Datatilsynet

Veileder

Databehandleravtale

Forholdet mellom en behandlingsansvarlig virksomhet og databehandleren skal være regulert i en databehandleravtale.

Innhold

Hva er en databehandleravtale?

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

Hvis en virksomhet setter ut hele eller deler av behandlingen av personopplysninger til andre virksomheter, er den eller de som behandler opplysningene definert som databehandlere. En databehandler kan ikke behandle personopplysninger på en annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. Den behandlingsansvarlige skal forsikre seg om at databehandleren har tilstrekkelig sikkerhetsnivå, jf. personopplysningsloven § 15.

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.

Definisjoner

Behandlingsansvarlig er den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Behandlingsansvarlig har ansvaret for at opplysninger behandles i tråd med personopplysningslovens krav.

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

En **databehandler** er den som behandler personopplysninger på vegne av den behandlingsansvarlige. Databehandleren har et selvstendig ansvar for å ha tilfredsstillende informasjonssikkerhet, for å verne personopplysningene som behandles på vegne av behandlingsansvarlige. Databehandleren skal bare behandle personopplysninger i tråd med det som er avtalt med den behandlingsansvarlige.

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

Eksterne lenker

- Om behandlingsansvarlig og databehandler
  Personopplysningsloven § 4
  [https://lovdata.no/lov/2000-04-14-31/§2]
- Om databehandleravtale
  Personopplysningsloven § 13
  [https://lovdata.no/lov/2000-04-14-31/§13]
- Personopplysningsloven § 15
  [https://lovdata.no/lov/2000-04-14-31/§15]

Publisert: 13.06.2017

God informasjonssikkerhet - en veileder i internkontroll

Med god internkontroll og et bevisst forhold til å sikre opplysninger sørger virksomheten for at den behandler personopplysninger lovlig, sikkert og forsvarlig.

- Gå til veilederen
  [/regelverk-og-skjema/veiledere/internkontroll_informasjonssikkerhet/]

Behandlingsansvarlig eller databehandler?

Hvem har behandlingsansvaret, og hvem er databehandleren? Vi har laget noen eksempler.

Eksempel 1

Når en kommune eller bedrift kjøper datalagringstjenester hos noen som tilbyr dette, og det skal lagres blant annet personopplysninger, må en databehandleravtale være på plass. Kommunen eller bedriften er dermed den **behandlingsansvarlige** part, mens tjenesteleverandøren er **databehandler** på vegne av kommunen/bedriften. Det kan være en leverandør av lønn- og personalsystemer hvor dataserveren er plassert hos leverandøren, som i tillegg drifter løsningen for kommunen eller bedriften.

Eksempel 2

Folkehelseinstituttet er **databehandler** for en rekke virksomheter i forbindelse med rustesting: Politi og domstoler, Kriminalomsorgen og landets kommuner (barnevern, LAR), og en rekke ulike arbeidsgivere. Folkehelseinstituttet har med andre ord databehandleravtaler med hver enkelt **behandlingsansvarlige** virksomhet de behandler data på vegne av.

Eksempel 3

Et helseforetak som for eksempel Oslo Universitetssykehus har en rekke forskjellige databehandleravtaler med ulike tjenesteleverandører. Utformingen av avtalene vil variere. Den vil være avhengig av formålet med behandlingen av personopplysninger (for eksempel forskning), om dataene er sensitive eller ikke-sensitive, og av om data skal behandles innenfor eller utenfor landegrensene.

Publisert: 13.06.2017

Kravene til avtalen

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.

Databehandleravtalen må

1. Angi formålet med behandlingen

Det skal gå klart frem 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.

Konkrete rutiner for bruk av personopplysningene Databehandler har ikke råderett over personopplysningene, og kan dermed heller ikke behandle disse til egne formål.

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.

[#Underleverandor]

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 registrertes 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
- retting og sletting, se personopplysningslovens § 27 og § 28

5. Pålegge databehandleren tilfredsstillende informasjonssikkerhet

Det fremkommer av personopplysningslovens § 13 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

1. konfidensialitet – hindre uvedkommende i å få tilgang på opplysningene
2. integritet – hindre uautorisert eller utilsiktet endring av opplysninger
3. tilgjengelighet – at opplysningene er tilgjengelige når tilgang er nødvendig

Avtalen bør inneholde bestemmelser om kravene i personopplysningsforskriften kapittel 2.

- avvikshåndtering
- 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
- taushetsplikt
- sikkerhetsrevisjoner
- fysiske sikringstiltak
- hvordan rutiner og lignende skal dokumenteres
- personell hos partene som skal ha tilgang til personopplysningene

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

6. Avtalens varighet må avtales

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

Eksterne lenker

- lovdata.no
  Personopplysningsforskriften kap. 2
  [https://lovdata.no/dokument/SF/forskrift/2000-12-15-1265/KAPITTEL_2#KAPITTEL_2]

Publisert: 13.06.2017

Maler for databehandleravtale

Disse malene kan lastes ned og benyttes ved bruk av underleverandører.

Bokmål:

Last ned mal – databehandleravtale etter personopplysningsloven (bokmål, doc)
[/globalassets/global/regelverk-skjema/veiledere/avtaleskisse_personopplysningsloven_20090526.docx]

Last ned mal – databehandleravtale etter personopplysningsloven(bokmål, odt)
[/globalassets/global/regelverk-skjema/veiledere/avtaleskisse-personopplysningsloven-20090526.odt]

Nynorsk:

Last ned mal – databehandleravtale etter personopplysningsloven (nynorsk, doc)
[/globalassets/global/regelverk-skjema/veiledere/databehandlaravtale_mal_nn.docx]

Last ned mal – databehandleravtale etter personopplysningsloven (nynorsk, odt)
[/globalassets/global/regelverk-skjema/veiledere/databehandlaravtale-mal-nn-odt.odt]

Publisert: 13.06.2017

God informasjonssikkerhet - en veileder i internkontroll

Med god internkontroll og et bevisst forhold til å sikre opplysninger sørger virksomheten for at den behandler personopplysninger lovlig, sikkert og forsvarlig.

- Gå til veilederen [/regelverk-og-skjema/veiledere/internkontroll_informasjonssikkerhet/]