

BILAG TIL AVTALE OM FELLES BEHANDLINGSANSVAR

DETTE DOKUMENT BESTÅR AV FØLGENDE BILAG:

BILAG A – OPPLYSNINGER OM BEHANDLINGEN

BILAG B - BETINGELSER FOR DATABEHANDLERENS BRUK AV UNDERDATABEHANDLERE

BILAG C - INSTRUKS VEDRØRENDE BEHANDLING AV PERSONOPPLYSNINGER

BILAG D - ENDRINGER ETTER AVTALEINNGÅELEN

Bilag A, B, C, og D til Avtale om felles behandlingsansvar

A.	Opplysninger om behandlingen	3
A.1	Generelle leveringsvilkår og formålet med behandlingen av personopplysninger ...	3
A.2	Behandling av pensjonsopplysninger på Portalen	4
A.3	Typer av personopplysninger	6
A.4	Kategorier av registrerte	6
A.5	Varighet av behandlingen	6
B.	Betingelser for bruk av databehandler og endring av eventuelle databehandlere.....	6
B.1	Partenes godkjenning av bruk av databehandlere	7
B.2	Godkjente Databehandlere og underdatabehandlere	7
C.	Instruks vedrørende behandling av personopplysninger	9
C.1	Behandlingens omfang og formål	9
C.2	Sikkerhet ved behandlingen.....	9
C.2.1	Angivelse av sikkerhetsnivå.....	9
C.2.2	Styringssystem for informasjonssikkerhet	9
C.3	Dokumentasjon	11
C.4	Overføring av personopplysninger - Lokasjon for behandling og tilgang.....	11
C.5	Rutiner for revisjon og tilsyn	11
C.6	Sletting og tilbakelevering av personopplysninger ved Behandlingsavtalens opphør 12	
C.7	Kontaktinformasjon.....	12

A. OPPLYSNINGER OM BEHANDLINGEN

A.1 Generelle leveringsvilkår og formålet med behandlingen av personopplysninger

Partenes felles behandlinger beskrives her.

Behandlingen har følgende formål:

Tjeneste	Formål	Behandlingsgrunnlag
Basistjenesten	Gjøre pensjonsopplysninger tilgjengelig for fysiske personer i Norsk Pensjon sin portal på www.norskpensjon.no samt i oversikt og pensjonskalkulatorer hos den enkelte pensjonsinnretning	Samtykke fra fysisk person
Uføresamordning	Tjeneste for sikker utveksling av data mellom pensjonsinnretninger som gir den enkelte pensjonsinnretning nødvendig datagrunnlag for samordning av uførepensjon etter tjenestepensjonsloven §8-7 annet ledd	Tjenestepensjonsloven § 8-7 annet ledd
Svartjeneste for personer som ikke kan logge inn samt oversikt til etterlatte	Forsikringstakere, etterlatte og verger kan henvende seg til Norsk Pensjon for å få informasjon om hvor vedkommende selv eller avdøde har en forsikring eller en pensjonsavtale.	Berettiget innsikt, fullmakt
Integrasjon med Statistisk sentralbyrå (SSB)	Norsk Pensjon sin tjeneste for å gi statistikkgrunnlag til SSB, der oppgaveplikten til pensjonsinnretningene kan gjennomføres automatisk via Norsk Pensjon.	Statistikkloven/ avtale (leveranseavtale for tjenester hos Norsk Pensjon)
Utlevering av pensjonstallet	Data om opptjening og prognose for pensjon kan også leveres via Pensjonsinnretningens egen pensjonskalkulator, gjennom andre pensjonsinnretningers	Samtykke fra fysisk person

	kalkulatorer samt gjennom NAV. Formålet er at Kundene skal kunne få en pensjonsoversikt der de befinner seg. Tjenesten inneholder informasjon om alle rettigheter og prognoser for private og offentlige pensjonsordninger.	
Levering til digitalt dødsbo	Norsk Pensjon utleverer på vegne av pensjonsinnretningene avtaler som skal gjøres tilgjengelig i Digitalt dødsbo driftet av Digdir	Hjemmel for utlevering av Opplysningene er arveloven § 88a fjerde ledd og forskrift om Digitalt dødsbo §§ 3 og 4 Det utleveres ikke personopplysninger via tjenesten. Opplysningene som utleveres gjelder døde personer.

A.2 Behandling av pensjonsopplysninger på Portalen

De Behandlingsansvarliges behandlinger omhandler (karakteren av behandlingen):

Tjeneste	Behandling av personopplysninger
Basistjenesten	Tjenesten henter opplysninger fra relevante pensjonsinnretninger og sammenstiller disse i pensjonsoversikten i pensjonsportalen. Videre innhentes og beregnes pensjon i pensjonskalkulatoren. For detaljerte opplysninger om hvilke data som innhentes vises til tjenestebeskrivelsen på samarbeidsportalen.
Uføresamordning	Norsk Pensjon har gjort tilgjengelig funksjonalitet via en applikasjon hos Norsk Pensjon som gjør det mulig for Pensjonsinnretningene å utveksle informasjon om utføret rettigheter. For detaljerte opplysninger om hvilke data som innhentes vises til tjenestebeskrivelsen på samarbeidsportalen.
Svartjeneste for personer som ikke kan logge inn samt oversikt til etterlatte	Tjenesten gjør det mulig for fysiske personer å henvende seg til Norsk Pensjon for å få utgitt opplysninger om pensjoner eller forsikringer. Norsk Pensjon lager på forespørsel en sammenstilling av tilgjengelig informasjon som sendes

Bilag A, B, C, og D til Avtale om felles behandlingsansvar

	tilbake til den fysiske personen, enten via e-post eller pr brev. For detaljerte opplysninger om hvilke data om innhentes vises til tjenestebeskrivelsen på samarbeidsportalen.
Integrasjon med Statistisk sentralbyrå (SSB)	På vegne av Pensjonsinnretningen henter Norsk Pensjon inn data ihht spesifikasjon fra Pensjonsinnretningen og oversender dette på sikker måte til SSB. For detaljerte opplysninger om hvilke data om innhentes vises til tjenestebeskrivelsen på samarbeidsportalen.
Utlevering av pensjonstallet	På forespørsel fra fysisk person hos Pensjonsinnretning, henter Norsk Pensjon inn data fra alle Pensjonsinnretningene med avtale med Norsk Pensjon og sammenstiller disse i en egen tjeneste. Den fysiske personen hos pensjonsinnretningen som har forespurt dataene får tilbake en oversikt over pensjonsavtaler og eventuelle prognoser som de kan benytte i sine nettløsninger. For detaljerte opplysninger om hvilke data om innhentes vises til tjenestebeskrivelsen på samarbeidsportalen.

A.3 **Typers av personopplysninger**

Behandlingen omfatter følgende typer av personopplysninger om de registrerte (flere valg mulig):

☐	<i>Særlige kategorier av personopplysninger i henhold til GDPR artikkel 9 (1):</i>
☒	<i>Andre opplysninger med særlig behov for beskyttelse: I tjenestene: Basistjenesten, Uføresamordning, Svartjeneste, Integrasjon med SSB og utlevering av pensjonstallet oppgis fødselsnummer og opplysninger om pensjonsrettigheter</i>
☒	<i>Andre personopplysninger: I alle tjenestene til Norsk Pensjon utveksles informasjon om navn</i>

A.4 **Kategorier av registrerte**

Behandlingen omfatter følgende kategorier av registrerte:

Fysiske personer med opptjente pensjonsrettigheter i Norge.

A.5 **Varighet av behandlingen**

Behandling av personopplysninger under Avtale om Felles Behandlingsansvar (Behandlingsavtalen) kan påbegynne når den har tredd i kraft. Behandlingen har følgende varighet (velg ett alternativ):

☒	Behandlingen er ikke tidsbegrenset, og varer frem til opphør av Behandlingsavtalen
☐	Behandlingen er tidsbegrenset, og gjelder frem til

Ved opphør (av avtalen eller en behandling) skal personopplysninger tilbakeleveres og slettes i samsvar med Behandlingsavtalens punkt 12 og instruksjonene i Bilag C.

B. BETINGELSER FOR BRUK AV DATABEHANDLER OG ENDRING AV EVENTUELLE DATABEHANDLERE

B.1 Partenes godkjenning av bruk av databehandlere

Ved inngåelse av Behandlingsavtalen godkjenner Partene bruk av de databehandlere som er oppført i punkt B.2.

For endringer i bruk av databehandlere er det i tillegg avtalt følgende:

☐	Databehandleren kan benytte Underdatabehandler som i samme konsern (mor-søster- eller datterselskap) som er etablert i et land innenfor EØS-området. Databehandleren skal på forhånd informere Behandlingsansvarlige om bruken av slik Underdatabehandler. (Dette alternativet kan kombineres med et av de andre alternativene.)
☒	NORSK PENSJON kan gjennomføre endringer i bruken av databehandlere forutsatt at PENSJONSINNRETNINGENE underrettes og gis mulighet til å motsette seg endringene. En slik underretning skal være mottatt av pensjonsinnretningen senest 1 måned før endringen trer i kraft, med mindre annet er avtalt skriftlig mellom Partene. Merk at endringer som medfører overføring av personopplysninger til land utenfor EØS-området (Tredjestater) uansett krever skriftlig godkjenning etter Behandlingsavtalens punkt 10. Hvis en av Partene motsetter seg endringen skal NORSK PENSJON underrettes så snart som mulig. En Part kan ikke motsette seg endringen uten saklig grunn.
☐	NORSK PENSJON kan kun gjennomføre endringer i bruken av Databehandlere etter spesifikk og forutgående skriftlig godkjenning fra PENSJONSINNRETNINGENE. Databehandleren kan ikke behandle personopplysninger under Generelle leveringsvilkår før slik godkjenning er gitt. Godkjenning kan ikke nektes uten saklig grunn.

B.2 Godkjente Databehandlere og underdatabehandlere

	Navn	Org.nr.	Adresse	Beskrivelse av behandling	Behandlings-sted	Kontaktinformasjon	Særlige kategorier personopplysninger
Databehandlere	Kantega	985 815 534	Kirkegata 5, 0153 Oslo	Kantega er leverandør av videreutvikling, forvaltning og drift av Norsk Pensjons IT-løsninger som behandler personopplysninger.	Norge	NorskPensjon@kantega.no Hans.Ove.Ringstad@kantega.no +47 922 42 560	
Databehandlere	Finans Norge Forsikringsdrift	999 523 625	Hanstensgt 2, 0253 OSLO	Finans Norge Forsikringsdrift administrerer, drifter og videreutvikler Norsk Pensjon sine løsninger på vegne av Norsk Pensjon AS	Norge	trond.torstad@finansnorge.no	
Underdatabehandlere	Basefarm AS	982 211 743	Nydalen allé 37A, 0484 Oslo	Basefarm er Kantegas underleverandør på drift, og leverer tjenester som datasenter, servere, driftsplattform, nettverk, brannmur, Intrusion Detection System (IDS), backup, driftsovervåkning, o.l.	Norge	support@basefarm.com +47 4000 4100	

Bilag A, B, C, og D til Avtale om felles behandlingsansvar

NORSK PENSJON kan ikke bruke den enkelte databehandleren til en annen behandling enn avtalt eller la en annen databehandler utføre den beskrevne behandlingen i andre tilfeller enn det som følger av Bilag B, punkt B.1 om skifte av databehandler.

C. INSTRUKS VEDRØRENDE BEHANDLING AV PERSONOPPLYSNINGER

C.1 Behandlingens omfang og formål

Personopplysningene skal utelukkende behandles i det omfang og for de formål som er beskrevet i

- Generelle leveringsvilkår og
- Denne Behandlingsavtalen

Partene har ikke råderett over personopplysningene utover det som er nødvendig for å oppfylle sine plikter etter Behandlingsavtalen, og kan ikke behandle disse til egne formål.

C.2 Sikkerhet ved behandlingen

C.2.1 Angivelse av sikkerhetsnivå

Ut fra en vurdering av omfanget av personopplysninger som blir behandlet, typen opplysninger og karakteren av behandlingen er det basert på en konkret risikovurdering fastsatt at behandlingen (velg ett alternativ):

☒ Krever et høyt sikkerhetsnivå. Begrunnelse:

Videre inneholder tjenestene opplysninger om en fysisk person sine opptjente pensjonsrettigheter.

Det er viktig at informasjonen som utveksles har høy grad av konfidensialitet og integritet. Dataene som utveksles skal ha en høy grad av tilgjengelighet, det vil si at mye informasjon er gjort tilgjengelig via løsninger på internett.

☐ Ikke krever et høyt sikkerhetsnivå. Begrunnelse:

<Vis til risikovurderingen som er gjort og skriv begrunnelse>

< F.eks.: Behandlingen omfatter bare opplysninger som er allment kjent som navn og adresse>

C.2.2 Styringssystem for informasjonssikkerhet

Bilag A, B, C, og D til Avtale om felles behandlingsansvar

Partene skal sørge for at databehandleren skal ha et egnet styringssystem for informasjonssikkerhet. Databehandleren skal etablere og forvalte tilstrekkelige sikkerhetstiltak for å ivareta informasjonssikkerheten for behandling av personopplysningene, herunder (flere valg mulig):

☐	Sikkerhetskrav som beskrevet i Hovedavtalen: <sett inn henvisning til konkret regulering i Hovedavtalen>
☒	Sikkerhetskrav som beskrevet nedenfor: <i>Partene skal vurdere risikoene for fysiske personers rettigheter og friheter som behandlingen utgjør og gjennomføre tiltak for å imøtegå disse risikoene. Tiltakene skal omfatte:</i> a. Krav til pseudonymisering og kryptering av personopplysninger Testdata skal være syntetiske. Personopplysninger som overføres via webtjenester krypteres på transportlaget med HTTPS. Personopplysninger som samles for Statistisk sentralbyrå (SSB) krypteres før de overføres til SSB. Øvrig kryptering vurderes i samråd med Norsk Pensjon. For mer detaljert informasjon vises til integrasjonsguider for de enkelte tjenestene. b. Krav stilt for å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene Data oppbevares fysisk sikkert i datasenter levert av underleverandør ihht bilag B. Underleverandøren er sertifisert i henhold til ISO 27001. Overføring av data gjøres på sikker måte ved å følge god praksis for dette. Kun personer som er involvert i drift og forvaltning av Norsk Pensjons systemer har tilgang til systemene og dataene. Tilgang skal skje på sikker måte, og følge rutiner som er spesifisert for det. Underleverandører skal ha en policy for bruk av hjemmekontor. Alle som har tilgang til Norsk Pensjons systemer og data skal ha signert taushetsplikt og ha gjennomført opplæring i sikkerhet eller fra før ha kompetanse på sikkerhet. Det gjøres backup av data regelmessig slik at de skal kunne gjenopprettes fra siste backup. Driftssystemer skal ha nødvendig redundans og tilgjengelighet. Autentisering av sluttbrukere gjøres med ID-porten, single sign-on eller andre metoder metoder som oppfyller kravene i selvdeklarasjonsforskriften og med nivå «betydelig» eller høyere.

	Løsningen logger ikke personopplysninger. c. Krav til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse Data skal kunne gjenopprettes fra siste backup. Applikasjoner skal kunne bygges og deployes på nytt. Driftsmiljø skal kunne gjenopprettes fra backup eller lages på nytt. Testing av evnen til å gjenopprette bestilles av Norsk Pensjon. d. Krav til prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er. Norsk Pensjon bestiller regelmessig en sikkerhetsgjennomgang av løsningene fra 3. parts ekspert, og det er underleverandørens ansvar å bistå i dette arbeidet. Det er Norsk Pensjon som bestemmer omfang og frekvens av sikkerhetsgjennomgangene. Underleverandør skal ha en prosess for å regelmessig kontrollere egne tiltak for å sikre personopplysningssikkerheten.
--	---

C.3 Dokumentasjon

Databehandler skal dokumentere de rutiner og tiltak som er iverksatt for å oppfylle kravene som fremkommer av Gjeldende personvernregler og Databehandleravtalen, herunder kravene til informasjonssikkerhet. Slik dokumentasjon skal oppbevares og ajourholdes så lenge Databehandleravtalen består, og gjøres tilgjengelig for Partene eller tilsynsmyndigheter på forespørsel.

C.4 Overføring av personopplysninger - Lokasjon for behandling og tilgang

Behandling av de personopplysninger som avtalen omfatter kan ikke uten den Behandlingsansvarliges forutgående skriftlige godkjennelse utføres på eller med tilgang fra andre lokasjoner enn de som er angitt i Bilag B.2. Med lokasjon menes:

- Sted det er mulig å få tilgang til personopplysningene fra (aksessering)
- Sted hvor personopplysningene bearbeides (prosesseres)
- Sted hvor personopplysningene lagres

Begrensningen ovenfor gjelder ikke Databehandlerens mor-, søster- og datterselskaper som er etablert innenfor EØS-området. Databehandleren skal imidlertid på forespørsel fra de felles Behandlingsansvarlige redegjøre for hvor personopplysningene til enhver tid behandles.

C.5 Rutiner for revisjon og tilsyn

Bestemmelsene i Behandlingsavtalens Punkt 11.

C.6 Sletting og tilbakelevering av personopplysninger ved Behandlingsavtalens opphør

Partene har avtalt følgende om sletting/tilbakelevering av personopplysninger (velg ett alternativ):

☒	Dersom annet ikke fremgår av lov eller forskrift: Alle personopplysninger som behandles under på Portalen skal slettes uten ugrunnet opphold og senest innen 90 kalenderdager etter opphør av Generelle leveringsvilkår. Dette samme gjelder eventuell annen relevant informasjon som forvaltes på vegne av en Part.
☐	Alle personopplysninger som behandles under denne Databehandleravtale, samt eventuell annen relevant informasjon som forvaltes på vegne av Behandlingsansvarlig, skal tilbakeleveres ved opphør av Hovedavtalen. Etter tilbakelevering er skjedd, plikter Databehandler å slette alle personopplysninger og annen relevant informasjon som forvaltes på vegne av Behandlingsansvarlig innen 30 kalenderdager. Tilbakelevering skal skje på følgende måte: NA

C.7 Kontaktinformasjon

Ved henvendelser i henhold til denne avtalen, eksempelvis ved varsling om brudd på personopplysningssikkerheten eller endring i bruk av underdatabehandlere, skal kontaktinformasjonen angitt på avtalens forside benyttes.