NORMEN

Bruk av databehandler (faktaark 10)

Versjon 6.0

Publisert: 04.02.2021

Utarbeidet med støtte fra direktoratet for e-helse

Vedtatt av styringsgruppen for Normen

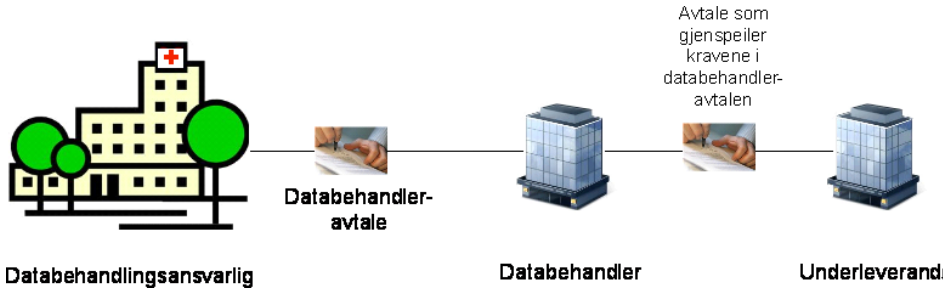
Dette faktaarket er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) som forvaltes av Styringsgruppen for Normen etter Normens forvaltningsmodell. Se mer på www.normen.no

Tema for faktaarket	Dette faktaarket omhandler bruk av databehandlere. Formålet med faktaarket er å sikre at databehandler behandler helse- og personopplysninger slik dataansvarlig har bestemt. Faktaarket har en praktisk tilnærming og inneholder forslag til fremgangsmåte ved valg av databehandler, eksempler på hvem som er/ikke regnes som databehandler,
Dette faktaarket er spesielt relevant for	Målgruppen for faktaarket er: • Virksomhetens leder/ledelse • Forskningsansvarlig • Prosjektleder forskning • Sikkerhetsleder • Personvernombud • IKT-ansvarlig • Databehandler • Leverandør
Krav i Normen	Faktaarket gjelder følgende kapitler i Normen • Kapittel 5.7.4 Databehandler
Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Følgende lov- og forskriftsbestemmelser, standarder og andre rammeverk er spesielt relevante for faktaarket: • Personvernforordningen artikkel 28 Databehandler • Personvernforordningen artikkel 29 Behandling som utføres for den behandlingsansvarlige eller databehandleren • Pasientjournalloven § 22 Informasjonssikkerhet • Helseregisterloven § 21 Informasjonssikkerhet • Protokoll over behandlinger av helse- og personopplysninger i virksomheten (faktaark 13) • Logging og innsyn i logg (faktaark 15) • Formål og behandlingsgrunnlag (faktaark 56) • Veileder for fjernaksess mellom virksomhet og leverandør • Veileder for personvern og informasjonssikkerhet i forskningsprosjekter innenfor helse- og omsorgssektoren • Direktoratet for e-helse sin mal for databehandleravtale (eksempel på databehandleravtale) -

NORMEN

Bruk av databehandler

Det skal etableres databehandleravtale mellom dataansvarlig og databehandler (ekstern driftsenhet). I tillegg må databehandler påse at kravene i databehandleravtalen gjenspeiles i avtale med sine underleverandører. En databehandler er en ekstern person eller virksomhet utenfor den dataansvarliges virksomhet. Databehandleren behandler helse- og personopplysninger på vegne av den dataansvarlige. Dette betyr at hvis virksomhetens IKT- systemer (alle eller noen) blir driftet av en ekstern driftsenhet, er denne eksterne driftsenheten en databehandler.



Databehandleravtale

Med behandling av helse- og personopplysninger menes enhver formålsbestemt bruk av helse- og personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter. Annen bruk som krever databehandleravtale er konvertering, bearbeiding, kobling mot andre registre, analyse, rapportering, test, avhending og sletting.
Det er altså tilstrekkelig at databehandler lagrer opplysningene for at det må inngås en databehandleravtale. Et annet eksempel er når databehandler kun registrerer opplysningene på vegne av virksomheten, så skal det inngås en databehandleavtale. Videre for eksempel ved å oppbevare opplysningene når det er nødvendig for å utføre service på datasystemer.

Et spørsmål som ofte reises er om det er nødvendig å opprette databehandleravtale når den eksterne virksomheten lagrer helse- og personopplysninger kryptert. Svaret er ja, og begrunnelsen er at kryptering kun er en sikkerhetsmekanisme og at den eksterne virksomheten fortsatt lagrer opplysningene.

<u>Eksempel på databehandler:</u>

- EPJ-leverandør hvor server fysisk er lokalisert hos leverandøren og hvor dataansvarlig (i virksomheten) har tilgang til EPJ-systemet i en terminalserverløsning.
- Leverandør med fjernaksess som drifter hele eller deler av EPJ-systemet eller sikkerhetsløsningen
- En av partene i et formalisert arbeidsfellesskap drifter EPJ-systemet på vegne av de andre partene. Hjemmel for samarbeid mellom virksomheter om behandlingsrettede helseregistre er pasientjournalloven § 9.
- Leverandør av lønn- og personalsystem hvor server fysisk er plassert hos leverandøren som også drifter løsningen for kunden. Vær oppmerksom på at

personopplysningsloven og ikke pasientjournalloven da regulerer forholdet, og at databehandleravtalen må endres bl.a. i forhold til dette (se eksempel på databehandleravtale nedenfor)
- Et konsern samler driften av EPJ-systemene i en egen virksomhet for drift av virksomhetenes 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
- Helseforetak setter ut drift av IKT-løsning for behandling av helse- og personopplysninger til driftsenhet utenfor HF
- Utrangering av lagringsenheter (multifunksjonsskriver, disker, osv) hvor leverandør utfører sletting av lagringsenheten
- Bruk av skytjeneste for behandling av helseopplysninger. Her må virksomheten kartlegge bruk av underleverandører til skytjeneste-leverandøren slik at det sikres at Normens krav gjelder for all behandling av helse- og personopplysninger

Det er kun leverandører/tjenesteytere som behandler helse- og opplysninger *på vegne av* virksomheten som regnes som databehandler. Det betyr at man kun er databehandler dersom man har fått en delegert oppgave om å behandle helse- og personopplysninger fra dataansvarlig. Å behandle helse- og personopplysninger må være en den av formålet med avtalen mellom virksomhetene. Der leverandøren får tilgang til opplysninger ved utførelse av service eller support, men det ikke er en del av oppdraget å behandle opplysningene, vil det være tilstrekkelig med taushetserklæring.

Eksempler på tjenester/leverandører som ikke er en databehandler:[1]

- En leverandør av teknisk utstyr. Formålet med oppdraget er ikke å behandle helse- og personopplysninger. Det foreligger derfor ikke et databehandleroppdrag selv om leverandøren potensielt *kan* få tilgang til slik informasjon, og det vil være tilstrekkelig med en taushetserklæring.
- En leverandør som skal utføre support på en fysisk server, programvare, el. Selv om leverandøren kan få tilgang til personopplysninger når support utføres, er ikke hovedoppdraget å behandle helse- og personopplysninger. Det kan oppstå en gråsone der leverandøren har kontinuerlig fjerntilgang til systemer hvor personopplysninger behandles, og det må gjøres en konkret vurdering av hvorvidt det foreligger et databehandlerforhold.
- Leverandør av bedriftshelsetjeneste som mottar liste over ansatte i din virksomhet som ønsker å bli kontaktet (Denne leverandøren vil ha selvstendig dataansvar for opplysningene).

[1] For mer informasjon og flere eksempler, se veiledning fra Datatilsynet: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/behandlingsansvarlig-og-databehandler/nar-foreligger-det-et-databehandleroppdrag/

Prosess for valg/bruk av databehandler

1. **Valg av databehandler**
   Virksomheten kan bare bruke databehandlere som oppfyller kravene i lov og forskrift samt Normens kapittel 3 og 4, og de kravene fra Normen som er relevante for det aktuelle avtaleforhold.

   Databehandleren skal ikke engasjere underleverandører uten at det på forhånd er innhentet skriftlig tillatelse til dette fra virksomheten, med mindre det er innhentet en generell, skriftlig tillatelse eller en slik tillatelse fremgår av databehandleravtalen. I sistnevnte tilfelle skal dataansvarlig varsles i forkant av endring og gis mulighet til å motsette seg endringen av underleverandør. Databehandleren er fullt ut ansvarlig for at dens underleverandører oppfyller sine forpliktelser.

2. **Beslutning om bruk av ekstern driftsenhet**
   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 inngås en databehandleravtale.

3. **Identifisering av ekstern driftsenhet**
   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. En slik oversikt kan for eksempel inngå i virksomhetens behandlingsprotokoll.

4. **Utforme databehandleravtale**
   Databehandler har et selvstendig ansvar for informasjonssikkerheten etter pasientjournalloven § 22, helseregisterloven § 21 og personvernforordningen artikkel 28 og 29, herunder underleverandører.

   <u>Følgende minimumskrav gjelder for en databehandler og må fremgå av avtalen:</u>

   a) Det anbefales at databehandleravtalen etableres som et kapittel i den generelle avtalen mellom virksomheten og databehandleren. For eksempel som en del av:
      - Tjenestenivåavtale og/eller kjøpsavtale om driftstjenester eller
      - Vedlegg til tjenestenivåavtale eller kjøpsavtale

   b) Databehandleravtalen skal beskrive:
      - Databehandlers oppgaver og plikter
      - Hva slags teneste/behandling databehandler skal utføre på vegne av dataansvarlig.
      - Varigheten av behandlingen
      - Behandlingens formål og art
      - Typen personopplysninger
      - Kategorier av registrerte
      - Dataansvarliges rettigheter og plikter

   c) Databehandleravtalen skal regulere:
      - Konkrete sikkerhetstiltak
      - Databehandler skal på eget initiativ treffe alle tiltak som er nødvendig for å sikre god informasjonssikkerhet, herunder å følge kravene i Normen
      - Databehandler skal bare kunne overføre personopplysningene til utlandet etter instruks fra den dataansvarlige
      - Databehandler skal bare autorisere personer som er underlagt taushetsplikt for behandling av helse- og personopplysninger

- Krav til bruk av underleverandører (annen databehandler)
- Dataansvarlig skal sikres innsynsrett for å forsikre seg om at kravene etterleves.

d) Databehandleravtalen skal regulere at databehandler har plikt til å bistå med/i:
- tekniske og organisatoriske tiltak for å utøve den registrertes rettigheter
- relevante tekniske og organisatoriske tiltak for å sikre god informasjonssikkerhet
- å melde brudd på personvernet til Datatilsynet
- å varsle den registrerte om brudd på personvernet
- dokumentasjon av allerede gjennomført relevant personvernkonsekvensvurdering eller gjennomføring av personvernkonsekvensvurdering
- forhåndsdrøftinger med Datatilsynet
- slette eller tilbakelevere personopplysningene etter instruks
- gjøre tilgjengelig all informasjon som viser at pliktene etter databehandleravtalen er ivaretatt
- å bidra i sikkerhetsrevisjoner
- å bidra i inspeksjoner
- å få endret instrukser fra den dataansvarlige er i strid med lovverket

5. Valg av databehandler Følge opp en databehandleravtale

Dataansvarlig 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.

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 ledelsens gjennomgang, sikkerhetsrevisjoner og/eller avviksbehandling som er relevante, blir sendt uoppfordret til dataansvarlig. Revisjon kan også gjennomføres av en avtalt tredjepart. Dersom revisjon skal gjøres av tredjepart bør partene på forhånd avklare hvordan dette skal gjøres og/eller hvem som skal bære kostnadene ved revisjonen.

Det er viktig at dataansvarlig ved utformingen av avtalen stiller krav til den eksterne driftsenheten. Følgende momenter bør vurderes og beskrives nærmere, avhengig av virksomhetens behov:

- Databehandler plikter å følge Normen
- Databehandler plikter å følge virksomhetens akseptkriterier (iht risikovurdering)
- Databehandler plikter å gjennomføre logging
- Mulighet for å gjøre endringer i databehandleravtalen (hvis den dataansvarliges sikkerhetsrevisjoner av databehandleren viser at dette er nødvendig)

6. Krav til tilbakerapportering

Databehandler skal jevnlig rapportere status om resultater fra sine ansvarsområder. Eksempel på forhold som kan inngå i rapportering fra databehandler (ikke uttømmende):

- Antall pålogginger til aktuelle system (autorisert bruk)
- Antall forsøk på uautorisert bruk
- Feilsituasjoner
- Oppetidsstatistikk
- Avvik som kan leses av hendelsesregistre
- Gjennomførte konfigurasjonsendringer

7. Avslutning av databehandleravtale

Når avtaleforholdet opphører med databehandler er det viktig at databehandler straks tilbakeleverer dokumenter og alle elektroniske data i lesbart format på det medium som er avtalt.
Ved tjenesteutsetting skal det i avtalen for tjenesteutsetting avtales tilbakeføring av helse- og personopplysninger til dataansvarlig ved opphør av avtalen.
Det er viktig å sikre at databehandler ikke har noen rett til å beholde en kopi av opplysningene. Dataansvarlig skal motta en skriftlig erklæring fra databehandler på at alle helse- og personopplysninger er overlevert til virksomheten og at databehandler ikke har beholdt kopi, avskrift eller annen gjengivelse av noen del av opplysningene på noe medium.
Avslutningsvis skal dataansvarlig sikre at databehandler, også etter at avtaleforholdet er avsluttet, fortsatt er bundet av taushetsplikten for de helse- og personopplysningene som er behandlet.
Etter at helse- og personopplysningene er overført til dataansvarlig, og bekreftet mottatt av denne, skal databehandler slette opplysningene i sitt system. Kravet til sletting omfatter også sikkerhetskopier av helse- og personopplysningene.

Databehandler skal slette eller forsvarlig destruere alle dokumenter, data, harddisker, cd-er og andre lagringsmedier som inneholder opplysninger som omfattes av avtalen. Sletting skal gjennomføres slik at opplysningene ikke kan gjenfinnes. Dette gjelder også for eventuelle sikkerhetskopier og utskrifter.
Virksomheten kan på bakgrunn av en risikovurdering vurdere om opplysninger slettes ved rotasjon innen rimelig tid, slik at det ikke er nødvendig med systematisk sletting av sikkerhetskopier.