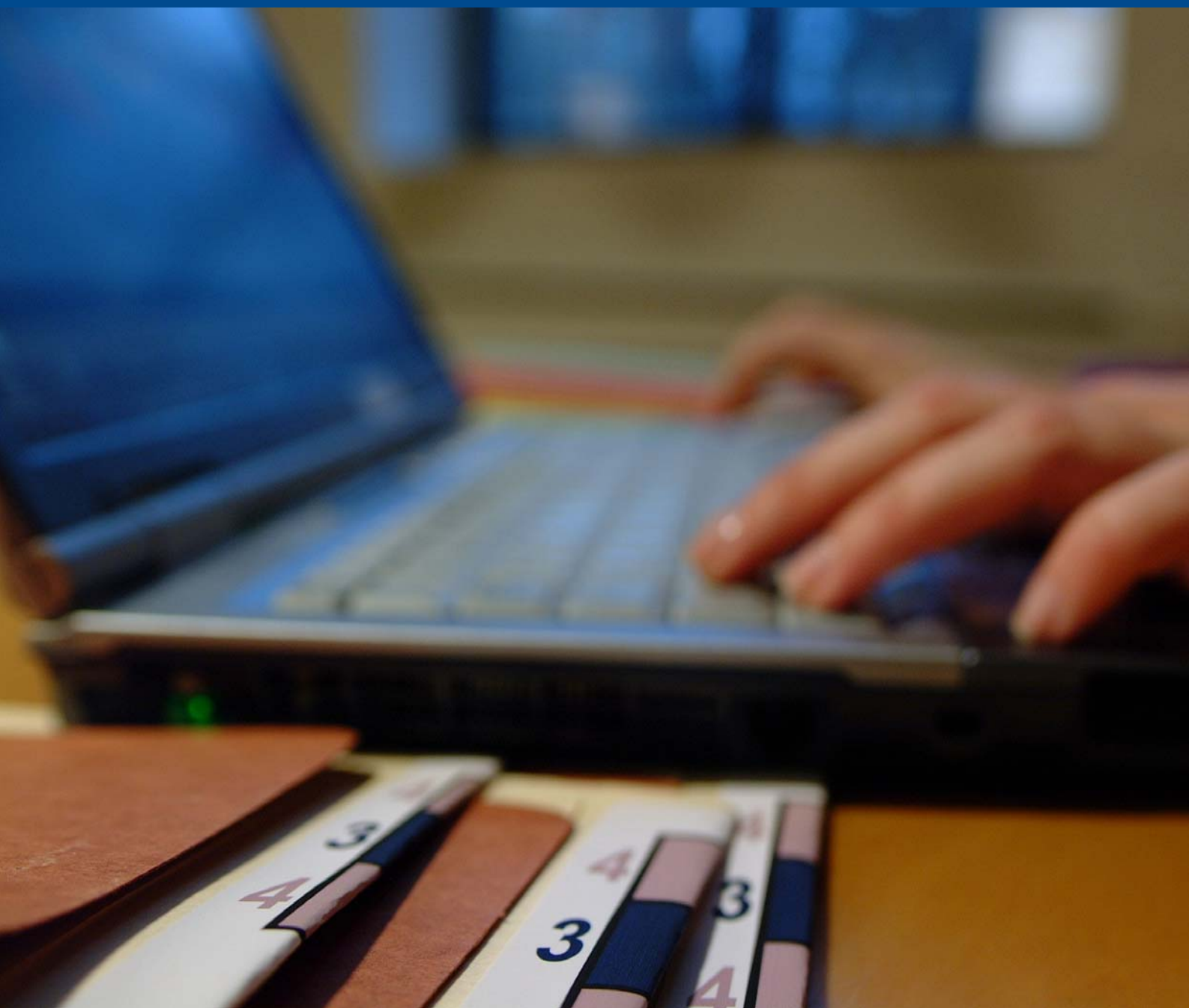


Databehandleravtaler

etter personopplysningsloven og helseregisterloven

Veileder

26.05.2009



Innholdsfortegnelse

DEL I	5
Veileder - databehandleravtaler	6
Datatilsynet.....	6
Forutsetninger og avklaringer.....	7
Minimumskrav	8
1 Angi formålet	8
2 Beskrive hvordan personopplysningene skal behandles.....	8
2.1 Konkrete rutiner for bruk av personopplysningene.	8
2.2 Regler for utlevering av personopplysningene.	8
3 Bruk av underleverandør skal reguleres i avtalen.....	8
4 Ivareta den registreres rettigheter.....	9
5 Avtalen må pålegge databehandleren å ha tilfredstillende informasjonssikkerhet.	9
6 Avtalens varighet	10
7 Overføring til utlandet.....	10
DEL II	11
<i>Vedlegg A: Avtaleskisse – databehandleravtale etter personopplysningsloven.....</i>	<i>12</i>
1. Avtalens hensikt	13
2. Formål	13
3. Databehandlers plikter.....	13
4. Bruk av underleverandør.....	13
5. Sikkerhet.....	14
6. Sikkerhetsrevisjoner	14
7. Avtalens varighet.....	14
8. Ved opphør	14
9. Meddelelser	15
10. Lovvalg og verneting	15
<i>Vedlegg B: Avtaleskisse – databehandleravtale etter helseregisterloven (NB – gjelder i hovedsak helse/forskning)</i>	<i>16</i>
1. Avtalens hensikt	17
2. Formål	17
3. Databehandlers plikter.....	17

4. Bruk av underleverandør.....	17
5. Sikkerhet	18
6. Sikkerhetsrevisjoner.....	18
7. Avtalens varighet	18
8. Ved opphør.....	18
9. Meddelelser	19
10. Lovvalg og vernetting	19

DEL I

Veileder - databehandleravtaler

Denne veilederen inneholder to skisser til databehandleravtaler. Veilederen, del I, bør leses parallelt med at man ser på en av avtaleskissene som er vedlegg i del 2. Vedlegg A inneholder et forslag til avtale etter personopplysningsloven, og vedlegg B inneholder et forslag til avtale etter helseregisterloven.

Det har ikke vært hensiktsmessig å lage en uttømmende mal eller liste over det som kreves av en databehandleravtale. Til det er de potensielle avtaleparter for forskjellige, og utkastene ville blitt uhåndterlige for de fleste.

Datatilsynet har likevel, med denne korte veiledningen og forslagene til utforming av en databehandleravtale etter henholdsvis personopplysningsloven og helseregisterloven, forsøkt å skissere hvordan hovedelementene bør være.

Om den behandlingsansvarlige er usikker på om avtalen blir tilstrekkelig konkret, kan virksomheten kontakte Datatilsynet og søke råd. Datatilsynet ser helst at virksomheten har laget et utkast til avtale før det søkes veiledning. På den måten blir vi sammen mer effektive, og Datatilsynet kan lettere svare på om det mener avtalen er tilstrekkelig knyttet til det den skal regulere.

Dokumentene kan lastes ned fra Datatilsynets hjemmesider:

www.datatilsynet.no/databehandler

Datatilsynet

Forutsetninger og avklaringer

Noen virksomheter velger å sette ut hele eller deler av behandlingen av personopplysninger til andre virksomheter, såkalte databehandlere. 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.

En databehandleravtale kan være en frittstående avtale mellom partene, eller en integrert del av annet avtaleverk.

Personopplysningslovens § 15 sier at en databehandler ikke kan behandle personopplysninger på en annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. Tilsvarende gjelder for helseregisterlovens § 18.

Den behandlingsansvarlige skal forsikre seg om at databehandleren har tilstrekkelig sikkerhetsnivå, jf. personopplysningslovens § 15 (helseregisterlovens § 18). For mer informasjon se temaside om internkontroll og informasjonssikkerhet på Datatilsynets nettsider.

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.

Den som fungerer som databehandler vil ha selvstendig ansvar for personopplysninger som behandles på egne vegne, eksempelvis opplysninger om egne ansatte.

Behandling av sensitive personopplysninger vil antagelig kreve en mer detaljert avtale enn en avtale om et enkeltstående faktureringsoppdrag. Videre vil detaljeringsgraden variere fra helt grunnleggende krav til klart spesifiserte tiltak for eksempel når det gjelder informasjonssikkerhet.

Minimumskrav

Punktene nedenfor, sammen med malen, er minimumskrav for hva som bør være med i en databehandleravtale. Behandlingsansvarlige kan sette strengere krav enn hva som følger av personopplysningsloven, men ikke avtale vilkår som er i strid med kravene personopplysningsloven stadfester.

1 Angi formålet

Det skal klart framgå av avtalen hva som er formålet med behandlingen av personopplysningene. Databehandler skal kun behandle opplysningene i henhold til formålet den behandlingsansvarlige har definert.

Typiske eksempler på databehandlerrelasjoner er makulering av papirdokumenter, IT-drift, fakturering, kameraovervåkning, håndtering av personalopplysninger som utbetaling av lønn og lignende.

2 Beskrive hvordan personopplysningene skal behandles

Det skal tydelig fremgå av avtalen hva databehandler skal gjøre med personopplysningene.

Skal de kun oppbevares/lagres for framtidig bruk (arkivinstans), eller skal de bearbeides? Avtalen skal også klart regulere/avklare om det skal skje andre behandlinger, som for eksempel kobling med andre personopplysninger/registre eller lignende.

2.1 Konkrete rutiner for bruk av personopplysningene.

Databehandler har ikke råderett over personopplysningene, og kan dermed heller ikke behandle disse til egne formål.

2.2 Regler for utlevering av personopplysningene.

Databehandler skal kun forholde seg til avtalen. Hvis han skal utlevere personopplysninger til andre eksterne parter må dette framgå klart av databehandleravtalen. Avtalen må inneholde bestemmelser om hvem som skal kunne få personopplysninger utlevert, og vilkår i tilknytning til dette.

3 Bruk av underleverandør skal reguleres i avtalen

Hvis databehandler gjør bruk av underleverandører av tjenester, skal dette klart framgå av avtalen mellom databehandler og behandlingsansvarlig. Personopplysningsforskriften stiller i § 2-15 krav til sikkerheten hos andre virksomheter – kontraktsparten.

4 Ivareta den registreres rettigheter

Avtalen kan inneholde en arbeidsfordeling mellom behandlingsansvarlige og databehandler, for eksempel hvem som skal håndtere og behandle henvendelser fra de registrerte. Typeeksemplet er at den behandlingsansvarlige mottar en henvendelse, videreformidler denne til databehandler som oppfyller den registrertes forespørsel. Dette kan for eksempel gjelde spørsmål om

- innsyn, se personopplysningslovens § 18 (helseregisterlovens § 22),
- retting og sletting, se personopplysningslovens § 27 og § 28 (helseregisterlovens kap. 5)

5 Avtalen må pålegge databehandleren å ha tilfredstillende informasjonssikkerhet.

Det fremkommer av personopplysningslovens § 13 (helseregisterlovens § 16) at det stilles krav om tilfredsstillende informasjonssikkerhet. Avtalen må klargjøre hva databehandler skal ha på plass av sikringstiltak for å ivareta konfidensialitet, integritet og tilgjengelighet for behandling av personopplysninger, jf. personopplysningsforskriftens kapittel 2.

Hva skal gjøres for å ivareta:

Konfidensialitet: Å sikre at informasjon bare er tilgjengelig for de som skal ha tilgang.

Integritet: Å sikre at personopplysninger ikke endres uautorisert eller utilsiktet.

Tilgjengelighet: Sikre tilgang til personopplysninger hvor tilgjengelighet er nødvendig.

Avtalen bør inneholde bestemmelser om:

- Avvikshåndtering, jf. forskriftens § 2-6 (avviksmelding).
- Avklaring av hvem som har ansvaret for å melde avviket til Datatilsynet dersom avviket har ført til uautorisert utlevering av personopplysninger.
- Tilgangskontroll og tilstrekkelige kontrollmekanismer f. eks. loggføring.
- Andre krav som fremkommer av forskriftens kapittel 2:
 - o Taushetsplikt
 - o Sikkerhetsrevisjoner
 - o Fysiske sikringstiltak
 - o Hvordan rutiner og lignende skal dokumenteres
 - o Personell hos partene som skal ha tilgang til personopplysningene

Begge parter har et selvstendig ansvar etter personopplysningslovens § 13 (helseregisterlovens § 16), jf. personopplysningsforskriftens kapittel 2, og avtalen kan regulere arbeidsdelingen mellom partene.

6 Avtalens varighet

Avtalen må inneholde:

- Opplysninger om avtalens varighet.
- Hva som skal skje med opplysningene etter at avtalen er opphørt – om opplysningene skal tilbakeføres eller slettes, og om lagrede sikkerhetskopier skal tilbakeføres eller slettes.
- Hvor ofte det skal foretas sikkerhetsrevisjon.

7 Overføring til utlandet

Dersom det er aktuelt at personopplysningene skal overføres til utlandet må dette reguleres i avtalen. Det vises til personopplysningslovens § 29 og § 30. Mer informasjon finnes på Datatilsynets hjemmesider vedrørende dette temaet.

DEL II

Vedlegg A: Avtaleskisse – databehandleravtale etter personopplysningsloven

Databehandleravtale

I henhold til personopplysningslovens § 13, jf. § 15 og personopplysningsforskriftens kapittel 2.

mellom

.....

behandlingsansvarlig

og

.....

databehandler

1. Avtalens hensikt

Avtalens hensikt er å regulere rettigheter og plikter etter Lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven) 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.

Avtalen regulerer databehandlers bruk av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse.

2. Formål

Her skal det redegjøres for formålet med databehandleravtalen. Herunder:

- hvilke personopplysninger som skal behandles
- hvilke behandlinger som omfattes av avtalen
- hva som er rammene for databehandlers håndtering av personopplysninger

3. Databehandlers plikter

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

Databehandler plikter å gi behandlingsansvarlig tilgang til sin sikkerhetsdokumentasjon, og bistå, slik at behandlingsansvarlig kan ivareta sitt eget ansvar etter lov og forskrift.

Behandlingsansvarlig har, med mindre annet er avtale eller følger av lov, rett til tilgang til og innsyn i personopplysningene som behandles og systemene som benyttes til dette formål. Databehandler plikter å gi nødvendig bistand til dette.

Databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til iht. denne avtalen. Denne bestemmelsen gjelder også etter avtalens opphør.

4. Bruk av underleverandør

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

Avtale med underleverandører

En slik avtale bør gjøres som et tillegg til denne avtalen.

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.

5. Sikkerhet

Databehandler skal oppfylle de krav til sikkerhetstiltak som stilles etter personopplysningsloven og personopplysningsforskriften, herunder særlig personopplysningslovens §§ 13 – 15 med forskrifter. Databehandler skal dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjonen skal være tilgjengelig på behandlingsansvarliges forespørsel.

Avviksmelding etter personopplysningsforskriftens § 2-6 skal skje ved at databehandler melder avviket til behandlingsansvarlig. Behandlingsansvarlig har ansvaret for at avviksmelding sendes Datatilsynet.

6. Sikkerhetsrevisjoner

Behandlingsansvarlig skal avtale med databehandler at det gjennomføres sikkerhetsrevisjoner jevnlig for systemer og lignende som omfattes av denne avtalen.

Revisjon

Revisjonen kan omfatte gjennomgang av rutiner, stikkprøvekontroller, mer omfattende stedlige kontroller og andre egnede kontrolltiltak.

7. Avtalens varighet

Avtalen gjelder så lenge databehandler behandler personopplysninger på vegne av behandlingsansvarlig.

eller

avtalen gjelder til _____

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

Avtalen kan sies opp av begge parter med en gjensidig frist på _____, jf. punkt 8 i denne avtalen.

8. Ved opphør

Ved opphør av denne avtalen plikter databehandler å tilbakelevere alle personopplysninger som er mottatt på vegne av den behandlingsansvarlige og som omfattes av denne avtalen.

Tilbakelevering

Videre kan det avtales at det skal gis en utskrift og kopi av alt innhold i databaser og lignende med data som er omfattet. Kostnader ved dette, eller om opplysningene skal leveres i et særskilt format, kan også inngå i en slik avtale.

Det skal avtales at databehandler skal slette eller forsvarlig destruere alle dokumenter, data, disketter, cd-er mv, som inneholder opplysninger som omfattes av avtalen. Dette gjelder også for eventuelle sikkerhetskopier.

Avtalen bør spesifisere på hvilken måte sletting og/eller destruksjon skal skje etter avtalens opphør.

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

9. Meddelelser

Meddelelser etter denne avtalen skal sendes skriftlig til: _____

10. Lovvalg og verneting

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

Valg av verneting kan avtales

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

Sted og dato

Behandlingsansvarlig

Databehandler

.....

(underskrift)

.....

(underskrift)

Vedlegg B: Avtaleskisse – databehandleravtale etter helseregisterloven (NB – gjelder i hovedsak helse/forskning)

Databehandleravtale

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

mellom

.....
databehandlingsansvarlig

og

.....
databehandler

1. 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.

Avtalen regulerer databehandlers bruk av personopplysninger på vegne av den databehandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse.

2. Formål

Her skal det redegjøres for formålet med databehandleravtalen. Herunder:

- hvilke personopplysninger som skal behandles
- hvilke behandlinger som omfattes av avtalen
- hva som er rammene for databehandlers håndtering av personopplysninger

3. Databehandlers plikter

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

Databehandler plikter å gi databehandlingsansvarlig tilgang til sin sikkerhetsdokumentasjon, og bistå, slik at databehandlingsansvarlig kan ivareta sitt eget ansvar etter lov og forskrift.

Databehandlingsansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i personopplysningene som behandles og systemene som benyttes til dette formål. Databehandler plikter å gi nødvendig bistand til dette.

Databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til iht. denne avtalen. Denne bestemmelsen gjelder også etter avtalens opphør.

4. 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.

Avtale med underleverandører

En slik avtale bør gjøres som et tillegg til denne avtalen.

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.

5. 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.

6. Sikkerhetsrevisjoner

Databehandlingsansvarlig skal avtale med databehandler at det gjennomføres sikkerhetsrevisjoner jevnlig for systemer og lignende som omfattes av denne avtalen.

Revisjon

Revisjonen kan omfatte gjennomgang av rutiner, stikkprøvekontroller, mer omfattende stedlige kontroller og andre egnede kontrolltiltak.

7. Avtalens varighet

Avtalen gjelder så lenge databehandler behandler personopplysninger på vegne av databehandlingsansvarlig.

eller

avtalen gjelder til _____

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

Avtalen kan sies opp av begge parter med en gjensidig frist på _____, jf. punkt 8 i denne avtalen.

8. Ved opphør

Ved opphør av denne avtalen plikter databehandler å tilbakelevere alle personopplysninger som er mottatt på vegne av den databehandlingsansvarlige og som omfattes av denne avtalen.

Tilbakelevering

Videre kan det avtales at det skal gis en utskrift og kopi av alt innhold i databaser og lignende med data som er omfattet. Kostnader ved dette, eller om opplysningene skal leveres i et særskilt format, kan også inngå i en slik avtale.

Det skal avtales at databehandler skal slette eller forsvarlig destruere alle dokumenter, data, disketter, cd-er mv, som inneholder opplysninger som omfattes av avtalen. Dette gjelder også for eventuelle sikkerhetskopier.

Avtalen bør spesifisere på hvilken måte sletting og/eller destruksjon skal skje etter avtalens opphør.

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

9. Meddelelser

Meddelelser etter denne avtalen skal sendes skriftlig til: _____

10. Lovvalg og verneting

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

Valg av verneting kan avtales

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

Sted og dato

Databehandlingsansvarlig

Databehandler

.....

(underskrift)

.....

(underskrift)

Datatilsynet

Gateadresse: Tollbugata 3, Oslo

*Postadresse: postboks 8177, dep
0034 Oslo*

E-post: postkasse@datatilsynet.no

Telefon: 22 39 69 00

Faks: 22 42 23 50

Forsidefoto: Linda Cartridge