

AVTALE OM BEHANDLING AV HELSE- OG  
PERSONOPPLYSNINGER  
(DATABEHANDLERAVTALE) I FORBINDELSE  
MED DRIFT AV HELSENETTET OG  
TILKNYTTEDE TJENESTER  
(HERETTER OMTALT SOM «AVTALEN»)

## 1. AVTALENS PARTER

Avtalen gjelder mellom databehandlingsansvarlig virksomhet, som har godtatt vilkår for medlemskap i Helsenettet, og databehandler Norsk Helsenett SF, org. Nr. 994 598 759. Databehandlingsansvarlige og databehandler samlet kalles heretter «partene».

Databehandlingsansvarliges navn, organisasjonsnummer og øvrig kontaktinformasjon finnes i databehandlers kundesystem, basert på databehandlingsansvarliges egne opplysninger.

Når databehandlingsansvarlig er kjedeeier, er kjedeeier ansvarlig for at egne avdelinger følger databehandleravtalen.

## 2. BAKGRUNN

Helsenettet er en lukket og sikret kommunikasjonsarena som består av alle tilknyttede virksomheter, de tjenestene de benytter, samt de kommunikasjonselementene og –systemene som binder dem sammen. I Helsenettet utveksles helse- og personopplysninger om innbyggerne i Norge innenfor rammen av den til enhver tid gjeldende "Norm for informasjonssikkerhet i helse- og omsorgstjenesten". Norsk Helsenett drifter Helsenettet på vegne av alle tilknyttede virksomheter.

Tilknytning til Helsenettet betinger aksept av vilkår for medlemskapet, og tilgang til tjenester reguleres i egne avtaler.

## 3. DATABEHANDLERAVTALENS HENSIKT OG OMFANG

Denne databehandleravtalen regulerer vilkårene for databehandlers behandling av helsepersonopplysninger på vegne av databehandlingsansvarlig når databehandler drifter de tjenestene kunden benytter - Helsenettet. Avtalen regulerer partenes rettigheter og plikter som følge av at databehandlingsansvarlig tegner medlemskap i Helsenettet og benytter de tjenestene databehandler drifter. De tjenester som innebærer behandling av personopplysninger er angitt i Bilag 1 til databehandleravtalen.

Avtalen regulerer partenes rettigheter og plikter etter personopplysningsloven og helselovgivningen. Helseopplysninger og personopplysninger betegnes i avtalen heretter med fellesbegrepet «personopplysninger».

Formålet med behandlingen av personopplysningene er å understøtte databehandlingsansvarliges behov for elektroniske løsninger i forbindelse med helsehjelp og tilhørende administrative oppgaver. Behandlingens art er 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.

Personopplysningene som skal behandles etter avtalens regulering gjelder opplysninger om databehandlingsansvarliges pasienter, kunder og ansatte. Disse opplysningene kan knyttes til informasjon om personalia, helseopplysninger og elektroniske spor.

Der databehandlingsansvarlig velger å ta i bruk nye tjenester i Helsenettet, skal det avklares om behandlingen ligger innenfor samme formål som det denne avtalen regulerer. Dersom den ligger innenfor samme formål, gjelder denne databehandleravtalen.

Avtalen er underlagt personopplysningslovens regulering, og følgelig forordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger, og om fri utveksling av slike opplysninger (heretter omtalt som «personvernforordningen»). Ved motstrid mellom avtalens regulering og de rammer som følger

av personopplysningsloven eller personvernforordningen, viker avtalens regulering.

#### 4. DATABEHANDLERS PLIKTER

Så lenge avtalen gjelder skal databehandler:

- a. sikre at databehandlers behandling av personopplysninger er i overensstemmelse med all relevant lovgivning om personopplysninger, og den til enhver tid gjeldende "Norm for informasjonssikkerhet i helse- og omsorgstjenesten";
- b. bare behandle personopplysninger etter dokumenterte instruksjoner som den databehandlingsansvarlige til enhver tid har bestemt skal gjelde, og ikke behandle personopplysninger utover hva som er nødvendig for å oppfylle databehandlers forpliktelser i sammenheng med driften av Helsenettet og tjenestene som tilbys der;
- c. ikke utlevere eller overlate personopplysninger til andre, herunder til stater utenfor EØS, med mindre databehandlingsansvarlig har godkjent dette skriftlig;
- d. etablere og etterkomme nødvendige tekniske og organisatoriske tiltak med hensyn til vedvarende konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger for å sikre tilfredsstillende informasjonssikkerhet i henhold til personopplysningslovens bestemmelser, herunder kravene etter personvernforordningen artikkel 32. Dette omfatter blant annet, alt etter hva som er relevant, nødvendige tiltak for å forhindre tilfeldig eller ulovlig ødeleggelse eller tap av data, ikke-autorisert tilgang til eller spredning av data så vel som enhver annen bruk av personopplysninger som ikke er i overensstemmelse med denne avtalen og tiltak for å gjenopprette tilgjengelighet og tilgang til personopplysninger ved hendelser;
- e. ha rutiner for autorisasjon og styring som sikrer at bare de av databehandlers medarbeidere som har reelt behov for tilgang til systemer og opplysninger for å ivareta nødvendige oppgaver for drift av Helsenettet og tjenestene. Tilgangsnivået skal være i henhold til reelt behov knyttet til å gjennomføre driften, og tilgangen skal være basert på individuelle brukernavn og passord;
- f. i henhold til databehandlers rutiner avdekke, registrere, rapportere og lukke avvik knyttet til informasjonssikkerhet, herunder loggføre og dokumentere ethvert forsøk på ikke-autorisert tilgang og andre brudd på sikkerheten i datasystemet. Slik dokumentasjon skal oppbevares hos databehandler;
- g. varsle Datatilsynet ved uautorisert utlevering av personopplysninger;
- h. registrere all autorisert og uautorisert tilgang til informasjon. Alle oppslag som gjøres skal registreres slik at de kan spores til den enkelte bruker (dvs. ansatte hos databehandler, underleverandører og databehandlingsansvarlig). Loggene skal oppbevares til det ikke lenger antas å være bruk for dem eller i henhold til det driftsavtalen spesifiserer;
- i. bistå databehandlingsansvarlig, idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for databehandleren, med å sikre overholdelse av forpliktelsene knyttet til personvernforordningen artiklene 32–36, dvs.
  - sikkerhet ved behandlingen
  - melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten
  - underretning av den registrerte om brudd på personopplysningssikkerheten
  - vurdering av personvernkonsekvenser og forhåndsdrøftinger;
- j. etablere rutiner for å slette informasjon når den ikke lenger er nødvendig ut fra formålet med behandlingen;
- k. idet det tas hensyn til behandlingens art og i den grad det er mulig, samarbeide med og

assistere databehandlingsansvarlig ved oppfyllelse av de registrertes rettigheter knyttet til tilgang til opplysninger, herunder å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III;

- I. omgående underrette den databehandlingsansvarlige dersom vedkommende mener at en instruks er i strid med denne forordning eller andre bestemmelser om vern av personopplysninger.

Ved brudd på denne avtalen kan databehandlingsansvarlig pålegge databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Databehandler skal dokumentere sine rutiner og alle tiltak truffet for å oppfylle kravene angitt ovenfor. Denne dokumentasjonen skal på forespørsel gjøres tilgjengelig for den databehandlingsansvarlige.

Databehandler plikter å påse at samtlige personer som gis tilgang til personopplysninger som behandles på vegne av databehandlingsansvarlig, er kjent med denne avtalen og underlagt avtalens bestemmelser.

Meddelelser, underretting, varsel eller annen kommunikasjon mellom behandlingsansvarlig og databehandler, skal sendes elektronisk til den e-postadresse som fremgår av databehandlingsansvarliges kontaktinformasjon.

## **5. DEN DATABEHANDLINGSANSVARLIGES PLIKTER**

Databehandlingsansvarlig skal etterleve de forpliktelser som følger av personopplysningsloven, forordningen og annen lovgivning samt denne avtalen, herunder å gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med det foran nevnte.

## **6. TAUSHETSPLIKT**

Databehandler behandler en rekke typer informasjon som må behandles konfidensielt.

Databehandlers ansatte og andre som opptrer på databehandlers vegne i forbindelse med behandling av personopplysninger i henhold til denne avtalen (heretter omtalt som «personer som er autorisert til å behandle personopplysningene»), er underlagt taushetsplikt, jf. personopplysningsloven og annen relevant lovgivning. Personer som er autorisert til å behandle personopplysningene forplikter seg til videre å behandle opplysningene fortrolig. Det samme gjelder eventuelle underleverandører. Databehandler skal påse at alle som behandler personopplysninger under avtalen er kjent med taushetsplikten.

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

Taushetsplikten gjelder også etter avtalens opphør.

Partene plikter å ta de forholdsregler som er nødvendige for å sikre at materiale eller opplysninger ikke blir gjort kjent for andre i strid med dette punktet.

## **7. INNSYN OG REVISJON MV.**

Databehandlingsansvarlig kan til enhver tid kreve innsyn i databehandlers behandling av personopplysninger tilhørende databehandlingsansvarlig, herunder i dokumentasjon for oppfyllelse av kravene til informasjonssikkerhet og databehandlers system for internkontroll. Retten til innsyn gjelder alle tekniske, organisatoriske og administrative forhold som er relevante for sikkerheten ved behandlingen av opplysningene som utføres av databehandler

på vegne av databehandlingsansvarlig, og øvrige innsynsrettigheter nedfelt i lov. En databehandlingsansvarlig som ber om innsyn skal gjøre generell informasjon fra revisjonen tilgjengelig for andre databehandlingsansvarlige som benytter samme tjeneste.

Databehandlingsansvarlig skal hvis mulig gi databehandler varsel i rimelig tid før krav om innsyn og kontroll, vanligvis minst 30 dagers varsel. For krav om dokumentinnsyn bør det gis minst 14 dagers varsel. Databehandlingsansvarlig skal medvirke til at innsyn og kontroll kan koordineres mellom flere databehandlingsansvarlige som får levert tjenester fra databehandler. Innsyn og kontroll kan gjennomføres av databehandlingsansvarlig eller den tredjepart databehandlingsansvarlige måtte velge til gjennomføring. Databehandler kan kreve dekket dokumenterte merkostnader som påløper ved slike revisjoner.

Databehandler skal gi Datatilsynet og annen relevant tilsynsmyndighet slik tilgang og innsyn i behandlingen av personopplysninger som følger av personopplysningsloven.

Databehandler skal uten ugrunnet opphold korrigere eventuelle avvik. Avvik som skyldes databehandler eller dennes underleverandører, skal korrigeres uten kostnad for databehandlingsansvarlig. Databehandler skal skriftlig redegjøre for korrektive tiltak og plan for gjennomføring.

## 8. BRUK AV UNDERLEVERANDØR

Databehandlingsansvarlig tillater at databehandler benytter underleverandører for oppfyllelse av forpliktelsene under avtalen.

Databehandler skal sikre at underleverandøren påtar seg tilsvarende forpliktelser som databehandleren under denne avtalen. Databehandler er fullt ut ansvarlig overfor databehandlingsansvarlig for alt arbeid som utføres av egne underleverandører.

Databehandleren skal underrette den databehandlingsansvarlige om eventuelle planer om å benytte andre databehandlere eller skifte ut databehandlere. En oppdatert oversikt over databehandlers underleverandører finnes ved oppslag på [www.nhn.no](http://www.nhn.no). Endringer i denne oversikten skal fremgå samme sted, slik at databehandlingsansvarlige gis mulighet til å motsette seg endringen.

Tilgang til personopplysninger for eksterne tredjeparter krever konkret avtale mellom partene utover denne avtalen for alle andre enn databehandlers underleverandører.

## 9. AVTALEPERIODE

Avtalen gjelder fra den er signert av partene og til det tidspunkt databehandlingsansvarlig avslutter sitt medlemskap i Helsenettet.

Avtalen skal revideres ved endringer som går utover avtalt formål og omfang etter denne avtalen. Databehandler vil ta initiativ til slik revisjon og foreslå nødvendige endringer. Avtalen skal også revideres hvis sikkerhetsrevisjoner eller nye krav gjennom lovgivning viser at dette er nødvendig.

## 10. OPPHØR AV AVTALEN

Ved opphør av avtalen skal databehandler tilrettelegge for og medvirke til tilbakeføring av alle opplysninger som databehandler har behandlet på vegne av databehandlingsansvarlig. Partene avtaler nærmere hvordan overføring konkret skal skje.

Etter at alle opplysningene er overført til databehandlingsansvarlig og bekreftet mottatt av denne, skal databehandler slette opplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene i sine systemer, med mindre ufravikelige rettsregler krever at

personopplysningene fortsatt skal lagres.

Benyttes delt infrastruktur der direkte sletting ikke er teknisk mulig, skal databehandler sørge for at data gjøres utilgjengelig inntil disse dataene er overskrevet av systemet.

Databehandler skal gi databehandlingsansvarlig skriftlig bekreftelse på at opplysningene er overført og slettet som angitt over.

## **11. AKSEPT AV AVTALE**

Denne avtalen er akseptert av begge parter og arkivert på databehandlingsansvarliges side på [www.nhn.no](http://www.nhn.no) .

## **12. VERNETING**

Partene vedtar Trondheim tingrett som verneting. Dette gjelder også etter opphør av avtalen.

## BILAG 1

### **DATABEHANDLERAVTALEN OM BEHANDLING AV HELSE- OG PERSONOPPLYSNINGER (DATABEHANDLERAVTALE) I FORBINDELSE MED DRIFT AV HELSENETTET**

#### **TJENESTER SOM INNEBÆRER BEHANDLING AV PERSONOPPLYSNINGER**

Nedenfor er en beskrivelse av informasjonselementene som er benyttet i tabellen nedenfor.

#### **TJENESTENS NAVN**

Oversikt over de tjenester Norsk Helsenett leverer til medlemmet i Helsenettet som innehar personopplysninger. Ytterligere informasjon om tjenestene finnes på [www.nhn.no](http://www.nhn.no).

#### **PERSONOPPLYSNINGER**

Personopplysninger er enhver opplysning som kan knyttes til en identifisert eller identifiserbar fysisk person.

#### **BEHANDLING**

Med behandling menes enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger.

#### **HENSIKTEN MED BEHANDLINGEN**

Her beskrives hva behandlingen av personopplysninger handler om.

#### **FORMÅLET MED BEHANDLING AV PERSONOPPLYSNINGER**

Med formålet menes til hvilket formål personopplysningene behandles.

#### **VARIGHETEN AV BEHANDLINGEN AV PERSONOPPLYSNINGER**

Når det ikke lenger er nødvendig å behandle personopplysninger for å gjennomføre formålet med behandlingen, skal opplysningene slettes.

**BEHANDLINGENS ART**

Her angis hvilken type behandling som gjøres, f.eks. registrering, lagring, bruk, utlevering eller annen behandling.

**TYPE PERSONOPPLYSNINGER**

Her angis type opplysning, f.eks. navn, personnummer, adresse eller andre identifikatorer.

**KATEGORIER AV REGISTRERTE**

De registrerte kategoriseres som f.eks. medlem, kunde, bruker, mv.

**OVERSIKT OVER TJENESTER MED PERSONOPPLYSNINGER SOM ER TILGJENGELIG FOR MEDLEMMER AV HELSENETTET**

Tjenestens navn	Innholdet i tjenesten	Formålet med behandlingen	Behandlings varighet	Behandlings art	Type personopplysninger	Kategorier registrerte
Elektronisk meldingsutveksling	Tjeneste for sikker elektronisk transport i helse- og omsorgstjenesten	Å transportere meldinger mellom aktører i Helsenettet	Inntil kunde har hentet ned melding fra meldingstjenesten.	Transport, mellomlagring	Navn, adresse fødselsnummer	Pasienter, brukere
Adresseregisteret	Samlet oppdatert adresse for alle tilknyttede virksomheter for elektronisk kommunikasjon	Å gi helse- og omsorgssektoren korrekte adresser for elektronisk kommunikasjon.	Så lenge kundeforholdet består	Transport, mellomlagring	Navn, adresse, epostadresse	Personell i helse- og omsorgstjenesten
Videotjenesten	Tjeneste for kommunikasjon ved hjelp av lyd og bilde i møter, undervisning, behandling mv	Pasientbehandling, undervisning og møtevirkosmhet	Konsultasjon: Så lenge videosamtalen pågår. Ingen lagring eller mellomlagring av personopplysninger. Undervisning: Opptak slettes etter 14 dager.	Transport, mellomlagring, lagring av opptak	Navn, bilde	Pasienter, brukere, Personell i helse- og omsorgstjenesten
Fjernhjelp	Tjeneste som muliggjør ekstern bistand med	Å gi tredjepartsleverandører tilgang til maskiner i	I oppdragsperioden	Mulighet for å gå inn i alle kundens systemer	Navn, adresse, helseopplysninger	Pasienter, brukere



Tjenestens navn	Innholdet i tjenesten	Formålet med behandlingen	Behandlingens varighet	Behandlingens art	Type personopplysninger	Kategorier registrerte
	brukerstøtte og vedlikehold	Helsenettet for å gjøre support- og driftsoppgaver		Transport, mellomlagring		
Samband	Leveranse av transporttjeneste for data i Helsenettet	Å gi kunden en tilknytning til Helsenettet	Så lenge kundeforholdet består	Transport	Personopplysninger	Pasienter, brukere
NHN fjernhjelp	Tjeneste der Norsk Helsenett gis aksess til virksomhetens utstyr	Å gi NHN tilgang til utstyr Helsenettet for å gjøre supportoppgaver	I oppdragsperioden	Mulighet for å gå inn i alle kundens systemer Transport, mellomlagring	Navn, adresse, helseopplysninger	Pasienter, brukere