Databehandleravtale

I henhold til helseregisterlovens § 16, jf. § 18 og
personopplysningsforskriftens kapittel 2.
mellom

Bærum kommune, Pleie- og omsorg

_____

databehandlingsansvarlig

og

Leverandør

_____

databehandler

Innholdsfortegnelse

1. Innledning

Forholdet mellom en behandlingsansvarlig og en databehandler skal være regulert i en avtale – databehandleravtale, jf. personopplysningslovens § 13, jf. § 15. Tilsvarende gjelder for helseregisterlovens § 16, jf. § 18.

Kommunen er databehandlingsansvarlig og Leverandør er databehandler.

Behandlingsansvarlig:

- Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes, jf. personopplysningslovens § 2 nr. 4 (helseregisterlovens § 2 nr. 8).
- Har ansvaret for at opplysninger behandles i henhold til de krav som personopplysningsloven oppstiller.

En behandling av personopplysninger er enhver bruk av personopplysninger, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

Databehandler:

- Den som behandler personopplysninger på vegne av den behandlingsansvarlige, jf. personopplysningslovens § 2 nr. 5 (helseregisterlovens § 2 nr. 9).
- Har et selvstendig ansvar for å ha tilfredsstillende informasjonssikkerhet, for å verne personopplysningene som behandles på vegne av behandlingsansvarlige jf. personopplysningslovens § 13 (helseregisterlovens § 16).
- skal bare behandle personopplysninger i henhold til avtale med den behandlingsansvarlige

2. Avtalens hensikt

Avtalens hensikt er å regulere rettigheter og plikter etter Lov av 18. mai 2001 nr. 24 om helseregistre og behandling av helseopplysninger (helseregisterloven) og forskrift av 15. desember 2000 nr. 1265 (personopplysningsforskriften). Avtalen skal sikre at personopplysninger om de registrerte ikke brukes urettmessig eller kommer uberettigede i hende, og at krav til konfidensialitet, integritet, tilgjengelighet og kvalitet ivaretas i henhold til helseregisterloven og personopplysningsloven m/forskrift.
Avtalen regulerer Databehandlers bruk av personopplysninger på vegne av den Databehandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse.

3. Krav til informasjonssikkerhet Databehandlers plikter

Databehandler plikter å behandle personopplysninger slik at krav til konfidensialitet, integritet, tilgjengelighet og kvalitet er ivaretatt etter Helseregisterloven §§ 16 og 18, Personopplysingsloven § 13, personopplysningsforskriften § 2-15 og Norm for informasjonssikkerhet.

Databehandler plikter å følge Norm for informasjonssikkerhet og oppfylle alle kravene i denne.
Norm for informasjonssikkerhet kan leses i sin helhet på www.normen.no, der er også lenker til Veiledere og faktaark.

Databehandler har det praktiske ansvaret for at tilfredsstillende informasjonssikkerhet er etablert gjennom planlagte og systematiske tiltak. Databehandler skal oversende dokumentasjon til Databehandlingsansvarlige med beskrivelse av mål og strategi for informasjonssikkerheten.
Dette skal skje første gang ved avtaleinngåelse og når denne avtalen blir revidert.

Databehandler plikter å behandle *helse- og personopplysninger* i henhold til avtale med databehandlingsansvarlig

Ingen andre enn databehandleren, de som arbeider under databehandlerens instruksjonsmyndighet og virksomheten selv har tilgang til *opplysningene.*
Databehandler skal i denne sammenheng også påse at det er iverksatt tiltak slik at Normens nivå for akseptable risiko følges.

Databehandler plikter å dokumentere sitt system for behandling av helse- og personopplysninger i forbindelse med databehandleravtalen. Med dokumentasjon menes bl.a. beskrivelse av prosedyrer for autorisasjon, autentisering og bruk, samt tekniske og organisatoriske sikkerhetstiltak. Dokumentasjon skal være tilgjengelig for databehandlingsansvarlig, sikkerhetsansvarlig i kommunen, Datatilsynet og Helsetilsynet

Databehandler skal til enhver tid oppfylle de krav til informasjonssikkerhet som følger av databehandleravtale og databehandlingsansvarliges sikkerhetsstrategi. Resultat fra gjennomført risikovurdering skal fremlegges av databehandler som dokumentasjon av egen og eventuelle underleverandørers sikkerhet.

Databehandler plikter å sørge for at ansatte har tilstrekkelig kompetanse i informasjonssikkerhet. Normen.no Faktaark : http://helsedirektoratet.no/lover-regler/norm-for-informasjonssikkerhet/velg-funksjon/medarbeider-ansatt/Sider/default.aspx

Databehandler skal følge de rutiner og instrukser for behandlingen som databehandlingsansvarlig til enhver tid har bestemt skal gjelde.

4. Krav til tilgangskontroll

Databehandler skal ha prosedyrer for autorisasjon og tilgangsstyring som sikrer at det bare gis tilgang der det er nødvendig for vedkommendes arbeid eller har særskilt hjemmel i lov eller forskrift.

Databehandler skal ha prosedyrer/løsninger for hendelsesregistrering som gjør det mulig for databehandlingsansvarlig å føre kontroll med hendelsesregistre. All autorisert tilgang, ethvert forsøk på ikke-autorisert tilgang, samt andre brudd på sikkerheten i systemet skal registreres og varsles til behandlingsansvarlige og sikkerhetsansvarlige.
Databehandler plikter å følge virksomhetens akseptkriterier (iht risikovurdering).

5. Taushetsplikt

Databehandlers ansatte og andre som opptrer på databehandlers vegne i forbindelse med behandling av helse- og personopplysninger i henhold til databehandleravtalen er underlagt taushetsplikt, jf. helseregisterloven § 15, helsepersonelloven og forvaltningsloven. Det samme gjelder eventuelle underleverandører.

Databehandler skal påse at alle som behandler helse- og personopplysninger er kjent med taushetsplikten.

Alle ansatte og andre som opptrer på databehandlers vegne i forbindelse med behandling av helse- og personopplysninger skal ha undertegnet taushetserklæring. Bestemmelsen gjelder tilsvarende for eventuelle Underleverandører

Taushetsplikten gjelder også etter databehandleravtalens opphør
Partene plikter å ta de forholdsregler som er nødvendig for å sikre at materiale eller opplysninger ikke blir gjort kjent for andre i strid med dette punktet

6. Den registrertes rettigheter

Databehandler plikter å ivareta den registrertes rettigheter.
Henvendelser fra den registrert med anmodning om innsyn, personopplysningsloven § 18, helseregisterloven § 22, pasientrettighetslovens kap. 5 skal skje i henhold til avtalt prosedyre.
Henvendelser fra den registrerte med anmodning om retting, sletting og sperring, personopplysningsloven § 27 og § 28, helseregisterlovens kap. 5, pasientrettighetslovens kap. 5 skal skje i henhold til avtalt prosedyre.

7. Bruk av underleverandør

Dersom databehandler benytter seg av underleverandør eller andre som ikke normalt er ansatt hos databehandler skal dette avtales skriftlig med databehandlingsansvarlige før behandlingen av personopplysninger starter.

Samtlige som på vegne av databehandler utfører oppdrag der bruk av de aktuelle personopplysningene inngår, skal være kjent med databehandlers avtalemessige og lovmessige forpliktelser og oppfylle vilkårene etter disse.

8. Sikkerhet

Databehandler skal oppfylle de krav til sikkerhetstiltak som stilles etter personopplysningsloven og personopplysningsforskriften, herunder særlig helseregisterlovens §§ 16 – 18 og personopplysningsforskriftens kap. 2 og 3. Databehandler skal dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjonen skal være tilgjengelig på databehandlingsansvarliges forespørsel.

Avviksmelding etter personopplysningsforskriftens § 2-6 skal skje ved at databehandler melder avviket til databehandlingsansvarlig. Databehandlingsansvarlig har ansvaret for at avviksmelding sendes Datatilsynet dersom avviket har ført til uautorisert utlevering av personopplysninger.

9. Sikkerhetsrevisjoner

Sikkerhetsrevisjon skal kunne gjennomføres jevnlig av sikkerhetsansvarlige og/eller databehandlingsansvarlig.

Revisjonen vil omfatte gjennomgang av rutiner og stikkprøvekontroller.

10. Avtalens varighet

Avtalen gjelder så lenge databehandler behandler helse- og personopplysninger på vegne av databehandlingsansvarlig, jf. avtalen mellom kommunen og leverandør om levering av tjenester.

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

11. Ved opphør

Når avtaleforholdet opphører, skal databehandler straks tilbakelevere dokumenter og alle elektroniske data på det medium (f.eks.: tape, CD, papir mv) som databehandler måtte besitte i egenskap av å være databehandler.
I avtalen for tjenesteutsetting er det avtalt tilbakeføring av helse- og personopplysninger til databehandlingsansvarlig ved opphør av avtalen.
Databehandler har ikke rett til å beholde en kopi av materialet.

Databehandlingsansvarlig skal ha en skriftlig bekreftelse fra databehandler på at alt materiale er overlevert til virksomheten og at databehandler ikke selv har beholdt noen kopi, avskrift eller annen gjengivelse av noen del av materialet på noe medium.

Databehandler er også etter at avtaleforholdet er avsluttet, bundet av taushetsplikten for de helse- og personopplysningene som er behandlet.
Etter at helse- og personopplysningene er overført til databehandlingsansvarlig, og bekreftet mottatt av denne, skal databehandler slette opplysningene i sitt system. Kravet til sletting omfatter også sikkerhetskopier av helse- og personopplysningene.

Databehandler skal skriftlig dokumentere at sletting og eller destruksjon er foretatt i henhold til avtalen innen rimelig tid etter avtalens opphør.

12. Forholdet til lov

Denne avtalen viker for gjeldende lover (Lov av 18. mai 2001 nr. 24 om helseregistre og behandling av helseopplysninger (helseregisterloven) og forskrift av 15. desember 2000 nr. 1265 (personopplysningsforskriften)) i den grad den er i strid med disse.

13. Meddelelser

Meddelelser etter denne avtalen skal sendes skriftlig til:
Databehandlingsansvarlige Bærum kommune ved: Kristin Standal, e-post: kristin.standal@baerum.kommune.no

14. Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar Asker og Bærum tingrett som verneting. Dette gjelder også etter opphør av avtalen.

***

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

Sted og dato

Databehandlingsansvarlig	**Databehandler**
……..	……
(underskrift)	(underskrift)