Direktoratet for e-helse

Versjon: Desember 2020

# VEILEDER
# - Standard databehandleravtale

Standard databehandleravtale med veileder er utarbeidet av Direktoratet for e-helse på oppdrag fra Helse- og omsorgsdepartementet.

Formålet ved denne veilederen er å gi nærmere informasjon om avtalens materielle innhold, samt gi en praktisk veiledning til hvordan avtalens vedlegg skal brukes og fylles ut.

Veilederen gir i kapittel 1 informasjon om bakgrunn, formål og virkeområdet for standardavtalen og hvordan denne er bygget opp.

I kapittel 2 gis det kommentarer til de enkelte punktene i standardavtalen. Kapittelet er bygget opp slik at hvert punkt er knyttet til tilsvarende punkt i avtalen..

I kapittel 3 gis det kommentarer til standardavtalens vedlegg og eksempler til bruk for utfylling av disse.

For nærmere beskrivelse av mer overordnede spørsmål, for eksempel om når det foreligger et databehandleroppdrag som krever avtale, ansvarsplassering og rolleavklaring i et slikt oppdrag, vises til veiledning fra Datatilsynet.

# Innhold

# 1 Om standardavtalen

## 1.1 Bakgrunn

Helse- og omsorgsdepartementet har i tildelingsbrevet for 2020 gitt Direktoratet for e-helse oppdrag om å:

- *Utarbeide en standard databehandleravtale med veileder som sektoren kan benytte ved inngåelse av slik avtaler*

Denne standardavtalen er basert på Mal for databehandleravtale, publisert på ehelse.no 05.11.2018. Det er ikke gjort vesentlige materielle endringer fra den tidligere avtalemalen. Det er foretatt noen strukturelle endringer ved at selve avtaleteksten skal ligge fast, se punkt 1.3 nedenfor. Videre er avtalen nå mer rettet mot behandling av helseopplysninger, se punkt 1.2.2. Det er også gjort enkelte språklige justeringer i avtaleteksten.

Det er en målsetting at en standard databehandleravtale for sektoren både vil bidra til å sikre etterlevelse av personvernregelverket og forenkle avtaleforvaltningen for den enkelte virksomheten.

## 1.2 Bruk av standardavtalen

### 1.2.1 Formålet med avtalen

Standardavtalen skal bidra til å sikre at helse- og personopplysninger blir behandlet i samsvar med regelverket ved bruk av databehandlere i helse- og omsorgssektoren.

Regelverket fastsetter ikke noe krav til utforming eller format ved etablering av en databehandleravtale. Man står dermed fritt til å utforme en slik avtale som man ønsker, forutsatt at kravene i regelverket oppfylles. I denne standardavtalen er de relevante kravene i personvernregelverket knyttet til innhold i en databehandleravtale tatt inn i teksten. Ved å benytte standardavtalen vil man dermed ha større sikkerhet for at avtalen som inngås dekker de nødvendige kravene.

Direktoratet for e-helse ønsker at virksomheter i helse- og omsorgssektoren benytter denne standardavtalen når de skal inngå databehandleravtale som omfatter helseopplysninger (se punkt 1.2.2 Virkeområde). Utbredt bruk av en standardisert avtale i sektoren vil forenkle både avtaleinngåelse og senere avtaleforvaltning for både dataansvarlige og databehandlere ettersom avtalestruktur og innhold blir ensartet og kjent.

### 1.2.2 Virkeområde – når bør standardavtalen benyttes?

- Helseopplysninger

  Standardavtalen er utarbeidet med sikte på behandling av helseopplysninger. Dette gjenspeiles både i avtalens begrepsbruk, omfang og regelverkshenvisninger. Det anbefales derfor at standardavtalen først og fremst benyttes der databehandler skal behandle helseopplysninger på vegne av dataansvarlig.

Det er i all hovedsak de samme krav som gjelder ved behandling av helseopplysninger som ved andre personopplysninger. Helseopplysninger er imidlertid "særlige kategorier av personopplysninger" slik at kravene skjerpes både når det gjelder krav til tydelighet og detaljeringsgrad og krav til informasjonssikkerhetstiltak.

Der hvor databehandleroppdraget ikke omfatter helseopplysninger, men utelukkende gjelder behandling av "vanlige" personopplysninger, kan det være mer hensiktsmessig å benytte et annet utgangspunkt for avtalen, for eksempel fra Datatilsynet eller Digitaliseringsdirektoratet.

**Datatilsynet** har utarbeidet veiledningsmateriell med praktisk innføring i når man må inngå en databehandleravtale og kravene til innhold i en slik avtale. Datatilsynet viser også til standard databehandleravtale som er vedtatt av Datatilsynet i Danmark. Den avtalen har vært fremlagt for Det europeiske personvernrådet (EDPB) og kan også brukes i Norge.

- Datatilsynets veileder – "Hvordan lage en databehandleravtale"
- Standard databehandleravtale (dansk/engelsk)

**Digitaliseringsdirektoratet** har utarbeidet en databehandleravtale som primært er beregnet på forholdsvis enkle databehandleroppdrag og som passer godt sammen med bruk av Statens standardavtaler (SSA). De har også laget en sjekkliste som kan brukes for å sjekke at en leverandørs standard databehandleravtale tilfredsstiller norske krav.

- Databehandleravtale og sjekkliste

## Databehandleroppdragets omfang

Standardavtalen kan benyttes både i omfattende databehandleroppdrag (flere behandlinger/stor mengde opplysninger) og i oppdrag av enklere karakter. De grunnleggende kravene til behandlingen vil være de samme, men oppdragets kompleksitet vil gjenspeiles i vedleggene til avtalen. Det må gjøres en forholdsmessighetsvurdering slik at avtaleomfanget tilpasses oppdraget. Jo mer omfattende databehandleroppdraget er, desto større krav stilles til beskrivelsen av dette i avtalens vedlegg.

## Forholdet til Tjeneste/oppdragsavtalen

Standardavtalen kan benyttes uavhengig av hvilken avtaletype som ligger til grunn for de tjenester/oppdrag som innebærer en behandling av personopplysninger på vegne av dataansvarlig. Dette kan f.eks. være statens standardavtaler (SSA), Dataforeningens kontraktstandarder (PS2000), bruksvilkår etc. Det vil variere i hvilken grad behandlingen av opplysninger er omtalt i Tjeneste/oppdragsavtalen. De relevante forholdene knyttet til selve databehandleroppdraget skal uansett presiseres i databehandleravtalen. Krav til slik avtaleregulering følger av personvernforordningen Art. 28 nr. 3. Dersom behandlingen av opplysninger er beskrevet på ulik måte (motstrid) i Tjeneste/oppdragsavtalen og i databehandleravtalen, er det omtalen i databehandleravtalen som skal gjelde.

"Battle of Forms" - Hvem bestemmer hvilket avtaleformat som skal benyttes?

Det er ikke fastsatt noe krav om å bruke et bestemt format eller krav til særlig utforming av en databehandleravtale. Flere virksomheter har utarbeidet sin egen avtalemal som de ønsker å benytte ved databehandleroppdrag, enten de er dataansvarlig eller databehandler. Avtalens utforming er av liten betydning, det avgjørende er at det materielle innholdet dekker kravene i regelverket. For den enkelte virksomhet vil det oppleves både enklere og gi økt trygghet for at kravene dekkes, dersom man benytter en avtaleform man er godt kjent med. Spørsmål om hvilken avtalemal som skal benyttes omtales gjerne som "Battle of Forms".

Som utgangspunkt er det den dataansvarlige som bestemmer hvilken avtaleform som skal benyttes. Det er den dataansvarlige som setter ut databehandleroppdraget og som bestemmer rammene for dette.

I en del tilfeller er dette utgangspunktet likevel ikke praktisk gjennomførbart. Eksempelvis vil det for leverandører som tilbyr kommersielle, standardiserte tjenester der behandling av personopplysninger inngår, være lite hensiktsmessig å måtte forholde seg til et stort antall ulike avtaleformater fra ulike kunder (dataansvarlige). I slike tilfeller vil leverandørens (databehandlers) avtalemal eller standardvilkår normalt måtte legges til grunn.

Selv om en slik standardisert databehandleravtale er utarbeidet av leverandøren, er det kunden, som dataansvarlig, som er ansvarlig for at regelverkets krav er oppfylt. Kunden må dermed forsikre seg om at avtalen dekker de forholdene den skal gjøre, eventuelt forsøke å få inn nødvendige endringer og vurdere om databehandleravtalen er akseptabel før den inngås. Her kan Digitaliseringsdirektoratets sjekkliste[1] for databehandleravtale være et utgangspunkt for vurderingen. Overfor store leverandører og internasjonale aktører vil det i mange tilfeller være begrenset eller ingen påvirkningsmulighet av innholdet i deres standard databehandleravtale/vilkår for behandling av personopplysninger. I så fall må kunden vurdere hvorvidt avtalen innebærer et akseptabelt risikonivå slik at den kan inngås, eller om man bør avstå fra dette.

## 1.3 Standardavtalens oppbygging

Avtaleteksten

Standardavtalen er bygget opp med en generell avtaletekst som alltid skal benyttes. Det skal ikke skrives inn endringer i selve avtaleteksten. Dersom det er behov for å gjøre endringer eller tilpasninger i selve avtaleteksten, skal dette beskrives i Vedlegg 5 - Endringer i den generelle avtaleteksten ved avtaleinngåelsen. Dette sikrer en enhetlig og oversiktlig avtaleutforming og samsvarer også med hvordan Statens standardavtaler (SSA) er bygget opp.

Vedleggene

- Vedlegg 1: Det konkrete oppdraget med tilhørende behandling av opplysninger skal spesifiseres i vedlegg 1.

[1] https://www.anskaffelser.no/sites/anskaffelser2/files/sjekkliste_databehandleravtale_2020.docx
Merk at denne ikke er oppdatert for så vidt gjelder Schrems II, se punkt 3.10.2 under.

- Vedlegg 2: I standardavtalen er de grunnleggende kravene til databehandlers informasjonssikkerhet beskrevet. Dette skal utdypes og konkretiseres etter behov i vedlegg 2.
- Vedlegg 3: Administrative bestemmelser, slik som kontaktopplysninger, nærmere revisjonsrutiner, regelmessige møter og rapportering mv, fylles ut i vedlegg 3.
- Vedlegg 4: Dersom databehandler benytter underleverandør til å behandle de aktuelle opplysningene, skal dette fremgå av vedlegg 4.
- Vedlegg 5: Det skal ikke gjøres endringer i selve avtaleteksten. Dersom det er behov for endringer eller tillegg i de generelle avtalebestemmelsene ved avtaleinngåelsen, skal dette gjøres i vedlegg 5.
- Vedlegg 6: Endringer etter avtaleinngåelsen samles i vedlegg 6.

# 2 Kommentarer til de enkelte punktene i standardavtalen

## Forsiden

På avtalens forside skal avtalepartene identifiseres ved virksomhetenes navn og organisasjonsnummer.

Databehandleravtalen vil være knyttet til en annen avtalerelasjon mellom partene som innebærer behandling av helse- og personopplysninger. En slik avtale kan være av ulik art, det kan være en oppdragsavtale, en tjenesteavtale, bruksvilkår osv. Det er viktig at tilknytningen til den overordnede avtalen fremkommer tydelig, med tittel, dato og eventuell saksreferanse. Dette særlig for å sikre at avtaleforholdene sees i helhetlig sammenheng på avtaletidspunktet, men også for å forenkle avtaleoppfølgingen over tid.

Avtalen skal signeres av en bemyndiget representant for virksomheten. Dette vil være virksomhetens øverste leder eller en i virksomheten som har fått delegert slik myndighet.

## 2.1 Om avtalen

Punktet angir det rettslige rammeverket for databehandleravtalen. Det skal ikke avtales forhold som er i strid med dette rammeverket, i så fall viker slike avtalebestemmelser.

Vedleggene til avtalen inngår i avtalen som helhet. Avtalte endringer som tas inn i endringsvedleggene (Vedlegg 5 og Vedlegg 6) går foran avtaleteksten. De øvrige vedleggene gir supplerende beskrivelser/tillegg til avtalen.

## 2.2 Definisjoner

Begrepene som benyttes i avtalen skal forstås slik de er definert i relevant lovgivning.

Ettersom avtalen er utformet særlig med sikte på behandling av helseopplysninger, benyttes begrepet "dataansvarlig" gjennomgående i avtalen i stedet for "behandlingsansvarlig". Uttrykkene er synonyme og skal forstås slik "behandlingsansvarlig" er definert i personvernforordningen artikkel 4 nr. 7. Dette følger av pasientjournalloven § 2.

## 2.3 Avtalens formål

Etter personvernforordningen artikkel 28 nr. 3 skal databehandlers behandling av opplysninger på vegne av den dataansvarlige avtalereguleres. Avtalen skal sikre at regelverket oppfylles og at den registrertes rettigheter ivaretas.

## 2.4 Omfang

Første avsnitt fastslår at databehandleravtalen regulerer behandlingen av opplysninger databehandler gjør på vegne av dataansvarlig som følge av tjeneste/oppdragsavtalen. Databehandleravtalen har forrang når det gjelder forhold spesifikt knyttet til behandling av personopplysninger dersom det skulle være konflikt mellom avtalene.

Annet avsnitt skal synliggjøre at databehandleravtalen kan utvides til å omfatte flere/nye databehandlerforhold mellom de samme partene. Det kan f.eks. være tilfelle der en driftsleverandør skal drifte nye løsninger for den samme kunden. Da vil det bli inngått en ny avtale mellom partene, ev. en endringsavtale til den opprinnelige driftsavtalen, om driften av den nye løsningen og dette vil være en "senere skriftlig avtale mellom partene".

I slike tilfeller er det ikke nødvendig å inngå en helt ny databehandleravtale. Partene kan i stedet bli enige om å endre den databehandleravtalen de allerede har inngått (se pkt. 14), ved å innarbeide driften av den nye løsningen i vedleggene til databehandleravtalen. Det kan være annet formål, andre behandlinger og andre typer opplysninger etc. knyttet til det nye databehandlerforholdet mellom partene og vedleggene må endres i tråd med de nye behandlingene.

## 2.5 Behandlingens formål, opplysninger og behandlinger

Punktet henviser til avtalens vedlegg 1 der det skal spesifiseres nærmere hva som er formålet med og varigheten av behandlingen(e), hvilke behandlinger og opplysningstyper som omfattes og hvilke kategorier av personer som registreres.

Nærmere omtale og eksempler gis nedenfor i pkt. 3.1 om Vedlegg 1.

## 2.6 Rammene for behandling av helse- og personopplysninger

Punktet gjenspeiler det overordnede prinsippet i et databehandlerforhold: Databehandler behandler opplysningene kun på vegne av den dataansvarlige og kun slik denne har bestemt.

## 2.7 Dataansvarliges plikter

Den dataansvarlige er ansvarlig for at regelverket følges. Dette innebærer også å sikre at det foreligger et gyldig behandlingsgrunnlag for behandlingen av opplysninger databehandler instrueres om å gjøre.

For utfyllende informasjon om dataansvarliges plikter, se Datatilsynets nettsider.

## 2.8 Databehandlers plikter

Databehandler skal bare behandle helse- og personopplysninger etter instruks fra dataansvarlig. De enkelte punktene skal konkretiseres og utdypes så langt det er nødvendig og relevant i avtalens vedlegg.

### 2.8.1 Generelt

I avtalens punkt 8.1 reguleres nærmere hvordan databehandler kan behandle data på vegne av dataansvarlig. Avtalepunktet er delt i to, som hver angir mer spesifikke krav til hva databehandler plikter å gjøre og å unnlate. Overordnet forplikter databehandler seg til å behandle personopplysninger i samsvar med gjeldende regelverk, dataansvarliges instrukser, samt krav i Norm for informasjonssikkerhet i helse- og omsorgssektoren.

### 2.8.2 Tekniske, organisatoriske og sikkerhetsmessige tiltak

Dataansvarlig og databehandler har en selvstendig plikt til å gjennomføre "*egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen*", jf. personvernforordningen art 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 helse- og personopplysninger som ikke er i overensstemmelse med databehandleravtalen, og tiltak for å gjenopprette tilgjengelighet og tilgang til opplysningene ved hendelser;

Sikkerhetstiltak skal innføres på bakgrunn av en risikovurdering, som blant annet skal ta hensyn til hva slags opplysninger som behandles.

I avtaleteksten er det videre listet opp noen obligatoriske minimumskrav til sikkerhetstiltak, basert på krav i personforordningen. Det er for eksempel krav til internkontrollsystem, logging og rutiner for å oppdage og behandle avvik.

Kravene til tekniske og organisatoriske sikkerhetstiltak bør beskrives og detaljeres nærmere i vedlegg 2 – Detaljerte krav til informasjonssikkerhet. For veiledning til utfylling av dette vedlegget, se veiledningens kapittel 3.2.

## 2.9 Bruk av underleverandør

Databehandler tillates å benytte underleverandører (underdatabehandler) i sin gjennomføring av databehandleroppdraget, forutsatt at disse er kjent for og akseptert av den dataansvarlige. Databehandlers bruk av underleverandører skal derfor til enhver tid fremgå av vedlegg 4.

Det kreves ikke eksplisitt godkjenning av den dataansvarlige ved skifte av eller ved bruk av ny underleverandør, men slike endringer må varsles den dataansvarlige slik at denne får mulighet til å ta stilling til endringen og eventuelt motsette seg endringen.

## 2.10 Overføring av personopplysninger til utlandet

Virksomheter som overfører personopplysninger til utlandet, skal påse at beskyttelsesnivået i personopplysningsloven ikke undergraves ved overføringen. Alle landene innenfor EU/EØS-området har innført personvernforordningen og slik sikret at personopplysninger behandles forsvarlig. Europakommisjonen har i tillegg anerkjent at noen tredjeland har et tilstrekkelig nivå for vern av personopplysninger. Derfor kan personopplysninger fritt overføres til disse statene (liste oppdatert av Europakommisjonen). Dette forutsetter at personopplysningslovens øvrige vilkår er oppfylt.

Dersom det skal benyttes leverandører eller tjenester etablert utenfor EU/EØS, er det krav om å vurdere sikkerhetsnivået i det aktuelle landet. Formålet er å sikre at opplysningene er underlagt samme beskyttelsesnivå som i EU/EØS-området. Når virksomheten overfører personopplysninger til stater utenfor EU/EØS-området, såkalte «tredjeland», skal den bruke et av overføringsgrunnlagene beskrevet i forordningen. Et slikt overføringsgrunnlag kan være EUs standardavtaler for overføring av personopplysninger eller en beslutning fra EU-kommisjonen om tilstrekkelig beskyttelsesnivå i det aktuelle tredjelandet,

Ved overføring av opplysninger til land utenfor EU/EØS må virksomheten sikre at den har tilstrekkelig kompetanse (f.eks. juridisk kompetanse) tilgjengelig for å gjennomføre vurderingene og følge opp databehandleravtalen i tråd med relevante krav.

Se Datatilsynets nettside for oppdaterte og utfyllende opplysninger om overføring til utlandet.

### 2.10.1 Særlig om bruk av skytjenester

En skytjeneste er en betegnelse for alt fra dataprosessering og datalagring til programvare på servere som står i eksterne serverparker, som vanligvis bruker Internett som bærer av datatrafikken.

Tjenestene i skyen kjennetegnes ved at de er laget for dynamisk skalering ved endring i kapasitetsbehov, og ved at det som regel betales for faktisk bruk. Leverandører tilbyr for eksempel serverkapasitet i skyen på timesbasis.

Dersom helse- og personopplysninger skal behandles ved bruk av en skytjeneste, er det noen særlige krav som bør stilles til leverandøren. Dette gjelder særlig kravene i databehandleravtalens punkter 8.1 og 8.2, og dataansvarlig må vurdere om disse kravene skal spesifiseres ytterligere i vedlegg 2 – Detaljerte krav til informasjonssikkerhet.

Se Normens veileder i bruk av skytjenester til behandling av helse- og personopplysninger for vurderingstemaer som dataansvarlig bør vurdere å inkludere i en databehandleravtale som knytter seg til leveranse av skytjenester. Vurderingene må gjøres før oppstart av tjenesten.

Særlige relevante punkter vil være:

- Prinsippene for tilgangsstyring
- Hvordan tilbakelevering av data/applikasjon skal skje ved avslutning av avtalen
- Hvordan dataansvarlig kan få innsyn i den tekniske løsningen
- Hvordan pasientens rettigheter til innsyn i personopplysningene, retting og sletting i varetas, samt innsyn i logger.

- Krav om at leverandør gjennomfører risikovurderinger og at disse revideres ved endringer, samt at dataansvarlig har rett til innsyn eller tilgang til vurderingene

Se også NSMs "Sikkerhetsfaglige anbefalinger ved tjenesteutsetting".

### 2.10.2 Vurderinger ved overføring til tredjeland

I juli 2020 ble kommisjonsbeslutningen Privacy Shield kjent ugyldig som overføringsgrunnlag for personopplysninger av EU-domstolen.[2] Konsekvensen er at virksomheter ikke kan bruke Privacy Shield som overføringsgrunnlag når behandlingen av personopplysninger skjer i USA. Vurderingene som nå må gjøres ved overføring av personopplysninger til USA, må også gjøres for samtlige tredjeland.

Dersom en virksomhet ønsker å overføre personopplysninger til tredjeland, må virksomheten vurdere hvilke andre overføringsgrunnlag som kan benyttes.

For mer informasjon om overføringsgrunnlag ved overføring til land utenfor EU/EØS og hvilke vurderinger som virksomheten må gjøre, se Datatilsynets nettsider.

## 2.11 Taushetsplikt

Databehandleravtalen fastslår at forvaltningslovens taushetspliktbestemmelser skal gjelde tilsvarende for partene og eventuelle underleverandører. I tillegg har enhver som behandler helseopplysninger i behandlingsrettet helseregister etter pasientjournalloven og/eller i helseregister etter helseregisterloven, taushetsplikt etter helsepersonelloven §§ 21 flg. Andre som får adgang eller kjennskap til helseopplysninger fra et behandlingsrettet helseregister eller helseregister, har samme taushetsplikt.

Partene skal ta nødvendige forholdsregler for å hindre at uvedkommende får innsyn i eller kan bli kjent med taushetsbelagt materiale eller informasjon.

Taushetsplikten gjelder også etter oppdragets opphør. Ansatte eller andre som fratrer sin tjeneste hos en av partene eller deres underleverandører, skal pålegges å bevare taushet om forhold som er nevnt ovenfor, også etter fratredelsen.

## 2.12 Revisjon

Punktet fastslår den dataansvarliges rett til innsyn i og kontroll med databehandlerens behandling av opplysninger. Dette gjenspeiler at databehandler kun behandler opplysningene på vegne av den dataansvarlige, og at det påligger den dataansvarlige å sikre at personvernregelverket etterleves.

Punktet om revisjon i standardavtalen er hentet fra tilsvarende bestemmelse i Digitaliseringsdirektoratets databehandleravtale. I bilag C til Digitaliseringsdirektoratets databehandleravtale er det gitt flere alternativer til nærmere rutiner for gjennomføring av revisjoner som kan knyttes til avtalen. Disse alternativene kan på samme måte benyttes i denne standardavtalen. Dersom slike revisjonsrutiner avtales, tas disse inn i vedlegg 3 –

[2] Case C-311/18 (Schrems II)

Administrative bestemmelser. I veiledningen til vedlegg 3 er det gitt eksempler som eventuelt kan benyttes.

## 2.13 Varighet og opphør

Avtalen gjelder så lenge databehandleroppdraget består. Etter at oppdraget er opphørt skal ikke databehandler lenger ha befatning med opplysningene som ble behandlet på vegne av den dataansvarlige. Punktet gir anvisning på hvordan opplysningene skal tilbakeføres/slettes etter at oppdraget er opphørt.

## 2.14 Endring av avtale

Endringer i rettslige rammebetingelser kan innebære behov for endring/tilpasning av avtalen. Partene skal samarbeide om slike nødvendige endringer.

Det vil også være behov for endring av avtalen dersom databehandleroppdraget endres underveis, f.eks. slik at oppdraget utvides til å omfatte nye formål eller behandlinger.

Slike endringer føres samlet i en endringskatalog i Vedlegg 6. Databehandler er ansvarlig for å holde denne oppdatert.

I tillegg må de øvrige vedleggene oppdateres etter behov.

## 2.15 Lovvalg, tvister og verneting

Dette vil være regulert i Tjeneste/oppdragsavtalen.

# 3 Kommentarer til vedleggene

I vedleggene til databehandleravtalen skal det beskrives konkret hva databehandler faktisk skal gjøre.

- **Vedlegg 1** skal alltid fylles ut, og skal fylles ut så godt det lar seg gjøre før avtalen presenteres for databehandleren. Dette omfatter:
    - Hva som er formålet med behandlingen
    - Hva slags type behandling(er) databehandleren skal utføre på vegne av dataansvarlig
    - Hva slags personopplysninger som skal behandles
    - Hvilke kategorier av registrerte som det behandles opplysninger om
- **Vedlegg 2** skal fylles ut, med mindre dette allerede er tilfredsstillende beskrevet i Tjeneste/oppdragsavtalen. Dette gjelder:
    - Hvilke tekniske og organisatoriske tiltak databehandler må iverksette for å ivareta informasjonssikkerheten
- **Vedlegg 3** skal alltid fylles ut med kontaktinformasjon og eventuelt øvrige relevante administrative opplysninger, for eksempel rutiner for revisjon.
- **Vedlegg 4** skal fylles ut dersom databehandler benytter underleverandører i utførelsen av behandlingen
- **Vedlegg 5** skal benyttes dersom partene er blitt enige om å gjøre endringer i den generelle avtaleteksten ved avtaleinngåelsen
- **Vedlegg 6** skal ikke fylles ut ved avtaleinngåelsen, men benyttes dersom det gjøres endringer i oppdraget/behandlingen eller avtalen for øvrig etter avtaleinngåelsen

Merk at eksemplene som gis i tabellene under verken er ment å være førende, begrensende eller uttømmende. Opplistingen er kun ment å være eksempler på behandlinger/behandlingsaktiviteter, opplysningstyper, personkategorier og sikkerhetskrav som ofte inngår eller typisk stilles i et databehandleroppdrag. Det må i ethvert tilfelle gjøres en konkret vurdering slik at tabellene fylles ut i samsvar med det aktuelle oppdraget.

Ofte vil det meste av informasjonen man trenger for vedlegg 1 og 2 ligge i behandlingsprotokollen knyttet til det enkelte formålet med behandlingen.[3] Hvis virksomheten (dataansvarlig) ikke har protokollført behandlingen som databehandler skal utføre, kan protokollen i stor grad fylles ut med opplysningene som skal fylles inn i vedlegg 1 og vedlegg 2, eventuelt også vedlegg 4.

[3] Datansvarlig har i hht. Personvernforordningen art. 30 plikt til å føre protokoll over alle behandlingsaktiviteter som gjennomføres i virksomheten. Protokollen skal i tilknytning til hver behandlingsaktivitet også inneholde formålene med behandlingen, kategoriene av registrerte og kategoriene av personopplysninger, mottakere av personopplysninger, eventuelle overføringer til tredjestater, planlagte frister for sletting og en generell beskrivelse av sikkerhetstiltak som nevnt i personvernforordningen artikkel 32.

Tabellene skal holdes oppdatert slik at de til enhver tid gjenspeiler de faktiske forhold i databehandleroppdraget. Dette innebærer at avtalens vedlegg må oppdateres hvis dataansvarlig for eksempel ønsker behandlet flere kategorier av personopplysninger eller pålegger databehandler å utføre andre typer tjenester.

## 3.1 Vedlegg 1 – Behandlingens formål, opplysninger og behandlinger

I dette vedlegget skal det det spesifiseres nærmere:

- hva som er formålet med og varigheten av behandlingen(e) – punkt A)
- hvilke behandlinger som omfattes – punkt B)
- hvilke opplysningstyper som omfattes – punkt C)
- hvilke kategorier av personer som registreres – punkt D)

Dersom databehandleroppdraget innebærer behandling av opplysninger i flere tjenester/til flere formål, anbefales å beskrive disse hver for seg slik at avtalen blir lettere å lese. Slik vil også hver behandling knyttes til spesifikke og uttrykkelig angitte formål.

Dersom oppdraget eksempelvis gjelder to tjenester: "*Saksbehandlingstjenesten XX"* og "*Overføringstjenesten YY*", vil en strukturering av vedlegg 1 kunne være:

1. Saksbehandlingstjenesten XX
   1A – Formålet med og varigheten av behandlingen
   1B – Behandling av helse- og personopplysninger
   1C – Typer av opplysninger
   1D – Kategorier av registrerte
2. Overføringstjenesten YY
   2A - Formålet med og varigheten av behandlingen
   2B - Behandling av helse- og personopplysninger
   2C - Typer av opplysninger
   2D - Kategorier av registrerte

### A. Formålet med og varigheten av behandlingen[4]

Formål

Før en behandling av helse- og personopplysninger kan starte, må det foreligge et eller flere klart definerte formål med behandlingen. Dette er et av de grunnleggende personvernprinsippene i personvernforordningen.

Et formål er en tydelig og avgrenset beskrivelse av hva personopplysningene skal brukes til. Det definerte formålet avgjør hva man kan bruke opplysningene til, og virksomheten

[4] For mer veiledning om fastsetting av formål, se Datatilsynets nettsider.

kan ikke bruke opplysningene til andre formål senere. Et eksempel på formål i helse- om omsorgssektoren kan være å oppfylle dokumentasjonsplikten for helsepersonell.

Det er ikke tilstrekkelig tydelig å angi for eksempel "*administrasjon av ansattopplysninge*r" som formål. Det må presiseres hva opplysningene skal brukes til, for eksempel "*registrering av arbeidstid og behandling av søknader om fravær*".

Varighet

Varigheten av behandlingen skal angis så presist som mulig. Dersom behandlingen for eksempel er knyttet til et tidsavgrenset prosjekt, vil oppstartdato og sluttdato for prosjektet kunne angis. I andre tilfeller vil det ikke være mulig å angi behandlingens varighet like presist, men må knyttes til andre vurderinger av når formålet med behandlingen er oppnådd.

Eksempler:

| Navn på tjeneste | Formålet med behandlingen | Varigheten av behandlingen |
|---|---|---|
| *Skylagringstjeneste* | *Oppbevaring av database/register* | *Til formålet er oppnådd* |
| *Helseinformasjon.no* | *Samle inn, lagre og videresende opplysninger slik at brukeren (forsker) kan søke om helsedata til sekundærbruk.* | *I utgangspunktet så lenge brukerprofilen består. Ytterligere detaljering vil gis i etterfølgende instruks.* |
| *Søknadsoversikten* | *Formålet med Søknadsoversikten er å ha en visuell fremstilling og løpende oversikt over alle søknader som har kommet inn i søknadsmottaket.* | *Fra oppstart av søknadsmottaket dato XX tom dato XX.* |
| *Søknad- og saksbehandlingstjeneste* | *Gi veiledning til søkere om søknadsprosess, datakilder og analysetjenester.*<br>*Bistå Dataansvarlig med å behandle søknad om tilgang til helsedata, herunder sikre likebehandling og oppfyllelse av Dataansvarliges utrednings- og informasjonsplikt.*<br>*Bistå Dataansvarlig med å sikre at søknader om tilgang til helsedata er tilstrekkelig opplyst* | *Starter ved førstegangs kontakt med bruker/søker.*<br>*Oppbevares så lenge det er relevant for å behandle søknaden eller oppfylle øvrige formål med behandlingen.*<br>*Arkivering skjer i samsvar med gjeldende regelverk.* |

| | | |
|---|---|---|
| | *Koordinere søknadsprosessen mellom ulike registre og andre offentlige aktører.*<br>*Tilrettelegge for søkers innsyn i saksgangen.*<br>*Kommunikasjon med søker under hele prosessen.*<br>*Tilrettelegge for arkivering.* | |

### B. Behandling av helse- og personopplysninger

Under "Behandling" skal den overordnede typen av behandling av helse- og personopplysninger angis. Alle behandlinger skal beskrives nærmere med tilhørende behandlingsaktiviteter. Eksempler på behandlinger er angitt i tabellen under. Andre typer behandlinger fylles inn ved behov.

Under "Behandlingsaktiviteter" skal behandlingen nærmere beskrives. Det skal gis en kort beskrivelse av hvordan behandlingen konkret utføres. Eksempelvis: Dersom "innsamling" er en behandling som utføres, skal det beskrives hvordan innsamlingen skjer, herunder hvilken teknisk løsning som benyttes og hvem opplysningene samles inn fra. Disse kan for eksempel samles inn ved at den registrerte legger inn opplysningene i en portal, eller at opplysningene samles inn automatisk fra en database.

I tabellen under brukes tjenesten "Søknad- og saksbehandlingstjeneste" (se tabellen over) som gjennomgående eksempel der det er relevant. Formålet med det gjennomgående eksemplet er å vise hensiktsmessig detaljeringsgrad av de ulike aktivitetene.

Eksempler:

| Behandling | Behandlingsaktiviteter |
|---|---|
| *Innsamling* | *Opplysningene samles inn ved at den registrerte legger inn opplysninger i en søknadsportal.* |
| *Registrering* | |
| *Organisering* | |
| *Strukturering* | *Søknadstjenesten strukturerer søknadsinformasjonen slik at den er lett lesbar og tilgjengelig for dataansvarlig.* |
| *Lagring* | *Databehandler lagrer søknadsinformasjonen til formålet er oppnådd. Dataansvarlig gir instruks om når opplysningene ikke lengre skal lagres.* |
| *Tilpasning eller endring* | |
| *Gjenfinning* | |
| *Sammenstilling* | |
| *Sletting eller tilintetgjøring* | *Databehandler sletter søknadsinformasjonen når Dataansvarlig gir instruks om dette/ Databehandler sletter* |

| | |
|---|---|
| | *søknadsinformasjonen dato XX, i henhold til instruks fra Dataansvarlig.*<br><br>*Databehandler skal sørge for sletting dersom den registrerte trekker sitt samtykke til behandling av personopplysninger eller begjærer sletting.* |
| *Utlevering* | *Databehandler utleverer opplysninger til den registrerte dersom den registrerte ber om innsyn i egne personopplysninger. Opplysningene skal gjøres tilgjengelig for den registrere i et lett tilgjengelig format.* |

## C. Typer av opplysninger

Med type personopplysninger menes de konkrete opplysningene som blir behandlet.

Eksempler:

| Personopplysninger | Særlige kategorier av personopplysninger: helseopplysninger |
|---|---|
| *Navn*<br><br>*Telefonnummer*<br><br>*Fødselsnummer*<br><br>*Bosted*<br><br>*Kundenummer*<br><br>*Logginformasjon*<br><br>*Arbeidserfaring* | *Legemiddelbruk*<br><br>*Diagnoseopplysninger*<br><br>*Opplysninger fra helseregistre*<br><br>*Identifiserende lyd- eller videoopptak*<br><br>*Skriftlig kommunikasjon mellom helsetjenesten og pasient* |

## D. Kategorier av registrerte

Her skal det beskrives hvem behandlingen av helse- og personopplysninger omfatter. Dersom det behandles opplysninger om særlig sårbare eller utsatte grupper, bør dette fremgå særskilt.

Eksempler:

| Kategorier av registrerte |
|---|
| *Pasienter* |
| *Barn* |
| *Foreldre* |

*Søkere av …*

*Brukere av …*

*Helsepersonell*

*Ansatte ved …*

*Medarbeidere i …*

*Leverandører til …*

## 3.2 Vedlegg 2 – Detaljerte krav til informasjonssikkerhet

I dette vedlegget skal man nærmere beskrive hvilke krav til informasjonssikkerhet som gjelder for databehandleroppdraget. Dataansvarlig bør innledningsvis beskrive hvilke krav som stilles til databehandler. Deretter bør det beskrives nærmere hvordan databehandler skal oppfylle pliktene i avtalens pkt. 8.2 "Databehandlers plikter".

Det er listet opp en rekke eksempler på krav i tabellen under. Alle kravene vil ikke være aktuelle for alle avtaler, men er ment som eksempler på krav og hvor presist kravene bør angis. Kravene kan for eksempel forplikte databehandler til å følge visse standarder, eller pålegge en bestemt måte å gjennomføre kryptering på.

I enkelte tilfeller vil krav til informasjonssikkerhet være spesifisert i Tjeneste/oppdragsavtalen. Dersom dataansvarlig vurderer disse kravene som tilstrekkelige for det konkrete databehandleroppdraget, er det ikke nødvendig å beskrive kravene en gang til i dette vedlegget. Da bør det henvises til hvor informasjonssikkerhet er regulert i Tjeneste/oppdragsavtalen.

Merk at databehandleravtalen med vedlegg går foran Tjeneste/oppdragsavtalen ved konflikt. Det betyr at dersom et forhold er ulikt regulert i databehandleravtalen og i Tjeneste/oppdragsavtalen, er det innholdet i databehandleravtalen som legges til grunn. Hvis det for eksempel er definert ulik lengde på lagringstiden for personopplysningene i de to avtalene, er det lagringstiden som er oppgitt i databehandleravtalen som er gjeldende.

Eksempler:

| Nr. | Tema | Krav |
|---|---|---|
| | *Norm for informasjonssikkerhet i helse- og omsorgssektoren* | *Databehandler skal følge relevante krav i Norm for informasjonssikkerhet (se faktaark 10, og hvilke krav som er angitt for databehandler)* |
| | *ISMS / styringssystem* | *Databehandler skal ha et styringssystem for informasjonssikkerhet som sikrer at databehandleren på en systematisk og dokumentert måte iverksetter og følger opp informasjonssikkerhet i virksomheten i tråd med relevante krav* |

| | | |
|---|---|---|
| | | *og innenfor akseptabel risiko. Styringssystemet skal være basert på anerkjente standarder.* |
| | *Sikkerhetsrevisjon*[5] | *Databehandler skal jevnlig gjennomføre interne revisjoner av informasjonssikkerhet. Dokumentasjonen skal være tilgjengelig for Dataansvarlig.*<br><br>*Dataansvarlig har adgang til å gjennomføre sikkerhetsrevisjoner hos Databehandler, også ved bruk av tredjepart. Revisjon skal varsles minimum 14 dager før.*<br><br>*Retten til revisjon inkluderer testing av tekniske, organisatoriske og fysiske sikkerhetstiltak.* |
| | *Sikring av data* | *Databehandler skal ha mekanismer for data under transport, prosessering og lagring for å ivareta integritet og konfidensialitet.* |
| | *Fjernaksess* | *Kravene i Normens veileder for fjernaksess skal følges.* |
| | *Tilgangsstyring* | *I utgangspunktet skal ikke Databehandler ha tilgang til innholdet i Dataansvarliges data, med mindre dette er nødvendig for å oppfylle forpliktelser Databehandler har etter denne avtalen. I slike tilfeller skal kun personell hos Databehandler med tjenstlig behov ha tilgang. Tilgang skal logges, og det skal vises til en begrunnelse for tilgang.*<br><br>*For brukere med privilegerte tilganger, uavhengig av om dette gir direkte tilgang til Dataansvarliges data, skal hver bruker være personlig, strengt begrenset og kontrollert, og med tilhørende nødvendige sikkerhetstiltak.* |
| | *Autentisering* | *Ved tilgang til data ved tjenstlig behov skal det benyttes personlige brukernavn med passord. Databehandler skal ha etablert passordpolicy.*<br><br>*Dataansvarlig kan i instruks stille spesifikke krav til autentisering, f.eks. at sterk autentisering skal benyttes.* |
| | *Tiltak mot digitale angrep* | *Databehandler skal implementere tiltak mot digitale angrep som f.eks. tjenestenektangrep og skadelig kode.* |
| | *Logging og sporbarhet* | *Databehandler skal implementere logging som viser tilgang til Dataansvarliges data, og hvilke operasjoner som Databehandler har utført på dataene.*<br><br>*Loggene skal sikres mot uautorisert innsyn, endring og sletting.*<br><br>*Oppbevaringstid skal bestemmes ut fra formålet med loggingen og avklares med Dataansvarlig.* |
| | *Redundans og skalering* | *Databehandler skal ha en infrastruktur som sikrer kapasitet og oppetid i tråd med avtalt tjenestenivå gjennom tiltak som redundans og skalering.* |
| | *Testdata* | *Dataansvarliges data skal ikke benyttes for testformål uten at det er avtalt skriftlig med Dataansvarlig. Eventuell anonymisering* |

[5] Se også merknader til pkt. 2.12

| | | |
|---|---|---|
| | | *skal skje på instruks fra Dataansvarlig. I tilfeller der Dataansvarliges data benyttes til test etter avtale, skal disse sikres på samme måte som produksjonsdata.*<br><br>*Der det benyttes produksjonsdata til testformål, skal disse slettes etter at test er utført.* |
| | *Sletting og tilbakelevering* | *Databehandler skal ha rutiner og tekniske løsninger som sikrer at alle Dataansvarliges data slettes eller leveres tilbake på instruks fra Dataansvarlig, eller ved opphør av databehandleravtalen. Dette omfatter også data lagret på backupmedia og logger.* |
| | *Lagringstid* | *Lagring av opplysninger skal bestemmes av Dataansvarlig ut fra formålet med behandlingen. Når formålet med behandlingen er oppnådd skal opplysningene slettes i henhold til punktet om sletting og tilbakelevering i dette vedlegget.* |
| | *Backup og restore* | *Databehandler skal ha forsvarlige backup- og restorerutiner som testes regelmessig.* |
| | *Kryptering ved lagring* | *Data skal krypteres ved lagring hvis Dataansvarlig stiller krav om dette.* |
| | *Kryptering i kommunikasjon* | *Data skal alltid krypteres i kommunikasjon i hht NSM spesifikasjoner.* |
| | *Adgangskontroll* | *Databehandler skal ha tilstrekkelig fysisk sikring hvor Dataansvarliges data er tilgjengelig.* |
| | *Sikkerhetsarkitektur* | *Databehandler skal separere data som tilhører forskjellige kunder. Databehandlers egne data skal separeres fra kundenes data. Databehandler skal ha rutiner som sikrer at Dataansvarliges data ikke overføres til andre virksomheter uten at dette er skriftlig avtalt med Dataansvarlig.* |
| | *Autorisasjonsregister* | *Databehandler skal til enhver tid ha et oppdatert autorisasjonsregister for personell som er autorisert for tilgang til Dataansvarliges informasjon og tjenester.* |

## 3.3 Vedlegg 3 – Administrative bestemmelser

I dette vedlegget skal partene angi hver sine kontaktpersoner.

Hver av partene bør oppgi navn og kontaktinformasjon til en hovedkontakt for Databehandleravtalen.

Det kan, om det er hensiktsmessig, angis flere kontaktpersoner med ansvar for ulike forhold - for eksempel hvem som skal motta meldinger om avvik og hvem som skal underrettes om eventuelle planer om å benytte andre underleverandører eller skifte ut underleverandører.

Dersom det avtales øvrige administrative forhold, slik som f.eks. regelmessige møter, rapportering, oversendelsesformater mv, skal dette også fylles ut i dette vedlegget.

Det samme gjelder dersom det avtales nærmere revisjonsrutiner, jf. avtalens punkt 12. Alternativene nedenfor er eksempler som kan benyttes som de er, enkeltvis eller samlet, avhengig av behov. De kan også benyttes som utgangspunkt for konkrete tilpasninger.

**Eksempler på revisjonsrutiner:**

*For å kontrollere etterlevelse av gjeldende personvernregler og Databehandleravtalen er det avtalt følgende revisjonsrutiner (flere valg mulig):*

Eksempel 1

*Dataansvarlig har rett til å utføre revisjon på Databehandlers forretningssted for å verifisere Databehandlers etterlevelse av sine plikter i henhold til denne Databehandleravtalen eller gjeldende personvernregler.*

*Slike revisjoner skal:*

- *Gjennomføres etter rimelig forhåndsvarsel og maksimalt én gang i året, med mindre sikkerhetsbrudd hos Databehandler eller andre særlige forhold gir grunn for hyppigere revisjoner;*
- *Foregå innenfor normal arbeidstid og ikke forstyrre Databehandlers virksomhet unødvendig;*
- *Utføres av ansatte hos Dataansvarlig eller av tredjepart som er godkjent av Partene og underlagt taushetsplikt.*

*Databehandler plikter å stille til rådighet de ressurser som med rimelighet kan kreves for å gjennomføre revisjonen.*

Eksempel 2

*Databehandleren skal benytte ekstern revisor til å attestere at sikkerhetstiltak er etablert og virker etter hensikten. Slik revisjon skal:*

- *gjennomføres én gang årlig,*
- *utføres i henhold til anerkjente attestasjonsstandarder, for eksempel ISAE 3402.*
- *utføres av en uavhengig tredjepart med tilstrekkelig kunnskap og erfaring*

*Rapportene skal fremlegges for Dataansvarlig på forespørsel. Databehandler skal i tillegg gi slik informasjon og bistand som er nødvendig for at Dataansvarlig kan etterleve sine forpliktelser etter gjeldende personvernregelverk.*

Eksempel 3

*For standardiserte tredjepartstjenester som leveres av Underleverandør kan det fremlegges tredjepartsrevisjon forutsatt at revisjonen er gjennomført etter alminnelig anerkjente prinsipper og av sertifisert revisor.*

## 3.4 Vedlegg 4 – Underleverandører

I tabellen skal det angis hvilke underleverandører Databehandler benytter seg av på tidspunktet for avtaleinngåelsen. Dersom Databehandler ønsker å benytte flere underleverandører eller skifte en underleverandør, skal Dataansvarlig varsles og gis mulighet til å motsette seg endringen. Dersom Dataansvarlig godtar endringen, enten eksplisitt eller ved passivitet, skal dette vedlegget oppdateres og sendes til Dataansvarliges kontaktperson (som skal angis i vedlegg 3 - Administrative bestemmelser).

I tabellen skal underleverandørens navn, organisasjonsnummer eller annen identifikator og adresse angis og hvilken tjeneste (overordnet beskrivelse av behandlingen) underleverandøren utfører på vegne av Databehandler. Videre skal helse- og personopplysningenes behandlingssted oppgis. Dette omfatter også steder hvor underleverandøren har tilgang til eller på annen måte behandler personopplysninger fra (fjernaksess). Behandlingssted er særskilt viktig å angi, siden den kan virke inn på Dataansvarliges plikt til å ha gyldig overføringsgrunnlag til land utenfor EU/EØS.

Nærmere omtale av kravene som gjelder ved overføring til utlandet er gitt i punkt 2.10.

Tabellene oppdateres ved endringer og sendes til Dataansvarliges kontaktperson.

Eksempler:

| Navn | Org.nr | Adresse | Leveransetype (behandling) | Behandlingssted |
|---|---|---|---|---|
| *[Navn]* | *[Org.nr]* | *[Adresse]* | *Datasenter, hosting* | *Stockholm, Sverige* |
| *[Navn]* | *[Org.nr]* | *[Adresse]* | *IT-supporttjenester* | *Oslo, Norge*<br>*Chennai, India*<br>*Kiev, Ukraina* |
| *[Navn]* | *[Org.nr]* | *[Adresse]* | *Backup* | *Paris, Frankrike* |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## 3.5 Vedlegg 5 - Endringer i den generelle avtaleteksten ved avtaleinngåelsen

Endringene til avtaleteksten eller tillegg til denne skal fremkomme her, slik at den generelle avtaleteksten forblir uendret i dokumentet. Det må fremkomme klart og utvetydig hvilke bestemmelser i avtalen det er gjort endringer til og hvordan punktet/avsnittet/setningen skal lyde etter endringen.

Det er mulig å gjøre endringer til alle punkter i avtalen, også der hvor det ikke klart henvises til at endringer kan avtales. Endringer som er i strid med relevant lovgivning vil ikke være gyldige, dette følger av avtalens punkt 1.

Eksempel på endringstabell:

| Punkt i avtalen | Erstattes med |
|---|---|
| *Kapittel x.x.x, avsnitt y* | *[Sett inn ny formulering/tekst]* |
| | |
| | |
| | |

## 3.6 Vedlegg 6 – Endringer etter avtaleinngåelsen

Dette bilaget skal ikke fylles ut ved avtaleinngåelse, men må ligge ved selv om det foreløpig er tomt.

Dersom partene har kommet til enighet om en endring i behandlingen/oppdraget, avtaleteksten eller andre forhold skal endringen fremkomme her. Berører endringen forhold som er regulert i et vedlegg til avtalen kan det være hensiktsmessig å utarbeide en oppdatert versjon av vedlegget som inkluderer endringen.

Hver endring skal være underskrevet av bemyndiget representant for partene.

Det er databehandler som er ansvarlig for at det føres en fortløpende katalog over endringene som utgjør bilag 6. Databehandler er også ansvarlig for at dataansvarlig uten ugrunnet opphold gis en oppdatert kopi.

Endringstabell:

| Nr. | Dato | Endring | Ev. vedlegg | Gjelder fra |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |