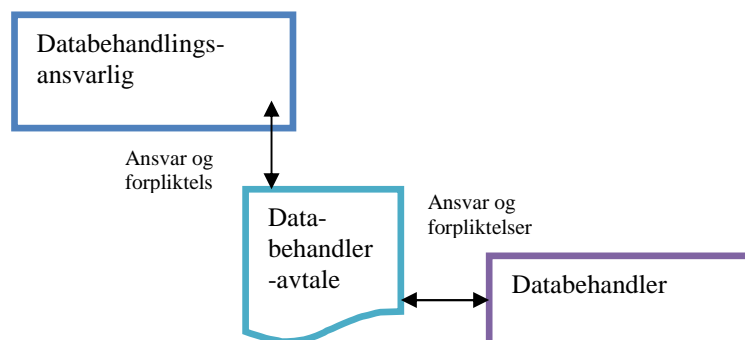


		Utgitt med støtte av:  Helsedirektoratet
Norm for informasjonssikkerhet <a href="http://www.normen.no">www.normen.no</a>		
<b>Bruk av databehandler (ekstern driftsenhet)</b>		<b>Støttedokument</b> <b>Faktaark nr 10</b> Versjon: 3.0 Dato: 15.12.2010

<b>Målgruppe</b> Dette faktaarket er spesielt relevant for:	<input checked="" type="checkbox"/> Leverandør <input checked="" type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Forsker <input checked="" type="checkbox"/> Prosjektleder	<input checked="" type="checkbox"/> Sikkerhetsleder/sikkerhetskoordinator <input checked="" type="checkbox"/> Virksomhetens leder/ledelse <input checked="" type="checkbox"/> Forskningsansvarlig	<input type="checkbox"/> Medarbeider/ansatt <input checked="" type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
<b>Ansvar</b>	Databehandlingsansvarlig v/virksomhetens ledelse har ansvar for å utforme databehandleravtale med databehandler (den eksterne driftsenheten). Databehandler har et selvstendig ansvar for å påse at behandling av helse- og personopplysninger skjer i samsvar med lovverket, samt at Normen følges om dette er avtalefestet.		
<b>Gjennomføring</b>	Når helse- og personopplysninger behandles av ekstern driftsenhet, eller når ekstern leverandør gjennomfører vedlikehold eller oppdatering som krever tilgang til helse- og personopplysninger.		
<b>Formål</b>	At helse- og personopplysninger ikke skal behandles av databehandler på annen måte enn det som er avtalt med databehandlingsansvarlig.		
<b>Omfang</b>	Alle virksomheter i helsesektoren skal inngå en databehandleravtale når helse- og personopplysninger driftes eksternt. Omfanget av databehandleravtalen må være tilpasset og avgrenset til behandlinger av helse- og personopplysninger som skal settes ut til den eksterne driftsenheten. Det skal også inngås tilsvarende avtaler med sikkerhetsleverandører som gjennomfører sikkerhetstiltak.		
<b>Hjemmel</b>	<ul style="list-style-type: none"> <li>• Helseregisterloven §§ 16 og 18</li> <li>• Personopplysningsloven § 13</li> <li>• Personopplysningsforskriften § 2-15</li> </ul>		
<b>Referanser</b>	<ul style="list-style-type: none"> <li>• Norm for informasjonssikkerhet, kapittel 5.8</li> <li>• Faktaark 15 – Hendelsesregistrering og oppfølging</li> <li>• Veileder for fjernaksess for vedlikehold og oppdateringer mellom leverandør og helsevirksomhet</li> <li>• Veileder for personvern og informasjonssikkerhet i forskningsprosjekter innenfor helse- og omsorgssektoren</li> <li>• Veileder i informasjonssikkerhet ved tilknytning mellom kommuner, fylkeskommuner og helsenettet</li> </ul>		

## Bakgrunn

En databehandleravtale er en avtale mellom databehandlingsansvarlige og databehandler (ekstern driftsenhet). En databehandler er en ekstern person eller virksomhet utenfor den databehandlingsansvarliges virksomhet. Databehandleren behandler helse- og personopplysninger på vegne av den databehandlingsansvarlige. Dette betyr at hvis helseforetakets IKT-systemer (alle eller noen) blir driftet av en ekstern driftsenhet, er denne eksterne driftsenheten en databehandler.



#### Eksempel på databehandler:

- EPJ-leverandør hvor server fysisk er lokalisert hos ekstern leverandør og hvor databehandlingsansvarlig (i virksomheten) har tilgang til EPJ-systemet i en terminalserverløsning.
- En supportleverandør med fjernaksess som drifter hele eller deler av EPJ-systemet eller sikkerhetsløsningen
- Et arbeidsfelleskap hvor arbeidsfelleskapet er et eget rettssubjekt (selskap) som drifter EPJ-systemet. Eller at en av partene i arbeidsfelleskapet drifter EPJ-system på vegne av de andre partene
- Leverandør av lønn- og personalsystem hvor server fysisk er lokalisert hos leverandøren som også drifter løsningen for kunden. Vær oppmerksom på at personopplysningsloven og ikke helseregisterloven da regulerer forholdet, og at databehandleravtalen må endres bl.a. i forhold til dette (se Eksempel på databehandleravtale nedenfor)
- Når et konsern samler driften av EPJ-systemene i et selskap for drift for alle selskapenes EPJ-systemer
- Kommune(r) som benytter vertskommune eller som oppretter interkommunale selskaper for drift av IKT-systemer med helse- og personopplysninger, herunder håndtering av kommunens/kommunenes tilknytning til Norsk Helsenett
- Virksomheten/forskningsprosjektet kan ha behov for at et utenforstående miljø, en underleverandør, bearbeider eller drifter data på vegne av prosjektet

Nr.	Aktivitet/Beskrivelse
1	<b>Beslutning om bruk av ekstern driftsenhet</b> Etter at beslutningen om at IKT-systemer (alle eller noen) skal driftes av en ekstern driftsenhet og før IKT-systemene faktisk settes ut for drifting skal det utformes en databehandleravtale.
2	<b>Identifisering av ekstern driftsenhet(er)</b> Hvis det allerede benyttes en ekstern driftsenhet uten at det i det eksisterende avtaleforholdet er definert krav til behandling av helse- og personopplysninger må dette utføres.  Det skal alltid finnes en oversikt over alle eksterne driftsenheter som behandler helse- og personopplysninger på vegne av virksomheten
3	<b>Utforme databehandleravtale</b> Databehandler har et selvstendig ansvar for informasjonssikkerheten etter Helseregisterloven § 16, Personopplysningsloven § 13, Personopplysningsforskriften § 2-15  <u>Følgende minimumskrav gjelder for en databehandler og må fremgå av avtalen:</u> a) Databehandler må tilfredsstille kravene i Normen. For å sikre seg dette anbefales det som et minimum at sikkerhetsmål og –strategi vedlegges avtalen (se ytterligere detaljer i punkt 4) b) Databehandler skal ikke behandle helse- og personopplysninger på annen måte enn det som er avtalt med databehandlingsansvarlig c) Hvis databehandler behandler helse- og personopplysninger for flere virksomheter skal databehandler ved hjelp av tekniske tiltak som ikke kan overstyres av brukerne ivareta at: <ul style="list-style-type: none"><li>- det er etablert skiller mellom virksomhetene i henhold til gjennomført risikovurdering, dette både i database hvor data er lagret og i kommunikasjon</li><li>- ingen andre enn databehandleren, de som arbeider under databehandlerens instruksjonsmyndighet og virksomheten selv har tilgang til opplysningene</li></ul> Databehandler skal i denne sammenheng også påse at det er iverksatt tiltak slik at Normens nivå for akseptable risiko følges. d) Det anbefales at databehandleravtalen etableres som et kapittel i den generelle avtalen mellom virksomheten og databehandleren. F.eks som en del av: <ul style="list-style-type: none"><li>- Service Nivå Avtale (SNA) (også kalt Service Level Agreement (SLA)) og/eller Kjøpsavtale om driftstjenester</li><li>- Eller vedlegg til SNA eller Kjøpsavtale</li></ul> e) 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 f) 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  (se eksempel på avtale og sjekkliste nedenfor)

Nr.	Aktivitet/Beskrivelse
4	<p><b>Følge opp en databehandleravtale</b></p> <p>Databehandlingsansvarlig skal ha innsyn i databehandlers prosedyrer og praksis for informasjonssikkerhet for å sikre at denne er tilfredsstillende iht. kravene. I praksis kan det være en utfordring for en liten helsevirksomhet å få et slikt innsyn. Dette gjerne pga. evt. forskjeller i virksomhetsstørrelse (ulikt maktforhold) og/eller kompetanse mellom helsevirksomheten og den eksterne driftsenheten.</p> <p>Det anbefales at det utformes en praktisk måte å håndtere dette på ifm avtalens utforming. F.eks. kan flere små virksomheter gå sammen om å få innsyn i relevant dokumentasjon hos databehandler. Eller en kan avtale at resultat av ledelsesgjennomganger, sikkerhetsrevisjoner og/eller avviksbehandling som er relevante, blir sendt uoppfordret.</p> <p>Det er derfor av betydning at databehandlingsansvarlig ifm forespørselen og ved utformingen av avtalen stiller krav til den eksterne driftsenheten. Følgende momenter bør vurderes og beskrives nærmere, avhengig av virksomhetens behov:</p> <ul style="list-style-type: none"> <li>- Databehandler plikter å følge Normen</li> <li>- Databehandler plikter å følge standarder som f.eks. EPJ-standard, meldingsstandarder, etc.</li> <li>- Databehandler plikter å følge virksomhetens akseptkriterier (iht risikovurdering)</li> <li>- Databehandler plikter å gjennomføre hendelsesregistrering</li> <li>- Databehandler plikter å inneha/følge visse sikkerhetssertifiseringer</li> <li>- Klart uttrykk for ansvar bl.a. i forhold til opplysningene som behandles og sikringen av disse</li> <li>- Mulighet for å gjøre endringer i databehandleravtalen (hvis den databehandlingsansvarliges sikkerhetsrevisjoner av databehandleren viser at dette er nødvendig)</li> </ul>
5	<p><b>Krav til tilbakerapportering</b></p> <p>Databehandler skal jevnlig gi statusrapporter om resultater fra sine ansvarsområder. Dette er særlig viktig dersom det benyttes en databehandler. Eksempel på parametere som <i>kan</i> inngå i rapportering fra databehandler (ikke uttømmende):</p> <ul style="list-style-type: none"> <li>- Antall pålogginger til aktuelle system (med hensikt å identifisere avvik)</li> <li>- Feilsituasjoner</li> <li>- Oppetidsstatistikk</li> <li>- Avvik som kan leses av hendelsesregistre</li> </ul>
6	<p><b>Avslutning av databehandleravtale</b></p> <p>Når avtaleforholdet opphører med databehandler er det viktig at databehandler straks tilbakeleverer dokumenter og alle elektroniske data på det medium (f.eks.: tape, CD, papir mv) som databehandler måtte besitte i egenskap av å være databehandler.</p> <p>Ved tjenesteutsetting skal det i avtalen for tjenesteutsetting avtales tilbakeføring av helse- og personopplysninger til databehandlingsansvarlig ved opphør av avtalen.</p> <p>Det er viktig å sikre at databehandler ikke har noen rett til å beholde en kopi av materialet. Det anbefales at databehandlingsansvarlig mottar 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.</p> <p>Avslutningsvis skal databehandlingsansvarlig sikre at databehandler, også etter at avtaleforholdet er avsluttet, fortsatt er bundet av taushetsplikten for de helse- og personopplysningene som er behandlet.</p> <p>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.</p>

## Eksempel på databehandleravtale

Følgende tekst er et eksempel på tekst som bør være med i en avtale mellom tilbyder og oppdragsgiver. Som beskrevet tidligere kan teksten inngå som en del av en kontrakt eller som et vedlegg til en kontrakt. Det anbefales at eksempelet på avtale bearbejdes i det aktuelle avtaleforholdet.

### Databehandleravtale mellom <Helsevirksomhet> og <Ekstern driftsenhet>

<b>Formål</b>	Avtale for å sikre at krav til konfidensialitet, integritet, tilgjengelighet og kvalitet ivaretas i henhold til helseregisterloven og personopplysningsloven m/forskrift.
<b>Forutsetninger</b>	At det foreligger en gjennomarbeidet avtale og øvrige prosedyrer er på plass.
<b>Dato</b>	<MM.DD.ÅÅÅÅ>
<b>Versjon</b>	<1.0>
<b>Gyldig</b>	<MM.DD.ÅÅÅÅ> til <MM.DD.ÅÅÅÅ>

<DATABASEHANDLER> plikter å behandle personopplysninger fra <DATABASEHANDLINGSANSVARLIG> slik at krav til konfidensialitet, integritet, tilgjengelighet og kvalitet er ivaretatt etter Helseregisterloven §§ 16 og 18, Personopplysningsloven § 13, personopplysningsforskriften § 2-15 og Norm for informasjonssikkerhet.

Det er <DATABASEHANDLINGSANSVARLIG>'s ansvar å påse at <DATABASEHANDLER>'s informasjonssikkerhet er tilfredsstillende. Om sikkerhetsnivået ikke er tilfredsstillende plikter <DATABASEHANDLER> å justere sikkerhetsnivået etter instruks fra <DATABASEHANDLINGSANSVARLIG>.

<DATABASEHANDLER> har det praktiske ansvaret for at tilfredsstillende informasjonssikkerhet er etablert gjennom planlagte og systematiske tiltak. I den forbindelse skal <DATABASEHANDLER> oversende dokumentasjon til <DATABASEHANDLINGSANSVARLIG> om mål og strategi for informasjonssikkerheten. Dette skal skje første gang ved avtaleinngåelse og når denne avtalen blir revidert.

Ved bruk av leverandører til vedlikehold og oppdatering av registre, databaser med mer, så plikter <DATABASEHANDLER> å sørge for at disse leverandørene etterlever de samme krav til informasjonssikkerhet. Dette på en slik måte at sikkerhetsnivået, som er beskrevet ovenfor, ikke blir svekket. Om helse- og personopplysningene skal overføres i eksterne nettverk skal disse krypteres etter gjeldene bestemmelser.

<DATABASEHANDLER> plikter å ha dokumentert systemet og prosedyrer som er relevant i forbindelse med denne avtalen. Med dokumentasjon menes prosedyrer for autorisasjon og bruk, ulike tekniske og organisatoriske sikkerhetstiltak. Dokumentasjonen skal være tilgjengelig for <DATABASEHANDLINGSANSVARLIG>, Datatilsynet og Helsetilsynet. Innsyn i dokumentasjonen skal reguleres strengt (gis til et begrenset antall autoriserte personer) slik at dette ikke svekker sikkerhetsnivået.<sup>1</sup>

Når det forekommer avvik iht. vedtatt informasjonssikkerhet skal <DATABASEHANDLER> som en del av avvikprosedyren sende avvikrapporter til <DATABASEHANDLINGSANSVARLIG> for avvik som har betydning i denne sammenhengen. <DATABASEHANDLINGSANSVARLIG> har rett til å la en tredje part revidere <DATABASEHANDLER>'s informasjonssikkerhet. Kostnadene for dette skal dekkes av <DATABASEHANDLINGSANSVARLIG>.

Ved opphør av avtaleforholdet plikter databehandler å tilbakelevere dokumenter og alle elektroniske data på det medium (tape, CD, papir mv) som <DATABASEHANDLER> måtte besitte i egenskap av å være databehandler. <DATABASEHANDLER> har ikke noen rett til å beholde kopi av materialet. <DATABASEHANDLINGSANSVARLIG> skal motta en skriftlig bekreftelse fra <DATABASEHANDLER> på at alt materiale er overlevert til <DATABASEHANDLINGSANSVARLIG>, og at <DATABASEHANDLER> ikke selv har beholdt noen kopi, avskrift eller annen gjengivelse av noen del av materialet på noe medium.

Taushetsplikten for de helse- og personopplysningene og annen relevant informasjon i tilknytning til dette skal overholdes underveis i avtaleforholdet. Taushetsplikten gjelder også for opplysninger om hvordan sikkerheten er ivaretatt (teknisk, fysisk, administrativt og organisatorisk). <DATABASEHANDLER> er bundet av den samme taushetsplikten også etter at avtaleforholdet er avsluttet for de helse- og personopplysningene som er behandlet.

\_\_\_\_\_  
<Databehandlingsansvarlig>  
<Helseforetak>

\_\_\_\_\_  
<Databehandler>  
<Ekstern driftsenhet>

<sup>1</sup> Det oppfordres å henvise til faktaark i avtalen vedrørende den aktuelle tjenesten (for eksempel hjemmekontor). Faktaarkene finnes på [www.normen.no](http://www.normen.no).

## Eksempel på sjekkliste med krav til databehandler og etablering av databehandleravtale

Nr	Krav	Krav ivaretatt			Kommentar
		Ja	Nei	Ikke aktuell	
1.	Databehandler plikter å følge Normen og oppfylle kravene i denne.				
2.	Databehandler plikter å følge meldingsstandarder der det er relevant.				
3.	Databehandler skal oversende til databehandlingsansvarlig beskrivelse av sikkerhetsmål, sikkerhetsstrategi og ansvar for informasjonssikkerheten.				
4.	Databehandler plikter å behandle all informasjon i henhold til databehandleravtale med databehandlingsansvarlig.				
5.	Krav til hendelsesregistrering:				
	- Databehandler skal sikre at all tilgang og bruk av IKT-systemet hendelsesregistreres				
	- Hendelsesregistre skal samles inn og tilgjengeliggjøres for databehandlingsansvarlig for spørringer og rapporter. Databehandlingsansvarlig skal fastsette hvilke rapporter som skal kunne tas ut				
	- Hendelsesregistre skal oppbevares i minimum 2 år				
	- Følgende skal som minimum registreres i hendelsesregistre: <ul style="list-style-type: none"> <li>o entydig identifikator for den autoriserte brukeren</li> <li>o rollen den autoriserte brukeren har ved tilgangen</li> <li>o virksomhetstilhørighet</li> <li>o organisatorisk tilhørighet til den som er autorisert</li> <li>o hvilke type opplysninger det er gitt tilgang til</li> <li>o grunnlaget for tilgangen</li> <li>o tidspunkt og varighet for tilgangen</li> </ul>				
6.	Databehandler kan ikke benytte underleverandører i forbindelse med behandling av helse- og personopplysninger uten at det er skriftlig avtalt med databehandlingsansvarlig.				
7.	Databehandler skal sikre at informasjon som behandles for databehandlingsansvarlig holdes adskilt fra egne og andre virksomheters informasjon og tjenester.				
8.	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, Datatilsynet og Helsetilsynet.				
9.	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.				
10.	Databehandler skal sikre at følgende minimumskrav til teknisk sikkerhet er oppfylt (kravene er ikke uttømmende):				
	- Tilgang til tjenester og opplysninger i nettverket og IKT-systemet skal være basert på individuelle brukernavn og passord				
	- Opplysninger overlevert av databehandlingsansvarlig skal sikres, slik at kun autoriserte medarbeidere har tilgang				
	- Tilgang til eksterne nett/Internett/helsenett, inkludert				

Nr	Krav	Krav ivaretatt			Kommentar
		Ja	Nei	Ikke aktuell	
	databehandlerens åpne nettverk, skal sikres med sikkerhetstiltak som ikke kan påvirkes eller omgås av eksterne og egne ansatte, og som forhindrer uforvarende eksponering av sensitive personopplysninger til nettverk med lavere sikkerhet				
	- Ved bruk av fjernaksess skal alle sikkerhetstiltak og avtale innføres iht. til dokumentet ” Veileder for fjernaksess for vedlikehold og oppdateringer mellom leverandør og helsevirksomhet”				
	- Påloggingsløsning som tilfredsstiller kravene til sikkerhetsnivå 4 i Normen skal benyttes til pålogging ved fjerndrift/-aksess				
	- Meldinger som inneholder sensitive personopplysninger skal sendes kryptert				
	- Hvis databehandler behandler helse- og personopplysninger for flere virksomheter skal databehandler ved hjelp av tekniske tiltak som ikke kan overstyres av brukerne ivareta at det er etablert skiller mellom virksomhetene i henhold til gjennomført risikovurdering. Dette gjelder både i database hvor data er lagret og i kommunikasjon				
11.	<b>Krav til tilgangsstyring</b>				
	- Databehandleren skal ha prosedyrer for å autorisere kun de av databehandlerens medarbeidere som har reelt behov for tilgang til IKT-systemer og informasjon for å gjennomføre leveransen/tjenesten				
	- Databehandler skal til enhver tid ha oversikt over eget personell som er autorisert for tilgang til databehandlingsansvarliges IKT-systemer og informasjon. På forespørsel skal slik oversikt forelegges databehandlingsansvarlig				
	- Dersom databehandlingsansvarlig har innvendinger mot at en gitt person har fysisk og/eller elektronisk tilgang til IKT-systemet, skal autorisasjonen inndras				
	- Det skal benyttes personlige brukerkonti for all tilgang knyttet til gjennomføring av leveransen				
	- Dersom databehandleren benytter mobilt utstyr til drift, skal databehandleren ha prosedyrer som sikrer at disse bare benyttes av driftspersonell og til driftsrelaterte oppgaver				
	- Dersom tredjepart eller underleverandør til databehandler, i forbindelse med support eller tilsvarende, skal ha tilgang til IKT-systemet, skal det benyttes sikkerhetsnivå 4 iht kravene i Normen.				
12.	<b>Taushetsplikt</b>				
	- 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				

Nr	Krav	Krav ivaretatt			Kommentar
		Ja	Nei	Ikke aktuell	
	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				
13.	<p>Tilbakerapportering.</p> <p>Databehandler skal jevnlig gi statusrapporter om resultater fra sine ansvarsområder. Eksempler på hva som skal inngå i rapportering fra databehandler:</p> <ul style="list-style-type: none"> <li>- Driftsstatus på kritiske systemer</li> <li>- Oppetid på systemer</li> <li>- Planlagte avbrudd og tidslengde på avbrudd</li> <li>- Planlagte endringer, forventet effekt og tidspunkt de skal utføres</li> <li>- Sikkerhetsoppdateringer</li> <li>- Feilsituasjoner/ -rettinger</li> <li>- Manglende oppfyllelse av tjenesteavtale og mulige årsaker</li> </ul>				