

Mal for databehandleravtaler

Avtaleteksten må tilpasses hver enkelt tjeneste/prosjekt og tjenesteleverandør

**I henhold til gjeldende norsk personopplysningslovgivning og forordning (EU) 2016/679 av 27.
april 2016, Artikkel 28 og 29, jf. Artikkel 32-36, inngås følgende avtale**

mellom

.....

(behandlingsansvarlig)

og

.....

(databehandler)

1. Avtalens hensikt

Avtalens hensikt er å regulere rettigheter og plikter i henhold til gjeldende norsk personopplysningslovgivning og forordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, samt om oppheving av direktiv 95/46/EF.

Avtalen skal sikre at personopplysninger ikke brukes ulovlig, urettmessig eller at opplysningene behandles på måter som fører til uautorisert tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Avtalen regulerer databehandlers forvaltning av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse, i forbindelse med bruk av/behandling i (navn på tjeneste/prosjekt).

Ved motstrid skal vilkårene i denne avtalen gå foran databehandlers personvernerklæring eller vilkår i andre avtaler inngått mellom behandlingsansvarlig og databehandler i forbindelse med bruk av/behandling i (navn på tjeneste/prosjekt).

2. Formålsbegrensning

Formålet med databehandlers forvaltning av personopplysninger på vegne av behandlingsansvarlig, er (fyll inn formålet).

Personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig kan ikke brukes til andre formål uten at dette på forhånd er godkjent av behandlingsansvarlig.

Databehandler kan ikke overføre personopplysninger som omfattes av denne avtalen til samarbeidspartnere eller andre tredjeparter uten at dette på forhånd er godkjent av behandlingsansvarlig, jf. punkt 10 i denne avtalen.

3. Instrukser

Databehandler skal følge de skriftlige og dokumenterte instrukser for forvaltning av personopplysninger i (navnet på tjeneste/prosjekt) som behandlingsansvarlig har bestemt skal gjelde.

(Navn på institusjon/virksomhet) forplikter seg til å overholde alle plikter i henhold til gjeldende norsk personopplysningslovgivning som gjelder ved bruk av (navn på tjeneste/prosjekt) til behandling av personopplysninger.

Databehandler forplikter seg til å varsle behandlingsansvarlig dersom databehandler mottar instrukser fra behandlingsansvarlig som er i strid med bestemmelsene i gjeldende norsk personopplysningslovgivning.

- Kommentar: Detaljerte instrukser til databehandler kan legges ved som bilag til databehandleravtalen.

4. Opplysningstyper og registrerte

Databehandleren forvalter følgende personopplysninger på vegne av behandlingsansvarlig:

- Kommentar: Gi en kort (gjærne punktvis) oversikt over hvilke hovedtyper personopplysninger som tjenesteleverandøren (databehandleren) forvalter på vegne av institusjonen/virksomheten (behandlingsansvarlig).

- Kommentar: Gi en kort oversikt over hvilke opplysninger som databehandler registrerer og lagrer i forbindelse med bruk av tjenesten, for eksempel ved bruk av informasjonskapsler, logger og sikkerhetskopier.

Personopplysningene gjelder følgende registrerte:

- Kommentar: Gi en kort oversikt over hvem opplysningene gjelder, for eksempel studenter og ansatte ved institusjonen.

5. De registrertes rettigheter

Databehandler plikter å bistå behandlingsansvarlig ved ivaretagelse av den registrertes rettigheter i henhold til gjeldende norsk personopplysningslovgivning.

Den registrertes rettigheter inkluderer retten til informasjon om hvordan hans eller hennes personopplysninger behandles, retten til å kreve innsyn i egne personopplysninger, retten til å kreve retting eller sletting av egne personopplysninger og retten til å kreve at behandlingen av egne personopplysninger begrenses.

I den grad det er relevant, skal databehandler bistå behandlingsansvarlig med å ivareta de registrertes rett til dataportabilitet og retten til å motsette seg automatiske avgjørelser, inkludert profilering.

Databehandler er erstatningsansvarlig overfor de registrerte dersom feil eller forsømmelser hos databehandler påfører de registrerte økonomiske eller ikke-økonomiske tap som følge av at deres rettigheter eller personvern er krenket.

6. Tilfredsstillende informasjonssikkerhet

Databehandler skal iverksette tilfredsstillende tekniske, fysiske og organisatoriske sikringstiltak for å beskytte personopplysninger som omfattes av denne avtalen mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Databehandler skal dokumentere egen sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, risikovurderinger og etablerte tekniske, fysiske eller organisatoriske sikringstiltak. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

Databehandler skal etablere kontinuitets- og beredskapsplaner for effektiv håndtering av alvorlige sikkerhetshendelser. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

Databehandler skal gi egne ansatte tilstrekkelig informasjon om og opplæring i informasjonssikkerhet slik at sikkerheten til personopplysninger som behandles på vegne av behandlingsansvarlig blir ivaretatt.

- Kommentar: Her kan det være behov for å konkretisere de viktigste sikringstiltakene som databehandleren har iverksatt, eventuelt at det henvises til dokumenter eller publikasjoner som forklarer hvordan databehandleren jobber med informasjonssikkerhet og hvilke sikringstiltak som er etablert for den aktuelle tjenesten. Konkretiseringene kan tas inn i selve avtaleteksten eller i billag til avtalen.

7. Taushetsplikt

Kun ansatte hos databehandler som har tjenstlige behov for tilgang til personopplysninger som forvaltes på vegne av behandlingsansvarlig, kan gis slik tilgang. Databehandler plikter å dokumentere retningslinjer

og rutiner for tilgangsstyring. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

Ansatte hos databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til i henhold til denne avtalen. Denne bestemmelsen gjelder også etter avtalens opphør. Taushetsplikten omfatter ansatte hos tredjeparter som utfører vedlikehold (eller liknende oppgaver) av systemer, utstyr, nettverk eller bygninger som databehandler anvender for å levere tjenesten.

Norsk lov vil kunne begrense omfanget av taushetsplikten for ansatte hos databehandler og tredjeparter.

8. Tilgang til sikkerhetsdokumentasjon

Databehandler plikter på forespørsel å gi behandlingsansvarlig tilgang til all sikkerhetsdokumentasjon som er nødvendig for at behandlingsansvarlig skal kunne ivareta sine forpliktelser i henhold til gjeldende norsk personopplysningslovgivning.

Databehandler plikter på forespørsel å gi behandlingsansvarlig tilgang til annen relevant dokumentasjon som gjør det mulig for behandlingsansvarlig å vurdere om databehandler overholder vilkårene i denne avtalen.

Behandlingsansvarlig har taushetsplikt for konfidensiell sikkerhetsdokumentasjon som databehandler gjør tilgjengelig for behandlingsansvarlig.

9. Varslingsplikt ved sikkerhetsbrudd

Databehandler skal uten ugrunnet opphold varsle behandlingsansvarlig dersom personopplysninger som forvaltes på vegne av behandlingsansvarlig utsettes for sikkerhetsbrudd.

Varslet til behandlingsansvarlig skal som minimum inneholde informasjon som beskriver sikkerhetsbruddet, hvilke registrerte som er berørt av sikkerhetsbruddet, hvilke personopplysninger som er berørt av sikkerhetsbruddet, hvilke strakstiltak som er iverksatt for å håndtere sikkerhetsbruddet og hvilke forebyggende tiltak som eventuelt er etablert for å unngå liknende hendelser i fremtiden.

Behandlingsansvarlig er ansvarlig for at Datatilsynet blir varslet når dette er påkrevd.

10. Underleverandører

Databehandler plikter å inngå egne avtaler med underleverandører som regulerer underleverandørenes forvaltning av personopplysninger i forbindelse med denne avtalen.

I avtaler mellom databehandler og underleverandører skal underleverandørene pålegges å ivareta alle plikter som databehandleren selv er underlagt i henhold til denne avtalen og lovverket. Databehandler plikter å forelegge avtalene for behandlingsansvarlig på forespørsel.

Databehandler skal kontrollere at underleverandører overholder sine avtalemessige plikter, spesielt at informasjonssikkerheten er tilfredsstillende og at ansatte hos underleverandører er kjent med sine forpliktelser og oppfyller disse.

Behandlingsansvarlig godkjenner at databehandler engasjerer følgende underleverandører for å oppfylle denne avtalen:

..... (navn
på underleverandører)

Databehandler kan ikke engasjere andre underleverandører enn de som er nevnt ovenfor uten at dette på forhånd er skriftlig godkjent av behandlingsansvarlig.

Databehandler er erstatningsansvarlig overfor behandlingsansvarlig for økonomiske tap som påføres behandlingsansvarlig og som skyldes ulovlig eller urettmessig behandling av personopplysninger eller mangelfull informasjonssikkerhet hos underleverandører.

11. Overføring til land utenfor EU/EØS

- Kommentar: Personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig kan bli overført til land utenfor EU/EØS (tredjestater). Slik overføring kan skje på visse vilkår og reglene om overføring til tredjestater finnes i Artikkel 45-47 og 49 i EUs personvernforordning. Disse reglene innebærer blant annet at overføringen vil være lovlig dersom den skjer til EU-godkjente tredjestater, til bedrifter som har sluttet seg til Privacy Shield-ordningen eller på grunnlag av EUs standardkontrakter for overføring av personopplysninger til databehandlere i tredjestater. Reglene gjelder også for sikkerhetskopiering og annen overføring av personopplysninger som skjer i forbindelse med administrasjon av den aktuelle tjenesten, for eksempel support.

Personopplysninger som databehandler forvalter i henhold til denne avtalen, vil bli overført til følgende mottakerland utenfor EU/EØS:

..... (navn på mottakerland)

Det rettslige grunnlaget for overføring av personopplysninger til de nevnte mottakerland utenfor EU/EØS er:

..... (kort redegjørelse for overføringsgrunnlaget)

12. Sikkerhetsrevisjoner og konsekvensutredninger

Databehandler skal jevnlig gjennomføre sikkerhetsrevisjoner av eget arbeid med sikring av personopplysninger mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utligningselighet.

Sikkerhetsrevisjoner skal omfatte databehandlers sikkerhetsmål og sikkerhetsstrategi, sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, etablerte tekniske, fysiske og organisatoriske sikringstiltak og arbeidet med informasjonssikkerhet hos underleverandører til denne avtalen. Det skal i tillegg omfatte rutiner for varsling av behandlingsansvarlig ved sikkerhetsbrudd og rutiner for testing av beredskaps- og kontinuitetsplaner.

Databehandler skal dokumentere sikkerhetsrevisjonene. Behandlingsansvarlig skal gis tilgang til revisjonsrapportene på forespørsel.

Dersom en uavhengig tredjepart gjennomfører sikkerhetsrevisjoner hos databehandler, skal behandlingsansvarlig informeres om hvilken revisor som benyttes og få tilgang til oppsummeringer av revisjonsrapportene på forespørsel.

Evt. tillegg: Partene kan avtale at behandlingsansvarlig selv, eller en uavhengig tredjepart som behandlingsansvarlig selv velger, utfører sikkerhetsrevisjoner hos databehandleren, eventuelt også hvordan kostnader som påløper i forbindelse med slike revisjoner skal fordeles.

13. Tilbakelevering og sletting

Ved opphør av denne avtalen plikter databehandler å tilbakelevere og slette alle personopplysninger som forvaltes på vegne av behandlingsansvarlig i henhold til denne avtalen. Behandlingsansvarlig bestemmer hvordan tilbakelevering av personopplysningene skal skje, herunder hvilket format som skal benyttes.

Sletting skal skje ved at databehandler sletter personopplysninger innen (fyll inn antall) dager etter avtalens opphør. Dette gjelder også for sikkerhetskopier av personopplysningene.

Databehandler skal dokumentere at sletting av personopplysninger er foretatt i henhold til denne avtalen. Dokumentasjonen skal gjøres tilgjengelig for behandlingsansvarlig på forespørsel.

Databehandler dekker alle kostnader i forbindelse med tilbakelevering og sletting av de personopplysninger som omfattes av denne avtalen.

14. Mislighold

Ved mislighold av vilkårene i denne avtalen som skyldes feil eller forsømmelser fra databehandlers side, kan behandlingsansvarlig si opp avtalen med øyeblikkelig virkning. Databehandler vil fortsatt være pliktig til å tilbakelevere og slette personopplysninger som forvaltes på vegne av behandlingsansvarlig i henhold til bestemmelsene i punkt 13 ovenfor.

Behandlingsansvarlig kan kreve erstatning for økonomiske tap som feil eller forsømmelser fra databehandlers side, inkludert mislighold av vilkårene i denne avtalen, har påført behandlingsansvarlig, jf. også punkt 5 og 10 ovenfor.

15. Avtalens varighet

Denne avtalen gjelder så lenge databehandler forvalter personopplysninger på vegne av behandlingsansvarlig

eller

avtalen gjelder til _____.

Avtalen kan sies opp av begge parter med en gjensidig frist på _____.

16. Kontaktpersoner

Kontaktperson hos databehandler for spørsmål knyttet til denne avtalen er: _____.

Kontaktperson hos behandlingsansvarlig for spørsmål knyttet til denne avtalen er: _____.

[Stryk det alternativet nedenfor – 17a eller 17b – som ikke passer]

17a. Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar (fyll inn navn på tingrett) som vernetting. Dette gjelder også etter opphør av avtalen.

- Kommentar: Dette punktet gjelder når databehandler er en privat aktør.

17b. Lovvalg og tvisteløsning

Partenes rettigheter og plikter etter denne avtalen bestemmes i sin helhet av norsk rett. Eventuelle tvister som springer ut av denne avtalen skal først søkes løst gjennom forhandlinger.

Dersom partene ikke oppnår enighet gjennom forhandlinger, skal tvisten løses med bindende virkning av Kunnskapsdepartementet. Hver av partene kan forlange at tvisten oversendes departementet.

- Kommentar: Dette punktet gjelder når databehandler er et annet statlig universitet eller høyskole.

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

Sted og dato

På vegne av behandlingsansvarlig

På vegne av databehandler

.....

(underskrift)

.....

(underskrift)