Databehandleravtaler
for backuptjenesten UH-BaaS
(heretter kalt Tjenesten)

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

Universitetet i Oslo, UIO/USIT

(databehandler)

09.10.2020

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 tjenesten.

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 tjenesten.

2. Formålsbegrensning

Formålet med databehandlers forvaltning av personopplysninger på vegne av behandlingsansvarlig, er kun å levere og administrere sikkerhetskopiering av behandlingsansvarlig sine data, herunder drift og administrasjon av tjenesten.

Personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig kan ikke brukes til andre formål uten at dette på forhånd er godkjent av behandlingsansvarlig. Databehandler har ikke eierskap eller råderett over personopplysninger, og kan ikke behandle disse til egne formål.

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 tjenesten som behandlingsansvarlig har bestemt skal gjelde.

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

Dersom behandlingsansvarlig har ytterligere instrukser til databehandler skal slike instrukser fremkomme i bilag 1 til denne avtalen.

4. Opplysningstyper og registrerte

Databehandler forvalter data på vegne av behandlingsansvarlig kun som sikkerhetskopier av behandlingsansvarligs datalagring. Databehandlers ansvar for dataene begrenses i henhold til ehandelsloven §18. Ansvaret for at dataene som lagres i henhold til denne avtalen ikke bryter med norsk lov ligger på behandlingsansvarlig som eier av primærdataene. Tjenesten skal ikke brukes for å ta sikkerhetskopi av data som bryter med norsk lov. Dersom databehandler gjennom revisjon eller på annen måte får kjennskap til data som bryter med norsk lov plikter databehandler å varsle behandlingsansvarlig slike funn. I spesielle tilfeller kan databehandler varsle andre myndigheter om slike funn.

Databehandler har ingen ansvar for at behandlingsansvarlig registrerer og lagrer personopplysninger på sine systemer som primærdata på en forskriftsmessig måte.

Dersom behandlingsansvarlig har behov for at databehandler forvalter personopplysninger skal dette spesifiseres i bilag 2 til 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.

Databehandler oppfatter at det bekreftes i regjeringens merknader til forskriften § 9.4 femte avsnitt at :

> **«… ingen selvfølge at også opplysninger på reservekopier og lignende blir slettet. Det er naturlig at arbeidsgiver i noen tid etter endt arbeidsforhold behandler opplysninger om tidligere arbeidstakere. Innsyn i slike opplysninger i reservekopier og lignende kan imidlertid kun skje dersom vilkårene i § 9-2 er oppfylt. Typisk vil være at arbeidsgiver har behov for innsyn for å lete frem avtaler eller annen dokumentasjon som er nødvendige for den daglige driften av virksomheten. Også personopplysninger på reservekopier skal slettes etter en viss tid, da det ikke lenger vil foreligge saklig behov for dem. De fleste virksomheter har rutiner for jevnlig sletting eller overskriving av reservekopier, f eks ca hver sjette måned. Slike rutiner vil da sikre at også dokumentasjon på reservekopiene slettes innen rimelig tid. Har arbeidsgiver ikke rutiner for sletting av reservekopier, må det iverksettes særskilte tiltak for å ivareta personvernet til arbeidstakere…»**
>
> Kilde:
>
> *https://www.regjeringen.no/globalassets/upload/fad/vedlegg/personvern/epostforskriften_merknader_rev.pdf?id=2176744*

For sikkerhetskopier gjennom bruk av tjenesten er det satt en lengde på lagring av sikkerhetskopier i henhold til inngått tjenesteavtale. Sikkerhetskopierte data blir automatisk slettet i henhold til lagringslengde slik de fremgår av inngått tjenestavtale. Databehandler oppfatter forskriften og merknadene til forskriften slik at databehandler har tilstrekkelige rutiner for sletting av data til å oppfylle kravene i forskriften og merknadene til disse.

09.10.2020

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.

Grunnleggende sikkerhetsinformasjon skal fremgå av bilag 3 – 6 i denne 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.

Behandlingsansvarlig skal sørge for tilsvarende tilgangskontroll og taushetsplikt om den dokumentasjon databehandler tilgjengeliggjør overfor behandlingsansvarlig.

Norsk lov vil kunne begrense omfanget av taushetsplikten for ansatte hos behandlingsansvarlig, 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.

Varselet 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.

Underleverandører som benyttes for å oppfylle avtalen skal angis i bilag 7 i denne avtalen.

Databehandler kan ikke engasjere andre underleverandører enn de som er nevnt i bilag 7 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

Ingen personopplysninger skal overføres til tredjeland av databehandler uten at det på forhånd er skriftlig godkjent av behandlingsansvarlig.

Overføring av sikkerhetskopierte data gjennom tilbakelegging av data som er initiert av behandlingsansvarlig eller på vegne av behandlingsansvarlig omfattes ikke av bestemmelsene i dette avsnittet.

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 utilgjengelighet.

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. Behandlingsansvarlig skal på forespørsel få tilgang til oppsummeringer av revisjonsrapportene.

Behandlingsansvarlig har taushetsplikt for konfidensiell informasjon som databehandler eller revisor gjør tilgjengelig for behandlingsansvarlig.

Dersom behandlingsansvarlig selv initierer å enten selv eller med en uavhengig tredjepart utføre sikkerhetsrevisjon for tjenesten vil behandlingsansvarlig selv være ansvarlig for kostnader som påløper i forbindelse med slike revisjoner.

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 av sikkerhetskopierte data skal skje ved at databehandler sletter personopplysninger innen den perioden som oppgis i inngått tjenesteavtale etter avtalens opphør.

Tilbakelevering av personopplysninger skal ikke gjøres for data som fremdeles eksisterer på kundens datasystemer.

Behandlingsansvarlig kan ikke kreve at databehandler kostnadsfritt tilrettelegger og tilbakefører sikkerhetskopier av data til tredjepart dersom behandlingsansvarlig inngår avtale med ny leverandør for tjenesten. I slike tilfeller vil det kun være sletting av personopplysninger fra tjenestens sikkerhetskopier som omfattes av denne avtalen.

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 til behandlingsansvarlig 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 seks (6) måneders skriftlig varsel.

16. Kontaktpersoner

Kontaktpersoner for spørsmål knyttet til denne avtalen er angitt i bilag 8 til denne avtalen.

17. 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.

***

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)

09.10.2020

Bilag 1: Instrukser

Behandlingsansvarlig har ikke gitt databehandler andre instrukser enn de som fremkommer i avtalen.

09.10.2020

Bilag 2: Behandling av personopplysninger

Databehandleren forvalter følgende personopplysninger på vegne av behandlingsansvarlig:

Personopplysningene gjelder følgende registrerte:

09.10.2020

Bilag 3 Sikring av system:

Grunnsikring av systemene er underlagt USIT sine krav om sikring av IT systemer slik det fremgår i USIT ledelsessystem for informasjonssikkerhet https://www.uio.no/tjenester/it/sikkerhet/lsis/ kapittel 8 grunnsikring av infrastruktur og tjenester.

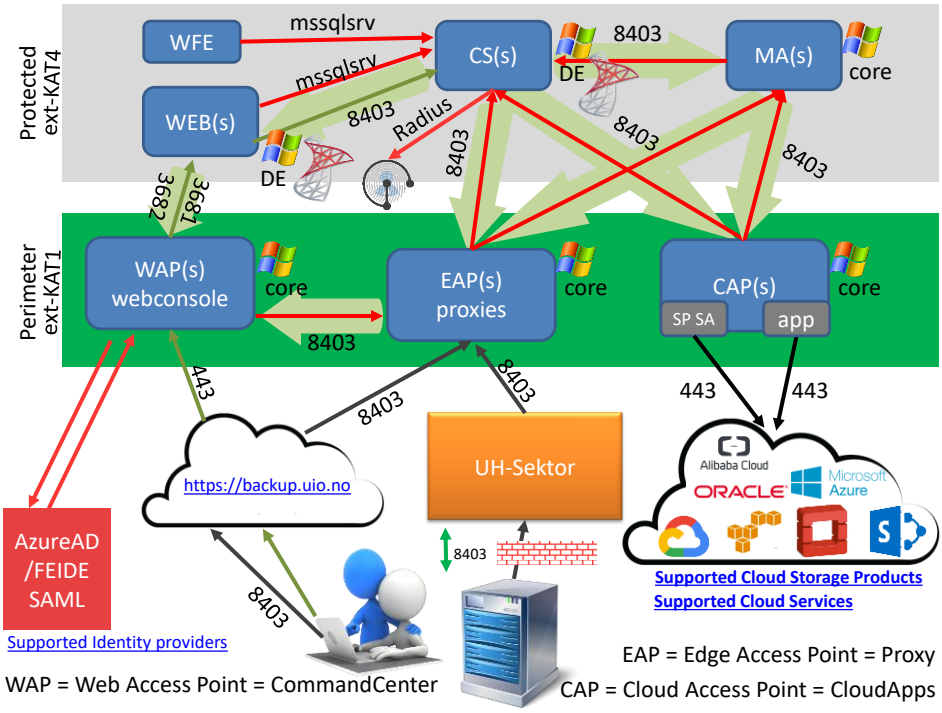
Sikring av universitetets informasjonsressurser avhenger av en trygg og veldrevet IT-infrastruktur.

USIT har ansvar for alle tjenermaskiner og alt infrastruktur-/nettutstyr på Universitetet i Oslo og utformer krav, retningslinjer og rutiner for driften av disse. Behov for sikring utover dette fremkommer eventuelt som resultat av en egen risiko- og sårbarhetsanalyse for tjenesten eller systemet.

Tjenermaskiner og tjenester som drives av andre enn USIT skal drives i tråd med disse kravene og retningslinjene og etter avtale med USIT.

09.10.2020

Bilag 4 Systemskisse



09.10.2020

Bilag 5 Firewall, ACL og kommunikasjonsporter

Backupløsningen benytter proxy servere for kommunikasjon mellom kundens nettverk og backup systemet. Det er ingen begrensninger i USIT nettverksoppsett på hvor trafikken skal komme fra eller gå til annet enn at det er sperret for alt annet enn TCP port 8403. Løsningen er tilgjengelig fra hele verden.

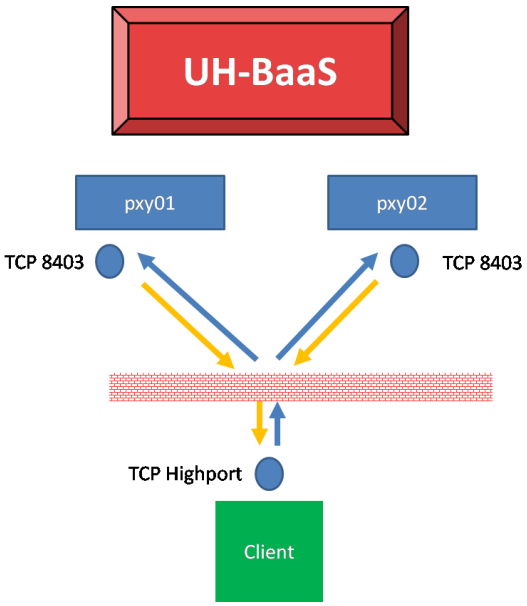
Trafikken vil gå gjennom en TCP tunell som initieres **fra** klienten hos kunden.

Trafikken initieres på høy port på klienten **mot** TCP port 8403 på våre backup proxy servere.

Proxy serverne vil svare fra TCP port 8403 og til den høye TCP porten som klienten initierte trafikken med.

En firewall hos kunde må tillate at trafikk går ut fra kundens nettverk til proxy serverne mot TCP port 8403, og kundens firewall må tillate at proxyene svarer med ESTABLISHED connection fra TCP port 8403 mot kundens klientmaskin.

All kommunikasjon mellom kundens nettverk og backupsystemet vil kjøres gjennom sertifikatbaserte krypterte tuneller i henhold til Commvault system konfigurasjon.



Dersom Kunden har avanserte firewall systemer som går ut over kun å være basert på port nummer. F.eks IPS eller Application control kan det være ytterligere krav som må tilfredsstilles på Kundens firewall systemer.

Bilag 6 Integrasjon mot ekstern autorisasjonstjeneste

Backuptjenesten skal ikke ha lokalt registrerte brukere. Alle brukere av systemet skal være autorisert gjennom andre metoder.

Tjenesten benytter i dag FEIDE og Azure AD, men det er mulighet for å tilrettelegge for en lang rekke andre integrasjonsmuligheter.

Avtalen skal identifisere hvilken autorisasjons provider som skal benyttes for tjenesten.

https://www.uio.no/tjenester/it/hosting/baas/mer-om/generell-info.html

09.10.2020

Bilag 7: Underleverandører

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

- **Commvault** (Systemleverandør, benyttes for håndtering av supportsaker, og kvalitetssikring av løsningen).
- **Core system integration/Dustin** (Benyttes for konsulentoppdrag for tjenesten)

Bilag 8: Kontaktpersoner

Kontaktperson hos databehandler for spørsmål knyttet til denne avtalen er: Kjell Erik Furnes.

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

09.10.2020

Bilag 9: Skytjenester

Leverandørens dokumentasjon for Microsoft MS365

https://documentation.commvault.com/commvault/v11_sp20/article?p=microsoft_office_365_backup.htm

Rettigheter
Det er to brukere som må defineres

- SharePoint online administrator user account that can connect to the tenant URL must have either SharePoint Administrator role or Global Administrator role assigned to it.
- The Azure storage account has "Resource Manager" as its deployment manager and "General Purpose V1 or V2" as its account kind. In the Advanced tab, verify that "Allow access from" is set to the default option "All networks".

Beskrivelse av SharePoint-admin rollen:
https://docs.microsoft.com/en-us/sharepoint/sharepoint-admin-role

Azure Storage Account brukes i forbindelse med restore operasjoner der Azure Storage benyttes som staging område for restore.

Performance for skybaserte tjenester

Performance for skybaserte tjenester er ofte begrenset pr connection. For å øke performance kan man benytte flere connections ved å definere flere conenction brukere i en connection pool.

09.10.2020