

**GDPR** (General Data Protection Regulation for EU/EØS) er et nytt personvernregelverk som trer i kraft, i Norge, den 1. juli 2018. Lovverket setter rammer for innhenting og bruk av person opplysninger og styrker rettighetene til deg som enkeltperson.

*Vi i HAVA BHT arbeider kontinuerlig for å være i samsvar med personvernregelverket slik at alle våre kunder og brukere skal være trygge på at innhentet, lagret og kommunisert personinformasjon blir behandlet på en forsvarlig måte.*

All behandling av personopplysninger skal være lovlig, rettfærdig og gjennomiktig. Med personopplysning menes enhver opplysning om en identifisert eller identifiserbar fysisk person (den registrerte). Helseopplysninger knyttet til en person defineres som sensitive personopplysninger.

Hava BHT tar personvern på alvor. Våre medarbeidere som kommer i befatning med personopplysninger har taushetsplikt. Vår håndtering av disse opplysningene skjer i samsvar med den til enhver tid gjeldende personvern lovgivingen i tillegg til regelverket for helse- og bedriftshelsetjenester.

Vi har som mål å ivareta alle våre kunder og deres ansatte på en best mulig måte. Vi ønsker at våre kunder skal kjenne sine ansattes databeskyttelsesrettigheter og vårt juridiske grunnlag for å behandle person opplysninger i henhold til EUs nye personvernforordning.

## Rettslig grunnlag for innsamling av personopplysninger

I vårt virke som bedriftshelsetjeneste, henter vi inn, bruker og lagrer både opplysninger om virksomheten og personopplysninger om deres ansatte.

Det rettslige grunnlaget finnes i GDPR artikkel 6 og 9, Arbeidsmiljøloven, Helseregisterloven, Helsepersonelloven, Pasientjournalloven, Forskrift om utførelse av arbeid og Forskrift om pasientjournal.

## Personvernerklæring for HAVA BHT

For å kunne følge opp kundeforholdet og de ansattes helse, registrerer vi enkelte opplysninger som er knyttet til en person. Dette innbefatter kontaktinformasjon for å opprette en bedriftsjournal og eventuelt en pasientjournal (f.eks. navn, fødselsnummer, adresse og telefonnummer), administrasjon av timeavtaler, helseopplysninger for å kunne jobbe forebyggende og øvrige forpliktelser vi har for å fungere som bedriftshelsetjeneste. Vi vil kun samle inn og bruke de personopplysninger som er nødvendige.

## Datakontroll

Våre systemer for lagring og ivaretagelse med tilhørende databaser forenkler gjenfinning, bidrar til en bedre internkontroll og sikrer personvernet for våre kunders ansatte.

## Retting og sletting

Det er viktig at opplysningene vi har registrert er riktige. Våre kunders ansatte kan, på egne vegne, kreve at vi retter eller sletter personopplysninger hvis disse er mangelfulle eller unødvendige.

Retting og sletting av opplysninger i pasientjournal er hjemlet i regelverket – som også gir noen begrensede unntak. Har du spørsmål om dette så kan du ta kontakt med oss.

Vi sletter registrerte personopplysninger når de ikke lenger er nødvendige for å oppfylle formålet de ble innhentet for. For pasientjournaler gjelder egne regler om oppbevaring og oppbevaringstid.

Allmennelseopplysninger skal, i utgangspunktet, slettes når det her gått mer enn 10 år etter siste journalpåføring. Unntaksvis skal pasientjournaler for ansatte som har vært utsatt for risikofylte eksponeringer; som asbeststøv, bly, kreftfremkallende kjemikalier, bergarbeid, m.fl., oppbevares i opptil 60 år.

## Innsyn

Registrerte ansatte hos våre medlemsbedrifter kan, på egne vegne, be om å få informasjon om hvilke personopplysninger vi behandler og hvordan vi håndterer disse.

Dette inkluderer den ansattes rett til innsyn i egen pasientjournal, hvem som har hatt tilgang til denne og hvem som har fått utlevert opplysninger herfra. Det som står i pasientjournalen er taushetsbelagt og vil ikke bli delt med andre, med mindre den ansatte/pasienten samtykker til dette.

Ledere, personal- eller HMS-ansvarlige kan få oversendt lister over deltagere ved lovpålagte leveranser (f.eks. arbeidshelseundersøkelser og yrkesvaksinering) og eventuelt helse erklæringer med konklusjon på skikkethet av helsen (som f.eks. godkjent/ikke godkjent).

## Databehandling av personopplysninger

HAVA BHT systematiserer innhentet bedriftshelseinformasjon i en database, der innsamlede data lagres sikkert enten i bedriftsjournal eller i pasientjournal. HAVA BHT sine faste medarbeidere har autorisert tilgang til bedriftsjournal med opplysninger om bedriften.

Når våre kunders ansatte mottar bedriftshelsetjenester, har vårt helsepersonell plikt til å føre en pasientjournal. I pasientjournalen registrerer vi de opplysningene som er nødvendige for å gi riktig tjeneste eller behandling, f.eks. sykdomshistorikk, tidligere behandling, medikamentbruk, resepter, diagnoser, prøveresultater, opplysninger fra andre behandlingssteder m.m.

Tilgang til pasientjournal er systematisk begrenset til helsepersonell og medhjelpere som bistår med bedriftshelsetjenester. Helselovgivningen gir klar føring på begrensning av innsyn i pasientjournal til helsepersonell med behandlerfunksjon.

Sammen med våre systemleverandører arbeider vi med å få gode og sikre personvernløsninger i våre helsesystemer.

## Databehandleravtale

HAVA BHT defineres som behandlingsansvarlig for personopplysninger fra ansatte hos våre kunder etter inngått avtale, både i forbindelse med leveranse av bedriftshelsetjenester og øvrige helsetjenester.

HAVA BHT inngår ikke databehandleravtaler med sine kunder. HAVA BHT behandler personopplysninger selvstendig som en del av tjenesteleveransene og ikke på vegne av eller etter instruks fra våre kunder.

Det at vi som bedriftshelse mottar ansattlister med navn, fødselsnummer, mailadresse og avdelingstilhørighet fra kundene, fordrer i seg selv ingen databehandleravtale, fordi dette anses som en overføring av data mellom to selvstendige behandlings-ansvarlige. Dette er også i henhold til Datatilsynets vurdering av ansvar for levering av bedriftshelsetjenester.

Som bedriftshelsetjeneste har HAVA BHT en fri og uavhengig stilling i arbeidshelse spørsmål og er ansvarlig for å operere i tråd med de krav som følger av lov og forskrift.

## Datasikkerhet

HAVA BHT er bevisst sitt ansvar for å vurdere sikkerhetsrisiko og konfidensialitet i forhold til personvernet. Det er viktig for oss at informasjonen vi sitter på blir behandlet i tråd med gjeldende lovverk og forskrifter. Ingen registrerte personopplysninger skal være tilgjengelig for uvedkommende. Medarbeidere i HAVA BHT, som gis tilgang til beskyttelsesverdige personopplysninger, må underskrive en taushetserklæring og skal ha et konkret tjenestebehov for å åpne en pasientjournal.

For å ivareta sikkerheten i registrerte personhelseopplysninger er det viktig at også all kommunikasjon er trygg. Helseopplysninger og andre sensitive opplysninger skal ikke sendes via e-post eller på andre (*inklusive sosiale*) medier som ikke ivaretar konfidensialiteten. Våre kunder blir informert om sikre måter for å utveksle personopplysninger.

Et eventuelt sikkerhetsbrudd vil bli varslet innen kort tid i henhold til GDPRs strenge krav til avvikshåndtering. Innhold i varslet og hvem som skal varsles er gjort kjent i vår organisasjon.

## Kontaktinformasjon

Dersom du har behov for å komme i kontakt med oss i forbindelse med vår jobb som databehandler, er våre kontaktopplysninger som følger:

Epost: [post@hava.no](mailto:post@hava.no)  
Telefon: 32 08 63 80