Databehandleravtale

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

NLA HØGSKOLEN

Orgnr: 995 189 186

(BEHANDLINGSANSVARLIG)

og

Unit - Direktoratet for IKT og fellestjenester i høyere utdanning og forskning

Orgnr: 919 477 822

(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 (GDPR) 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 behandling i tjenesten, som spesifisert i vedlegg "Avtalens inkluderte tjenester". Vedlegget henviser videre til vedlegg for tjenestebeskrivelser som detaljerer innholdet i tjenesten.

Inkluderte tjenester som inngår i avtalen kan endres gjennom skriftlig meddelelse, jf avtalens punkt 17, og slik endring føres i endringsprotokoll. Se også avtalens punkt 16 angående vilkår for avslutning av avtalen.

Ved motstrid skal vilkårene i denne avtalen gå foran databehandlers personvernerklæring eller vilkår i andre avtaler inngått mellom behandlingsansvarlig og databehandler i forbindelse med behandling i eller bruk av tjenesten.

2. Formålsbegrensning

2.1 Beskrivelse av tjenesten

Tjenesten beskrives i vedlegg for tjenestebeskrivelse som definert i avtalens punkt 1. Se også tilhørende tjenesteavtale.

2.2 Rammer for behandling av personopplysninger

Formålet med databehandlers forvaltning av personopplysninger på vegne av behandlingsansvarlig, er å levere og administrere tjenesten, herunder:

- Drift og vedlikehold
- Utvikling, test og migrering
- Brukerstøtte

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

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

2.3 Ved endring av formål eller tjenestens funksjon

Behandlingsansvarlig skal informeres om endringer i tjenesten.

Endring i formål for forvaltning av tjenesten, jf avtalens punkt 2.2, skal godkjennes av styringsgruppe for inkluderte tjenester i avtalen, jf. avtalens punkt 1, hvis styringsgruppe er definert i tilhørende tjenesteavtale. Hvis inkluderte tjenester ikke har en definert styringsgruppe skal behandlingsansvarlig godkjenne endringen.

Ved vesentlig endring i tjenestens behandling av persondata, jf avtalens punkt 2.1, eller ved endring som vesentlig øker risiko for personvernet, skal endringen godkjennes av styringsgruppe for inkluderte tjenester i avtalen, jf. avtalens punkt 1, hvis styringsgruppe er definert i tilhørende tjenesteavtale. Hvis inkluderte tjenester ikke har en definert styringsgruppe skal behandlingsansvarlig godkjenne endringen.

3. Instrukser

Databehandler skal følge de skriftlige og dokumenterte instrukser for forvaltning av personopplysninger i tjenesten som behandlingsansvarlig har bestemt skal gjelde.

Databehandler og behandlingsansvarlig forplikter seg til å overholde alle plikter i henhold til gjeldende norsk personopplysningslovgivning som gjelder ved bruk av og behandling i tjenesten 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.

4. Opplysningstyper og registrerte

Databehandler forvalter personopplysninger på vegne av behandlingsansvarlig i forbindelse med levering og administrasjon av tjenesten som beskrevet i vedlegg for tjenestebeskrivelse, jf. punkt 1 i denne avtalen.

5. De registrertes rettigheter

Databehandler plikter å bistå behandlingsansvarlig ved ivaretakelse 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.

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

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.

Databehandler skal dokumentere opplæringen av egne ansatte i informasjonssikkerhet. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig.

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.

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 eller administrere tjenesten.

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

8. Tilgang til sikkerhetsdokumentasjon

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

Ansatte hos behandlingsansvarlig har taushetsplikt for konfidensiell sikkerhetsdokumentasjon som databehandler gjør tilgjengelig for behandlingsansvarlig.

9. Varslingsplikt ved sikkerhetsbrudd

Databehandler skal uten ubegrunnet opphold varsle behandlingsansvarlig dersom personopplysninger som forvaltes på vegne av behandlingsansvarlig utsettes for sikkerhetsbrudd som innebærer risiko for krenkelser av de registrertes personvern.

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 varsler om sikkerhetsbrudd fra databehandler blir videreformidlet til Datatilsynet.

10. Underleverandører

Databehandler plikter å inngå egne avtaler med underleverandører til tjenesten som regulerer underleverandørenes forvaltning av personopplysninger i forbindelse med levering og administrasjon av tjenesten.

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

Databehandler skal kontrollere at underleverandører til tjenesten 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 underleverandører i forbindelse med levering og administrasjon av tjenesten, som beskrevet i vedlegg for tjenestebeskrivelse, jf. punkt 1 i denne avtalen.

Databehandler kan ikke engasjere andre underleverandører enn de som er nevnt ovenfor uten at dette på forhånd er godkjent i henhold til avtalens punkt 2.3.

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 til tjenesten.

11. Overføring til land utenfor EU/EØS

Overføring til land utenfor EU/EØS er definert i vedlegg for tjenestebeskrivelse, jf. punkt 1 i denne avtalen.

Hvis ny overføring utenfor EU/EØS er godkjent i henhold til avtalens punkt 2.3, og hvis grunnlaget for overføring er anvendelse av EUs standardkontrakter, godkjenner behandlingsansvarlig at databehandler kan signere EUs standardkontrakt for overføring til 3. land på behandlingsansvarliges vegne.

12. Arkivlova

Behandlingsansvarlig og databehandler sin håndtering av arkivdata er underlagt Arkivlova (1992, nr. 24). I henhold til Arkivlova skal arkivdata lagres i Norge. Kopi av arkivdata kan lagres i EU/EØS.

13. 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 utilgjengelighet.

Databehandler skal gjennomføre sikkerhetsrevisjoner av informasjonssikkerheten i tjenesten. 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 tjenesten. 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.

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

Databehandler skal bistå behandlingsansvarlig dersom bruk av/behandling i tjenesten medfører at behandlingsansvarlig har plikt til å utrede personvernkonsekvenser før tjenesten tas i bruk, jf. forordning (EU) 2016/679 av 27. april 2016, Artikkel 35 og 36. Databehandler kan bistå behandlingsansvarlig ved iverksetting av personvernfremmende tiltak dersom konsekvensutredningen viser at dette er nødvendig.

14. Tilbakelevering og sletting

Ved opphør av denne avtalen, for en eller flere tjenester som inngår i avtalens punkt 1, plikter databehandler å slette og tilbakelevere alle personopplysninger som forvaltes på vegne av behandlingsansvarlig i forbindelse med levering og administrasjon av gjeldende tjenester. Behandlingsansvarlig bestemmer hvordan tilbakelevering av personopplysningene skal skje. Behandlingsansvarlig og databehandler avtaler hensiktsmessig format for tilbakelevering ved tidspunkt for opphør av avtalen.

Databehandler skal slette personopplysninger fra alle lagringsmedier som inneholder personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig. Sletting

skal skje ved at databehandler skriver over personopplysninger etter avtalens opphør, med frist definert i vedlegg for tjenestebeskrivelse som definert i avtalens punkt 1. 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.

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

15. 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 14 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 avtalens punkt 5 og 10 ovenfor.

16. Avtalens varighet

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

Avtalen kan sies opp av begge parter med gjensidig frist tilsvarende oppsigelsestid gitt i tjenesteavtale for de enkelte tjenester som er definert inn i avtalen, jf avtalens punkt 1.

Avtalen kan sies opp for enkelttjenester definert inn i avtalen, jf avtalens punkt 1, uten at avtalen sies opp for resterende tjenester.

17. Meddelelser

Meddelelser etter denne avtalen skal sendes skriftlig til

Databehandler: firmapost@bibsys.no

Behandlingsansvarlig: tj@nla.no / post@nla.no

18. Lovvalg og verneting

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.

Sør-Trøndelag tingrett vedtas som verneting. Dette gjelder også etter opphør av avtalen.

Dersom avtalen er mellom statlige aktører underlagt Kunnskapsdepartementet, og partene ikke oppnår enighet gjennom forhandlinger, skal tvisten løses med bindende virkning av Kunnskapsdepartementet. Hver av partene kan forlange at tvisten oversendes departementet.

***

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

Sted og dato

På vegne av BEHANDLINGSANSVARLIG	På vegne av DATABEHANDLER
_____	Frode Arntsen, avdelingsdirektør
_____	Unit - Direktoratet for IKT og fellestjenester i høyere utdanning og forskning
_____	

Avtalens inkluderte tjenester

Tekniske tjenester

Inngår i avtale (JA/NEI)	Navn på tjeneste	Tilhørende tjenestebeskrivelse er definert i vedlegg med tittel:
JA	Brukerhåndtering	"Tjenestebeskrivelse - Brukerhåndtering"

Bibliotektjenester og lenketjenester

Inngår i avtale (JA/NEI)	Navn på tjeneste	Tilhørende tjenestebeskrivelse er definert i vedlegg med tittel:
JA	Alma	"Tjenestebeskrivelse - Alma"
JA	Oria	"Tjenestebeskrivelse - Oria"
JA	Felles autoritetsregister	"Tjenestebeskrivelse - Felles autoritetsregister"
NEI	Pensumlistesystem	"Tjenestebeskrivelse - Pensumlistesystem"

Tjenester for lagring og publisering

Inngår i avtale (JA/NEI)	Navn på tjeneste	Tilhørende tjenestebeskrivelse er definert i vedlegg med tittel:
JA	Brage	"Tjenestebeskrivelse - Brage"
NEI	Bird	"Tjenestebeskrivelse - Bird"
NEI	DLR	"Tjenestebeskrivelse - DLR"
NEI	OJS	"Tjenestebeskrivelse - OJS"
NEI	MOOC	"Tjenestebeskrivelse - MOOC"

Endringsprotokoll

Protokoll over endringer i avtalen mellom databehandler og behandlingsansvarlig.

Styringsgruppe knyttet til tjenesten, nærmere definert i tilhørende tjenesteavtale for inkluderte tjenester, jf avtalens punkt 1, fører egen protokoll over endringer de vedtar. Behandlingsansvarlig skal informeres om endringer vedtatt i styringsgruppe.

Punkt	Beskrivelse av endring	Dato	Signatur