BILAG TIL DATABEHANDLERAVTALEN

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 TIL DATABEHANDLERAVTALENS STANDARDTEKST OG ENDRINGER ETTER AVTALEINNGÅELSEN

A. Opplysninger om behandlingen 3
A.1 Hovedavtalen og formålet med behandlingen av personopplysninger 3
A.2 Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige 3
A.3 Typer av personopplysninger 6
A.4 Kategorier av registrerte 7
A.5 Varighet av behandlingen 7
B. Betingelser for databehandlerens bruk og endring av eventuelle underdatabehandlere 7
B.1 Behandlingsansvarliges godkjennelse av bruk av underdatabehandlere 7
B.2 Godkjente underdatabehandlere 9
C. Instruks vedrørende behandling av personopplysninger 10
C.1 Behandlingens omfang og formål 10
C.2 Sikkerhet ved behandlingen 10
C.2.1 Angivelse av sikkerhetsnivå 10
C.2.2 Styringssystem for informasjonssikkerhet 10
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 avtalens opphør 12
C.7 Sektorspesifikke bestemmelser om behandling av personopplysninger 13
C.8 Kontaktinformasjon 13
D. Endringer til databehandleravtalens standardtekst og endringer etter avtaleinngåelsen 14

A. OPPLYSNINGER OM BEHANDLINGEN

A.1 Hovedavtalen og formålet med behandlingen av personopplysninger

Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige er knyttet til å levere tjenester som beskrevet i hovedavtalen.

Med hovedavtalen menes følgende avtale(r) inngått mellom partene:

Dokumentskanning – saksnr. 2022/751

Behandlingen har følgende formål:

- *Bruk av skytjenestesystem til innsamling og behandling av opplysninger om behandlingsansvarliges kunder.*

A.2 Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige

Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige omhandler (karakteren av behandlingen):

Informasjonsverdiprofil: Kundeopplysninger		
Informasjonsverdi	**Hvorfor er denne viktig for Lånekassen?**	**Beskrivelse**
Kundeopplysninger	*Lånekassens kjernevirksomhet er basert på behandling av våre kunders opplysninger. Lånekassen har litt over 1 million aktive kunder, og deres tillit er avgjørende for virksomheten.*	*Informasjonsverdien kundeopplysninger består av flere underkategorier:* *- **Fortrolig/strengt fortrolig informasjon om kode 6/7 kunder.** Dette gjelder i hovedsak lokaliserende informasjon.* *- **Personsensitiv informasjon.** Dette inkluderer i hovedsak helseinformasjon og soningsforhold.* *- **Generelle personopplysninger som sendes inn av kunden*** *- **Generelle personopplysninger som Lånekassen generer**, slik som klagesaksinformasjon, avtaler til signering, tilskrifter, vedtak, låneinnformasjon (inn/ut, renter)* *- **Generelle opplysninger som hentes fra tredjeparter**, slik som eksamensdata, studentstatus, informasjon fra NAV, folkeregisteret, skatt, UDI og andre tredjeparter* *- **Personopplysninger som ikke er kunderelaterte**, men som Lånekassen likevel får inn.*

Informasjonsverdiprofil: Personalopplysninger		
Informasjonsverdi	**Hvorfor er denne viktig for Lånekassen?**	**Beskrivelse**
Personalopplysninger	*Personalopplysninger er alle opplysninger om medarbeidere og konsulenter i Lånekassen. Dette er informasjon som Lånekassen behandler som en naturlig del av et ansatt, eller kontraktsforhold.*	*- **Sensitive personopplysninger**, slik som sykemeldinger og annen informasjon om sykdomsforhold og fagforeningsmedlemsskap* *- **Generelle personopplysninger**, slik som personaladministrative dokumenter, arbeidsavtaler, lønnsbilag, dokumentasjon fra medarbeidersamtaler.*

Informasjonsverdiprofil: Låneforvaltning/økonomiske data		
Informasjonsverdi	**Hvorfor er denne viktig for Lånekassen?**	**Beskrivelse**
Låneforvaltning/økonomiske data	*Låneforvaltning/økonomiske data er informasjonen som benyttes i Lånekassens låneforvaltning.*	*Informasjonsverdien inkluderer følgende komponenter:* *- **Hovedbok med relevante kontoer*** *- **Kontotransaksjoner, kundeinfo, låneavtaleinfo til/fra hovedbok*** *- **Transaksjoner til/fra samarbeidsbank*** *- **Kodeverk knyttet til låneforvaltning*** *- **Effektuering av sak*** *- **Avstemming sak/lån*** *Kundekontoinformasjon kan være kundeinfo, konto, tilbakebetaling, innbetaling, utbetaling, renteberegning,*

Informasjonsverdiprofil: Lærestedsinformasjon		
Informasjonsverdi	**Hvorfor er denne viktig for Lånekassen?**	**Beskrivelse**
Lærestedsinformasjon	*Lærestedsinformasjon benyttes av Lånekassen for å vurdere om utdanningsstedet kan godkjennes for støtterett.*	*Denne informasjonsverdien inkluderer følgende komponenter:* *- Utdanningsopplegg* *- Vedtak om støtterett* *- Lærestedsinformasjon*

Informasjonsverdiprofil: IT-infrastruktur		
Informasjonsverdi	**Hvorfor er denne viktig for Lånekassen?**	**Beskrivelse**
IT-infrastruktur	*Lånekassen har en visjon om må oppfattes som den mest moderne offentlige virksomhet, og har kommet langt i moderniseringsarbeidet. IT-infrastrukturen står sentralt i all saksbehandling internt i Lånekassen og ut mot kundene.* *Administrative støtteprosesser er også avhengige av IT-systemer.* *IT-systemene behandles som en informasjonsverdi i seg selv, da sårbarheter og svakheter i systemene kan gi tilgang til alle andre informasjonsverdier i Lånekassen.*	*Denne informasjonsverdien inkluderer følgende komponenter:* *- **Driftsoppfølging**, inkluderer teknisk systemdokumentasjon, driftsdokumentasjon, systemlogger, auditlogger, rutinebeskrivelser/sjekklister for brukeradministrasjon, utstyrsavvikling, tilgangsstyring, endringsrutiner, med mer.*

Informasjonsverdiprofil: Leverandørinformasjon		
Informasjonsverdi	**Hvorfor er denne viktig for Lånekassen?**	**Beskrivelse**
Leverandørinformasjon	*Lånekassen samarbeider tett med en rekke private virksomheter, både i form av konsulenttjenester og produktkjøp og er avhengig av et godt, tillitsfult samarbeid for å kunne realisere våre mål.*	*Denne informasjonsverdien inkluderer følgende komponenter:* ***- Leverandøravtaler og kontrakter*** ***Informasjon om ansatte hos leverandøren**, herunder navn, adresse, telefonnummer, epostadresse osv.* ***- Pristilbud*** ***- Løsningsforslag/IPR***

Informasjonsverdiprofil: Virksomhetsstyring		
Informasjonsverdi	**Hvorfor er denne viktig for Lånekassen?**	**Beskrivelse**
Virksomhetsstyring	*Virksomhetsstyringsinformasjon benyttes i den daglige driften til styring og kontroll i Lånekassen.*	*Denne informasjonsverdien inkluderer følgende komponenter:* *- **Dokumenter som har kommet fra eksterne**, slik som forslag til regelverksendringer og info om statsbudsjett fra KD, brev fra offentlige virksomheter* *- **Interne dokumenter og informasjon**, slik som Interne budsjett-, plan- og styringsdokumenter, slik som strategier, VP, disponeringsskriv, årsplaner, datavarehus/analysegrunnlag/aggregert produktinformasjon, utkast til tildelingsbrev med vedlegg*

Informasjonsverdiprofil: Registerdata		
Informasjonsverdi	**Hvorfor er denne viktig for Lånekassen?**	**Beskrivelse**
Registerdata	*Personopplysninger som ikke er kunderelaterte, men som Lånekassen henter inn som følge av maskinelle grensesnitt og prosesser mot tredjeparter slik som eksamensresultater for personer som ikke har et kundeforhold hos Lånekassen.*	*Slik data er:* *- Eksamensresultater for alle som har avlagt eksamen uavhengig av kundeforhold i Lånekassen* *- Likningsopplysninger om hele Norges befolkning* *- Opptaksinformasjon for videregående og høyere utdanning*

A.3 Typer av personopplysninger

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

☒	*Særlige kategorier av personopplysninger i henhold til GDPR artikkel 9 (1):* *Se pkt A2 over, f eks. helseopplysninger, rasemessig eller etnisk opprinnelse eller fagforeningstilhørighet.*
☒	*Andre opplysninger med særlig behov for beskyttelse:* *F.eks. fødselsnummer, opplysninger om økonomi, prestasjonsvurderinger i ansettelsesforhold osv.*
☒	*Andre personopplysninger:* *F.eks. navn og kontaktinformasjon, utdanning, kommunikasjonspreferanser m.m.*

A.4 Kategorier av registrerte

Behandlingen omfatter følgende kategorier av registrerte:

Kunder av Lånekassen.

A.5 Varighet av behandlingen

Databehandlers behandling av personopplysninger under hovedavtalen kan påbegynne når databehandleravtalen har trådt i kraft. Behandlingen har følgende varighet (velg ett alternativ):

☒	Behandlingen er ikke tidsbegrenset, og varer frem til opphør av hovedavtalen.
☐	Behandlingen er tidsbegrenset, og gjelder frem til *<angi dato eller kriterium for avslutning, eksempelvis avslutningen av et prosjekt. Merk at behandlingen normalt ikke kan avslutte før hovedavtalen utløper>.*

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

B. BETINGELSER FOR DATABEHANDLERENS BRUK OG ENDRING AV EVENTUELLE UNDERDATABEHANDLERE

B.1 Behandlingsansvarliges godkjennelse av bruk av underdatabehandlere

Ved inngåelse av databehandleravtalen godkjenner behandlingsansvarlig bruk av de underdatabehandlere som er oppført i punkt B.2. Merk at også mor-, søster- og datterselskaper til databehandleren regnes som underdatabehandlere hvis de bidrar til leveransen og behandler personopplysninger.

For endringer i bruk av underdatabehandlere 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 EU/EØS-området. Databehandleren skal på forhånd informere behandlingsansvarlige om bruken av slik underdatabehandler. (Dette alternativet kan kombineres med et av de andre alternativene.)
☒	Databehandler kan gjennomføre endringer i bruken av underdatabehandlere forutsatt at den behandlingsansvarlige underrettes og gis mulighet til å motsette seg endringene. En slik underretning skal være mottatt av behandlingsansvarlig 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 EU/EØS-området (tredjestater) uansett krever skriftlig godkjenning etter databehandleravtalens punkt 10. Hvis behandlingsansvarlig motsetter seg endringen skal databehandler underrettes så snart som mulig. Den behandlingsansvarlige kan ikke motsette seg endringen uten saklig grunn.
☒	Databehandler kan kun gjennomføre endringer i bruken av underdatabehandlere etter spesifikk og forutgående skriftlig godkjennelse fra behandlingsansvarlig.

	Underdatabehandleren kan ikke behandle personopplysninger under hovedavtalen før slik godkjennelse er gitt. Godkjennelse kan ikke nektes uten saklig grunn.

Merknad: Hvis databehandler benytter underleverandør (tredjepart) som leverer standardiserte tredjepartstjenester (typisk skytjenester), og som oppfyller vilkårene i databehandleravtalen punkt 9.7, slik at tredjepartens standard databehandleravtale kommer til anvendelse direkte overfor den behandlingsansvarlige, vil skifte av underleverandør hos tredjeparten følge bestemmelsene i tredjepartens databehandleravtale.

B.2 Godkjente underdatabehandlere

Den behandlingsansvarlige har godkjent bruk av følgende underdatabehandlere (Settes inn senere, ref til SSA-Bilag):

Navn	Org.nr.	Adresse	Beskrivelse av behandling	Behandlingssted	Kontaktinformasjon	Særlige kategorier personopplysninger
[Navn]	*[Org.nr.]*	*[Adresse]*	*[Overordnet beskrivelse av behandlingen hos underdatabehandleren]*	*[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]*	*[Kontaktinformasjon]*	*[Angi om det behandles særlige kategorier av personopplysninger]*
[Navn]	*[Org.nr.]*	*[Adresse]*	*[Overordnet beskrivelse av behandlingen hos underdatabehandleren]*	*[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]*	*[Kontaktinformasjon]*	
[Navn]	*[Org.nr.]*	*[Adresse]*	*[Overordnet beskrivelse av behandlingen hos underdatabehandleren]*	*[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]*	*[Kontaktinformasjon]*	
[Navn]	*[Org.nr.]*	*[Adresse]*	*[Overordnet beskrivelse av behandlingen hos underdatabehandleren]*	*[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på annen måte behandles i]*	*[Kontaktinformasjon]*	

Databehandleren kan ikke bruke den enkelte underdatabehandleren til en annen behandling enn avtalt eller la en annen underdatabehandler utføre den beskrevne behandlingen i andre tilfeller enn det som følger av bilag B, punkt B.1 om skifte av underdatabehandler.

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

- Hovedavtalen
- Databehandleravtalen med bilag

Databehandler har ikke råderett over personopplysningene utover det som er nødvendig for å oppfylle sine plikter etter databehandleravtalen, 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:
Behandlingen omfatter store mengder av «særlige kategorier av personopplysninger» i henhold til GDPR artikkel 9 (1) som krever særlig beskyttelse.

☐ Ikke krever et høyt sikkerhetsnivå. Begrunnelse:

C.2.2 Styringssystem for informasjonssikkerhet

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: Pkt. 7 Sikkerhet i *Hovedavtalen.*
☐	Sikkerhetskrav som beskrevet nedenfor: *<Sett inn beskrivelse av relevante sikkerhetskrav>*

C.3 Dokumentasjon

Databehandler skal dokumentere de rutiner og tiltak som er iverksatt for å oppfylle kravene som framkommer av gjeldende personvernregler og databehandleravtalen, herunder kravene til informasjonssikkerhet. Slik dokumentasjon skal oppbevares og ajourholdes så lenge databehandleravtalen består, og gjøres tilgjengelig for behandlingsansvarlig 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 EU/EØS-området. Databehandleren skal imidlertid på forespørsel fra den behandlingsansvarlige redegjøre for hvor personopplysningene til enhver tid behandles.

C.5 Rutiner for revisjon og tilsyn

For å kontrollere etterlevelse av gjeldende personvernregler og databehandleravtalen er det avtalt følgende (flere valg mulig):

☒	Behandlingsansvarlig har rett til å utføre revisjon på databehandlers forretningssted for å verifisere databehandlers etterlevelse av sine plikter i henhold til denne databehandleravtalen eller gjeldende personvernregler. Slike revisjoner skal: • Gjennomføres etter rimelig forhåndsvarsel og maksimalt én gang i året, med mindre sikkerhetsbrudd hos databehandler eller andre særlige forhold gir grunn for hyppigere revisjoner; • Foregå innenfor normal arbeidstid og ikke forstyrre databehandlers virksomhet unødvendig; • Utføres av ansatte hos behandlingsansvarlig eller av tredjepart som er godkjent av partene og underlagt taushetsplikt. Databehandler plikter å stille til rådighet de ressurser som med rimelighet kan kreves for å gjennomføre revisjonen. Behandlingsansvarlig skal dekke kostnader for eventuelle tredjeparter som benyttes til å gjennomføre revisjonen. For øvrig dekker partene sine egne kostnader ved gjennomføring av revisjonen. Dersom revisjonen avdekker vesentlige brudd på forpliktelsene etter gjeldende personvernregler eller databehandleravtalen, skal

	databehandler likevel dekke behandlingsansvarliges rimelige kostnader ved revisjonen.
☒	Databehandleren skal benytte ekstern revisor til å attestere at sikkerhetstiltak er etablert og virker etter hensikten. Slik revisjon skal: i. gjennomføres én gang årlig, ii. utføres i henhold til anerkjente attestasjonsstandarder, for eksempel ISAE 3402. iii. utføres av en uavhengig tredjepart med tilstrekkelig kunnskap og erfaring Rapportene skal fremlegges for behandlingsansvarlig på forespørsel. Databehandler skal i tillegg gi slik informasjon og bistand som er nødvendig for at behandlingsansvarlig kan etterleve sine forpliktelser etter gjeldende personvernregelverk.
☒	For standardiserte tredjepartstjenester som leveres av underdatabehandler kan det fremlegges tredjepartsrevisjon forutsatt at revisjonen er gjennomført etter alminnelig anerkjente prinsipper og av sertifisert revisor.

C.6 Sletting og tilbakelevering av personopplysninger ved avtalens opphør

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

☒	Alle personopplysninger som behandles under denne databehandleravtale skal slettes uten ugrunnet opphold og senest innen 90 kalenderdager etter opphør av hovedavtalen. Dette samme gjelder eventuell annen relevant informasjon som forvaltes på vegne av behandlingsansvarlig.
☒	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: *Avtales i fm avslutning av avtalen.*

C.7 Sektorspesifikke bestemmelser om behandling av personopplysninger

Ingen.

C.8 Kontaktinformasjon

Ved henvendelser i henhold til denne avtalen, eksempelvis ved varsling om brudd på personopplysningssikkerheten eller endring i bruk av underdatabehandlere, skal følgende kanaler benyttes:

Hos behandlingsansvarlig	**Hos leverandøren**
Sikkerhetsbrudd:	Sikkerhetsbrudd:
Telefon: *90039898*	Telefon: *[Fyll ut]*
E-post: georg.eie@lanekassen.no	E-post: *[Fyll ut]*
Andre henvendelser:	Andre henvendelser:
Navn: *Georg A. Eie*	Navn: *[Fyll ut]*
Stilling: IT-driftsleder	Stilling: *[Fyll ut]*
Telefon: 90039898	Telefon: *[Fyll ut]*
E-post: georg.eie@lanekassen.no	E-post: *[Fyll ut]*

D. ENDRINGER TIL DATABEHANDLERAVTALENS STANDARDTEKST OG ENDRINGER ETTER AVTALEINNGÅELSEN

Ingen endringer avtalt.