

Merk: Grå felter i malen skal fylles ut av partene. Tekst markert med gult er eksempler eller veiledning, og skal fjernes før ferdigstillelse og signering.

Databehandleravtale

mellom

Statens pensjonskasse

Org.nr.: 982583462

(heretter kalt "Behandlingsansvarlig")

og

.....

Org.nr.: xxxxxxxx

(heretter kalt "Databehandler")

1 Bakgrunn og formål

Statens pensjonskasse (heretter kalt Behandlingsansvarlig) og [Leverandørens navn] (heretter kalt Databehandler), har [xx.xx.20xx] signert en avtale om leveranse av [kort beskrivelse av hva leveransen går ut på] til Behandlingsansvarlig, heretter kalt «Hovedavtalen». I den forbindelse skal Databehandler behandle personopplysninger på vegne av Behandlingsansvarlig.

Databehandleravtalen regulerer rettigheter og plikter etter General Data Protection Regulation 2016/679/EC (personvernforordningen) og lov om behandling av personopplysninger (personopplysningsloven) som gjennomfører EUs personvernforordning i Norge, gjeldende fra 20.07.2018. Avtalen er utformet med henblikk på partenes etterlevelse av personvernforordningens artikkel 28 nr. 3, som stiller spesifikke krav til innholdet i en databehandleravtale.

Formålet med denne databehandleravtalen er å sikre at personopplysninger behandles i overensstemmelse med personvernforordningen og personopplysningsloven, og ikke brukes urettmessig eller kommer uberettigede i hende. Avtalen fastsetter vilkår for behandlingen av personopplysninger som Databehandler utfører på vegne av Behandlingsansvarlig.

Til denne avtalen hører tre bilag. Bilagene fungerer som en integrert del av databehandleravtalen.

- Bilag A inneholder nærmere opplysninger om behandlingen, herunder om behandlingens formål og karakter, typen av personopplysninger, kategoriene av registrerte og varigheten av behandlingen. Bilag A inneholder også en liste over de eventuelle underleverandører som Behandlingsansvarlig har godkjent.
- Bilag B inneholder en nærmere instruks om hvilken behandling databehandleren skal foreta på vegne av Behandlingsansvarlig (behandlingens gjenstand), hvilke sikkerhetskrav som minimum skal følges, samt eventuell instruks eller godkjennelse av overføring av personopplysninger til tredjeland.
- Bilag C inneholder partenes eventuelle regulering av forhold som ikke ellers fremgår av databehandleravtalen eller partenes hovedavtale.

Beskrivelse av Databehandlers tjenester fremgår av Hovedavtalen.

Denne databehandleravtalen frigjør ikke Databehandler fra forpliktelser som etter personvernforordningen, personopplysningsloven eller enhver annen lovgivning direkte er pålagt databehandleren.

2 Behandlingsansvarliges forpliktelser og rettigheter

Behandlingsansvarlig har ovenfor omverdenen (herunder den registrerte) som utgangspunkt ansvaret for at behandlingen av personopplysninger skjer innenfor rammene av personvernforordningen og annen lovgivning om vern av personopplysninger.

Behandlingsansvarlig har derfor både rettighetene og forpliktelsene til å treffe beslutninger om, til hvilke formål og med hvilke hjelpemidler behandlingen skal foretas.

Behandlingsansvarlig er blant annet ansvarlig for at det foreligger hjemmel til den behandling, som Databehandler instrueres til å foreta.

3 Databehandlers plikter

3.1 Generelt

Databehandleren skal kun behandle personopplysninger etter dokumentert instruks fra Behandlingsansvarlig, medmindre det kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som Databehandler er underlagt. I så fall skal Databehandler underrette Behandlingsansvarlig om nevnte rettslige krav før behandlingen foretas, med mindre denne rett av hensyn til viktige samfunnsinteresser forbyr en slik underretning, jf. art 28, nr. 3, litra a.

Databehandler skal omgående underrette Behandlingsansvarlig dersom Databehandler er av den oppfatning at instruks fra Behandlingsansvarlig er i strid med personvernforordningen, databehandleravtalen eller annen lovgivning om vern av personopplysninger.

Personopplysningene skal ikke behandles på annen måte, til annet formål eller i større grad enn det som følger av denne databehandleravtalen og eventuelle senere skriftlige avtaler mellom partene. Eventuell annen bruk av personopplysningene skal skriftlig og i forkant av behandlingen avtales særskilt med Behandlingsansvarlig. Databehandler kan ikke benytte opplysningene til egne formål.

Databehandler skal ikke utlevere data eller personopplysninger i noen form på eget initiativ. Enhver henvendelse som rettes til Databehandler fra andre enn behandlingsansvarlig om å få utskrift av rådata eller personopplysninger, skal straks videreformidles til Behandlingsansvarlig. Behandlingsansvarlig vil vurdere hvorvidt opplysninger skal utleveres i det enkelte tilfellet, og kan stille vilkår for slik utlevering.

Databehandler er underlagt plikt om protokollføring som fremgår av personvernforordningen art. 30, og skal føre skriftlig protokoll over alle kategorier av behandlingsaktiviteter som utøves på vegne av Behandlingsansvarlig.

3.2 Bistand til den behandlingsansvarlige

Databehandler skal bistå Behandlingsansvarlig med å ivareta de registrertes rettigheter fastsatt i kapittel III i personvernforordningen. Dette innebærer at Databehandler skal, i den grad det er mulig og hensyntatt behandlingens art, bistå Behandlingsansvarlig med å sikre overholdelse av blant annet:

- Informasjonsplikten ved innsamling av personopplysninger etter art. 12-14
- Retten til innsyn etter art. 15
- Retten til korrigeringer etter art. 16
- Retten til sletting («retten til å bli glemt») etter art. 17
- Retten til dataportabilitet etter art. 20

Databehandler plikter å bistå Behandlingsansvarlig med ovennevnte ved hjelp av egnede tekniske og organisatoriske tiltak.

Databehandler skal også bistå Behandlingsansvarlig med å sikre overholdelse av forpliktelser i henhold til personvernforordningen art. 32-36, hensyntatt behandlingens art og informasjonen som er tilgjengelig for Databehandler.

3.3 Krav til informasjonssikkerhet

Databehandler skal iverksette de sikkerhetstiltak som kreves i henhold til personvernforordningen artikkel 32. Databehandler skal gjennomføre nødvendige tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet i forhold til relevante risikoer ved behandlingen. Hva som er å anse som akseptabelt risikonivå avgjøres av Behandlingsansvarlig.

Ovennevnte forpliktelse innebærer at Databehandler skal foreta en risikovurdering, og gjennomføre tiltak for å imøtegå identifiserte risikoer. Det kan herunder bl.a., alt etter hva som er relevant, være tale om følgende sikkerhetstiltak:

- Pseudonymisering og kryptering av personopplysninger
- Evne til å sikre vedvarende fortrolighet, integritet, tilgjengelighet og robusthet av behandlingssystemer og – tjenester
- Evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse
- En prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er

Databehandler skal i forbindelse med ovennevnte som minimum iverksette det sikkerhetsnivået og de sikkerhetstiltak som er beskrevet nærmere i denne avtalens bilag B.

3.4 Lagring og sletting av data

Databehandler har ansvar for at personopplysningene underlegges tilstrekkelig sikkerhet ved lagring. Databehandler skal ikke lagre personopplysningene lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Hvis ikke personopplysningene deretter skal returneres Behandlingsansvarlig eller oppbevares i henhold til arkivloven eller annen lovgivning, har Databehandler ansvar for at de slettes. Tilsvarende gjelder for eventuelle kopier/ backup av personopplysningene.

Oppbevaringsperiode og sletterutine for personopplysninger som omfattes av denne avtalen er nærmere beskrevet i bilag B.

3.5 Varsel om brudd på personopplysningssikkerheten

Ved mistanke eller konstatering av brudd på personopplysningssikkerheten, skal Databehandler uten ugrunnet opphold varsle Behandlingsansvarlig. Varselet skal sendes til den kontaktperson hos Behandlingsansvarlig som er angitt under punkt 8 i denne avtalen.

Databehandler skal i varselet opplyse om følgende:

- Arten av bruddet
- Hvilke opplysningskategorier og antall registrerte personer som omfattes av bruddet
- Antatte konsekvenser av bruddet
- Hvilke umiddelbare tiltak som er igangsatt eller vurderes igangsatt

Dersom det ikke er mulig å straks gi samlet all informasjon som nevnt ovenfor, skal informasjon om at brudd mistenkes eller er konstatert gis umiddelbart, og øvrig informasjon gis fortløpende og så snart som mulig.

Behandlingsansvarlig har ansvaret for at avviksmelding sendes Datatilsynet. Databehandler skal samarbeide med Behandlingsansvarlig for å fremskaffe nødvendig informasjon i denne sammenhengen.

3.6 Bruk av underleverandør

Databehandler skal oppfylle de betingelser som stilles i personvernforordningen art. 28, nr. 2 og 4, for å gjøre bruk av en annen databehandler (underleverandør). Databehandler kan således ikke benytte underleverandør til oppfyllelse av sine plikter etter databehandleravtalen uten forutgående særskilt eller generell skriftlig samtykke fra Behandlingsansvarlig.

I tilfelle av generell skriftlig samtykke skal Databehandler underrette Behandlingsansvarlig om eventuelle planer om å benytte andre underleverandører eller skifte ut underleverandører, og dermed gi Behandlingsansvarlig mulighet for å motsette seg slike endringer.

Når Databehandler har Behandlingsansvarliges samtykke til å gjøre bruk av en underleverandør, skal Databehandler i skriftlig avtale med sin underleverandør pålegge denne de samme forpliktelsene med hensyn til vern av personopplysninger som gjelder mellom Databehandler og Behandlingsansvarlig. Databehandler er fullt ut ansvarlig for underleverandørenes brudd på forpliktelsene som følger av personvernforordningen og denne databehandleravtalen.

Databehandler skal fremlegge kopi av avtalen(e) som er inngått med underleverandør(ene) på Behandlingsansvarliges forespørsel. Slik avtale skal være inngått før behandlingen av opplysningene starter. Samtlige som på vegne av Databehandler utfører oppdrag der bruk av de aktuelle personopplysningene inngår, skal være kjent med Databehandlers avtale- og lovmessige forpliktelser, samt oppfylle vilkårene i denne databehandleravtalen og gjeldende lovgivning om vern av personopplysninger.

Behandlingsansvarliges eventuelle godkjenning av spesifikke underleverandører er oppgitt i databehandleravtalens bilag A.

3.7 Lagring og overføring til tredjeland

Databehandler må kun behandle personopplysninger etter dokumentert instruks fra Behandlingsansvarlig, herunder også hva gjelder overførsel av personopplysninger til tredjeland (land utenfor EU/EØS) eller internasjonale organisasjoner, med mindre det kreves i henhold til EU-rett eller medlemstatenes nasjonale rett, som Databehandler er underlagt. I så fall underretter Databehandler Behandlingsansvarlig om dette rettslige krav i forkant av behandling, med mindre denne rett forbyr slik underretting av hensyn til viktige samfunnsmessige interesser, jf. art 28, nr. 3, bokstav a.

Uten Behandlingsansvarliges instruks eller godkjenning kan Databehandler derfor bl.a. ikke;

- Gi videre personopplysningene til en behandlingsansvarlig i et tredjeland eller i en internasjonal organisasjon
- Overlate behandlingen av personopplysninger til en underleverandør i et tredjeland
- La personopplysningene behandles i en annen av Databehandlers avdelinger, som er plassert i et tredjeland

Behandlingsansvarliges eventuelle instruks eller godkjenning av at det foretas overførsel av personopplysninger til et tredjeland, vil fremgå av denne databehandleravtalens bilag B.

4 Taushetsplikt

Databehandler har taushetsplikt om personopplysninger som vedkommende får tilgang til i henhold til Avtalen.

Databehandler skal videreføre taushetsplikten til underleverandører og skal der det er nødvendig pålegge underleverandør å undertegne særskilte taushetserklæringer med sine ansatte.

Taushetsplikten gjelder også etter databehandleravtalens opphør.

5 Tilsyn og revisjoner

Behandlingsansvarlig har på forespørsel rett til å gjennomføre sikkerhetsrevisjoner hos Databehandler. Databehandler plikter i denne sammenheng å tilrettelegge for revisjonene og stille til rådighet alle opplysninger som er nødvendige for å påvise Databehandlers overholdelse av personvernforordningens art. 28 og denne databehandleravtalen, herunder interne revisjonsrapporter, prosedyrer, rutiner, sikkerhetsarkitektur med tiltak mm.

Revisjonene utføres av Behandlingsansvarlig selv, eller en tredjepart utpekt av Behandlingsansvarlig.

Revisjoner skal gjennomføres på en slik måte at den i minst mulig grad forstyrrer alminnelig drift og tjenesteleveranser fra Databehandler og dennes underleverandører.

6 Avtalens varighet

Databehandleravtalen gjelder fra den er signert av begge parter og løper så lenge Databehandler behandler eller har tilgang til personopplysninger på vegne av Behandlingsansvarlig, eller avtalen erstattes av en ny avtale mellom partene.

Behandlingsansvarlig kan ved brudd på denne avtalen eller på bestemmelsene i gjeldende personvernregelverk pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning. Behandlingsansvarlig kan ved vesentlige brudd si opp denne avtalen med 14 dagers varsel.

7 Ved opphør

Databehandleren skal, etter Behandlingsansvarliges valg, slette eller tilbakelevere alle personopplysninger til den Behandlingsansvarlige etter at tjenestene knyttet til behandlingen er levert, og slette eksisterende kopier, med mindre det er et lovmessig krav om at personopplysningene fortsatt skal lagres. Dette gjelder også for eventuelle sikkerhetskopier, men hvor det er tilstrekkelig å overskrive etter de etablerte rutiner for sikkerhetskopiering.

Databehandler skal skriftlig bekrefte eller dokumentere at sletting og/eller destruksjon er foretatt i henhold til nærmere avtalt tidspunkt etter avtaleforholdets opphør.

8 Meddelelser

Meddelelser etter denne avtalen skal sendes skriftlig til:

Behandlingsansvarlig	Databehandler
Navn:	Navn:
Tittel:	Tittel:
Telefon:	Telefon:
E-post:	E-post:

9 Lovvalg og verneting

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

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

Sted og dato
Oslo, xx.xx.xxxx

For Behandlingsansvarlig

.....
[Navn]

[Tittel]

For Databehandler

.....
[Navn]

[Tittel]

Bilag A Opplysninger om behandlingen av personopplysningene

Merk: Grå felter i malen skal fylles ut av partene. Tekst markert med gult er eksempler eller veiledning, og skal fjernes før ferdigstillelse og signering.

A.1 Formålet

Personopplysningene behandles for følgende formål:

- [Beskriv formålet med behandlingen].

Eksempel: "at Behandlingsansvarlig kan anvende systemet X, som eies og administreres av Databehandler, til å innsamle og behandle opplysninger om Behandlingsansvarliges medlemmer".

A.2 Behandlingens karakter

Behandlingen dreier seg primært om:

- [Beskriv karakteren av behandlingen].

Eksempel: "at Databehandler stiller systemet X til rådighet for Behandlingsansvarlig og herigjennom oppbevarer personopplysninger om Behandlingsansvarliges medlemmer på virksomhetens servere."

A.3 Kategorier av personopplysninger

Behandlingen omfatter følgende kategorier av personopplysninger:

- [Beskriv typen av personopplysninger som behandles].

Eksempel: "Navn, e-mailedresse, telefonnummer, adresse, personnummer, betalingsopplysninger, medlemsnummer, type av medlemskap."

Behandlingen omfatter også følgende sensitive personopplysninger: *Fjern avsnittet hvis ikke aktuelt*

- [Beskriv typen av sensitive personopplysninger som behandles].

Eksempel: "Etnisk opprinnelse, politiske meninger, religiøs overbevisning, fagforeningsmedlemskap, seksuell legning, helseopplysninger."

A.4 Kategorier av registrerte

Behandlingen omfatter følgende kategorier av registrerte:

- [Beskriv kategorien av registrerte].

Eksempel: "Personer som har eller har hatt medlemskap hos Behandlingsansvarlig."

A.5 Varighet

Behandlingen skal ha følgende varighet:

- [Beskriv varighet av behandlingen].

Eksempel: "Behandlingen er ikke tidsbegrenset og varer inntil Hovedavtalen sies opp."

A.6 Godkjennelse av underleverandører

Behandlingsansvarlig har ved databehandleravtalens ikrafttredelse godkjent anvendelsen av følgende underleverandører:

Navn	Org.nr.	Adresse	Beskrivelse av behandling
[Navn]	[Org.nr]	[Adresse]	[Overordnet beskrivelse av behandlingen hos underleverandør]
[Navn]	[Org.nr]	[Adresse]	[Overordnet beskrivelse av behandlingen hos underleverandør]
[Navn]	[Org.nr]	[Adresse]	[Overordnet beskrivelse av behandlingen hos underleverandør]

Databehandler kan ikke – uten Behandlingsansvarliges særskilte og skriftlige samtykke – anvende den enkelte underleverandør til en annen behandling enn avtalt eller la en annen underleverandør foreta den beskrevne behandling.

Bilag B Instruks vedrørende behandling av personopplysninger

B.1 Behandlingens gjenstand/ instruks

Databehandlers behandling av personopplysninger på vegne av Behandlingsansvarlig skjer ved at Databehandler utfører følgende:

- [Beskriv behandlingen som Databehandler skal foreta, eller henvis eventuelt til konkrete avsnitt i Hovedavtalen.]

B.2 Krav til informasjonssikkerhet

Databehandler er berettiget og forpliktet til å treffe beslutninger om hvilke tekniske og organisatoriske sikkerhetstiltak som skal anvendes for å skape det nødvendige sikkerhetsnivå omkring personopplysningene.

Databehandleren skal dog – i alle tilfelle og som minimum – gjennomføre følgende tiltak, som er avtalt med Behandlingsansvarlig:

Merk: Kravene nedenfor er kun eksempler. Kravene må tilpasses Databehandlers spesifikke leveranse/oppdrag. Kravene trenger ikke stå i tabell – det viktigste er at de fremkommer tydelig. Viktig at disse kravene også inntas i kravspesifikasjonen ved anskaffelse av tjenesteleveransen.

- **Isolasjon:** Databehandler skal sikre at personopplysninger tilgjengeliggjort av Behandlingsansvarlig holdes atskilt fra egne og andre kunders personopplysninger.
- **Kryptering ved lagring:** Databehandler skal sørge for kryptering ved lagring til disk og til backup/arkiv, for å ivareta konfidensialitet og integritet. TLS-kryptering skal brukes ved sending av e-post.
- **Begrensning av tilgang til data:** Databehandler skal sikre at antall medarbeidere med tilgang til Behandlingsansvarliges personopplysninger begrenses til de som har behov for tilgang begrunnet i sin stilling. Tilganger som ikke lenger er nødvendige skal slettes.
- **Sletting og lagringstid:** Databehandler skal ha rutiner for sletting. Rutiner skal omfatte sletting av logger og data, enten etablering av funksjonalitet for automatisk sletting, markere data som slettet, eller tilrettelegging for manuell sletting.
- **Autentisering i admingrensesnitt:** 2-faktor autentisering og/eller SSO (for eksempel SAML og OpenID) for administrasjonsgrensesnittene skal benyttes.
- **Krav til passord:** Databehandler skal ha etablert passordpolicy.

B.3 Oppbevaringsperiode/sletterutine

Oppbevaringsperiode og sletterutine for personopplysninger som omfattes av denne avtalen er som følger:

- [Angi eventuell oppbevaringsperiode/sletterutine for Databehandler]

Eksempel:"

Personopplysningene oppbevares i [angi tidsperiode eller hendelse], hvorefter de slettes hos Databehandler."

eller

"Personopplysningene oppbevares hos Databehandler, inntil Behandlingsansvarlig anmoder om å få opplysningene slettet eller tilbakelevert".

B.4 Instruks eller godkjenning vedrørende overføring av personopplysninger til tredjeland

[Beskriv en eventuell instruks eller godkjenning vedrørende overføring av personopplysninger til et tredjeland]

[Anfør overførselsgrunnlag etter personvernforordningens kapittel 5]

Hvis Behandlingsansvarlig ikke i dette avsnittet eller ved en etterfølgende skriftlig meddelelse har angitt en instruks eller godkjenning vedrørende overføring av personopplysninger til et tredjeland, må Databehandler ikke innenfor rammene av denne databehandleravtalen foreta en slik overføring. **Fjern avsnittet hvis instruks eller godkjenning er gitt**

Bilag C Partenes regulering av andre forhold

C.1 [Overskrift]

C.2 [Overskrift]

C.3 [Overskrift]

C.4 [Overskrift]