap og kan ikke overstige det totale vederlag betalt av Behandlingsansvarlig de siste 12 måneder.

11.2 Unntak

Ansvarsbegrensningen gjelder ikke ved:

- Forsettlig eller grovt uaktsomt brudd på Avtalen
 - Brudd som skyldes manglende etterlevelse av Behandlingsansvarliges lovlige instruks
-

12. Avtalens varighet og oppsigelse

12.1 Ikrafttredelse

Avtalen trer i kraft når Behandlingsansvarlig oppretter en bedriftskonto i Tjenesten.

12.2 Varighet

Avtalen gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig.

12.3 Opphør

Avtalen opphører automatisk når:

- Hovedavtalen (brukervilkårene) sies opp
 - Alle personopplysninger er slettet eller tilbakelevert
-

13. Endringer i avtalen

13.1 Endringsadgang

Databehandler kan gjøre endringer i denne Avtalen dersom det er nødvendig for å:

- Overholde endringer i gjeldende lovgivning
- Implementere vedtak fra Datatilsynet eller andre myndigheter
- Forbedre sikkerhetstiltakene

13.2 Varsling

Ved vesentlige endringer skal Behandlingsansvarlig varsles minst 30 dager før endringene trer i kraft.

14. Lovvalg og tvister

14.1 Lovvalg

Avtalen er underlagt norsk rett.

14.2 Tvister

Tvister som oppstår i forbindelse med denne Avtalen skal søkes løst gjennom forhandlinger. Dersom partene ikke kommer til enighet, skal tvisten avgjøres ved Sandnes tingrett.

15. Kontaktinformasjon

Databehandler

Vemento AS Organisasjonsnummer: 929 628 675 Adresse: Bekkedalen 15, 4325 Sandnes E-post: kontakt@hmsveileder.no Nettsted: www.hmsveileder.no

For henvendelser vedrørende personvern og denne avtalen: E-post: kontakt@hmsveileder.no

16. Vedlegg

Vedlegg A: Tekniske og organisatoriske sikkerhetstiltak

Se punkt 5.3 for detaljert beskrivelse.

Vedlegg B: Liste over godkjente underleverandører

Se punkt 7.1 for oppdatert liste.

Sist oppdatert: 12. desember 2025

Denne databehandleravtalen er utarbeidet i henhold til GDPR artikkel 28 og Datatilsynets veiledning for databehandleravtaler.