Avtaleteksten må tilpasses hver enkelt tjeneste/system og tjenesteleverandør

I henhold til gjeldende norsk personopplysningslovgivning og forordning (EU) 2016/679 av 27. april 2016 (GDPR), artikkel 28, jf. artikkel 29 og 32-36, inngås følgende avtale

mellom

Lindås kommune, org.nr 935084733
Alver kommune, org.nr 920290922 (gjelder fra 01.01.2020 pga kommunesammenslåing)

.....

(behandlingsansvarlig)

og

Inkrement as

.....

(databehandler)

Innhold

30.08.2019

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 (GDPR).

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 Campus Inkrement.

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 Campus Inkrement.

2. Definisjoner

Følgende definisjoner, som gjøres gjeldende i denne avtalen, fremgår av GDPR artikkel 4:

> Nr. 1: «personopplysninger» enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar
> fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en online-identifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet,
>
> Nr. 7: «behandlingsansvarlig» en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige

kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett,

Nr. 8: «databehandler» en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.

3. Formålsbegrensning

Formålet med databehandlers forvaltning av personopplysninger på vegne av behandlingsansvarlig, er å levere og administrere Campus Inkrement.

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

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 11. Underleverandører og 12. Overføring til land utenfor EU/EØS i denne avtalen.

4. Instrukser

a) Databehandler

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

Databehandler forplikter seg til å varsle behandlingsansvarlig dersom databehandler mottar instrukser fra behandlingsansvarlig som er i strid med bestemmelsene i gjeldende norsk personopplysningslovgivning.

b) Behandlingsansvarlig

Lindås kommune/Alver kommune som behandlingsansvarlig forplikter seg til å overholde alle plikter i henhold til gjeldende norsk personopplysningslovgivning som gjelder ved bruk av/behandling i Campus Inkrement til behandling av personopplysninger.

Behandlingsansvarlig skal uten ugrunnet opphold varsle databehandler om forhold behandlingsansvarlig forstår eller bør forstå kan få betydning for oppdragets/tjenestens gjennomføring.

5. Opplysningstyper og registrerte

Databehandleren forvalter følgende personopplysninger på vegne av behandlingsansvarlig i forbindelse med levering og administrasjon av Campus Inkrement:

- Navn og epostadresser til brukerne av tjenesten.
- Kurshistorikk og oppgavebesvarelser.

Personopplysningene gjelder følgende registrerte:

- Ansatte (lærere og eventuelle administratorer av tjenesten)
- Elever

6. De registrertes rettigheter

Databehandler plikter å bistå behandlingsansvarlig ved ivaretakelse av den registrertes rettigheter i henhold til gjeldende norsk personopplysningslovgivning og GDPR.

Den registrertes rettigheter kan inkludere 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.

7. 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, herunder taushetserklæringer for egne ansatte, se punkt 8. Taushetsplikt. 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.

Se ellers vedlegg: *Sikkerhetsdokumentasjon Campus Inkrement.pdf*

8. Taushetsplikt

Taushetspliktbestemmelsene i lov om behandlingsmåten i forvaltningssaker 10. februar 1967 (forvaltningsloven) kommer til anvendelse for databehandler og eventuelle underleverandører.

Kun ansatte hos databehandler som har tjenstlige behov for tilgang til personopplysninger som forvaltes på vegne av behandlingsansvarlig, skal gis slik tilgang. Databehandler plikter å dokumentere retningslinjer og rutiner for tilgangsstyring, herunder sørge for at egne ansatte

undertegner en taushetserklæring.. 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 Campus Inkrement.

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

9. 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 og GDPR.

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.

10. 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 eller de registrerte.

11. Underleverandører

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

I avtaler mellom databehandler og underleverandører skal underleverandørene pålegges å ivareta alle 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 Campus Inkrement 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 følgende underleverandører i forbindelse med levering og administrasjon av Campus Inkrement:

Microsoft Azure: Hosting av tjenesten. Data lagres i Nederland

Freshworks Kundestøttesystemer: For support og oppfølging. Data lagres i Tyskland

Databehandler kan ikke engasjere andre underleverandører enn de som er nevnt ovenfor uten at dette på forhånd er 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 til Campus Inkrement.

12. Overføring til land utenfor EU/EØS

Personopplysninger som databehandler forvalter i henhold til denne avtalen, vil bli overført til følgende mottakerland utenfor EU/EØS:

Ikke Aktuelt

Det rettslige grunnlaget for overføring av personopplysninger til de nevnte mottakerland utenfor EU/EØS er:

Ikke Aktuelt

13. Sikkerhetsrevisjoner og konsekvensutredninger

Databehandler skal jevnlig gjennomføre sikkerhetsrevisjoner av informasjonssikkerheten i Campus Inkrement. 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 Campus Inkrement. 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 Campus Inkrement medfører at behandlingsansvarlig har plikt til å utrede personvernkonsekvenser, jf. GDPR 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 plikter databehandler å slette og tilbakelevere alle personopplysninger som forvaltes på vegne av behandlingsansvarlig i forbindelse med levering og administrasjon av Campus Inkrement. Behandlingsansvarlig bestemmer hvordan tilbakelevering av personopplysningene skal skje, herunder hvilket format som skal benyttes.

Lindås/Alver kommune ønsker at

- Svar: Databehandler skal tilbakelevere personopplysningene på et maskinlesbart format, fortrinnsvis CSV eller JSON.

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 innen (fyll inn antall dager) etter avtalens opphør. 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. Tilbakelevering og sletting ovenfor.

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. Behandlingsansvarlig kan kreve erstatning for økonomiske tap som feil eller forsømmelser fra databehandlers side, inkludert mislighold av vilkårene i denne avtalen.

16. Avtalens varighet

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

Oppsigelse av avtale om bruk av Campus Inkrement medfører samtidig oppsigelse av denne databehandleravtalen.

17. Kontaktinformasjon

Alle henvendelser vedrørende denne avtalen rettes til:

Hos behandlingsansvarlig:	Hos databehandler:
Nils-Erik Buck	Lars Andreas Aas

30.08.2019

+4756375449	+47 995 10 988
nils-erik.buck@lindas.kommune.no	lars.aas@inkrement.no

18. Lovvalg og verneting

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

***

Undertegning

For behandlingsansvarlig:
Knarvik 05.09.19

NILS-ERIK BUCK
IKT-LEIAR

For databehandler:
Oslo 30.08.10

Lars Unneberg, Partner

Vedlegg

INKREMENT

Datasikkerhet i Campus Inkrement

Internkontroll

Databehandleren har et internkontrollsystem i tråd med hva datatilsynet anbefaler ved behandling av ikke sensitive personopplysninger.

Ansvar og oppgaver for informasjonssikkerhet er dokumentert.

Ansvarsforholdene er gjort kjent for alle i organisasjonen.

Sikkerhetsrevisjoner

De gjennomføres årlige sikkerhetsrevisjoner. Behandlingsansvarlig får tilgang ved forespørsel.

Avvikshåndtering

Avvik i informasjonssikkerhet registreres og rapporteres. Den behandlingsansvarlige varsles i de tilfeller hvor avvikene er av en slik art at datatilsynet skal varsles.

Taushetsplikt

Alle medarbeidere er informert om sin taushetsplikt og er klar over dens innhold og omfang.

Alle medarbeidere er informert om sin taushetsplikt og er klar over dens innhold og omfang.

Pseudonymisering og kryptering av personopplysninger

All data på i Campus Inkrement (både data på disk og backup) er kryptert med Storage Service Encryption (SSE).
Kommunikasjon mellom klient og server og kommunikasjon internt i datasenteret er kryptert.
Krypteringsnøkler håndteres sikkert av Azure Key Vault.

Konfidensialitet, integritet, tilgjengelighet og robusthet

Alle ansatte signerer konfidensialitetserklæringer som er vedvarende.

Hardware er redundant i alle ledd. Tjenesten har en målt oppetid > 99.9 % over de siste 2 årene.

Disker som inneholder brukerdata destrueres i hht retninslinjene i NIST 800-88

Brukerdata anonymiseres 3 måneder etter avtalens avslutning eller etter 2 års inaktivitet fra en bruker.

Gjenopprette tilgjengeligheten og tilgangen

Det opprettes daglige «Recovery Points» med Azure Backup som gjør det mulig å gjenopprette tjenesten raskt dersom en alvorlig hendelse skulle inntreffe. Daglig backup av brukerdata (database) til lokal disk. Daglig backup av server ut av datasenter hver natt. Daglig backup holdes i 7 dager, ukentlig backup holdes i 4 uker og månedlig backup holdes i 12 mnd.

Konfidensialitet, integritet, tilgjengelighet

I tråd med hva som personvernforordningen krever og hva datatilsynet anbefaler ved behandling av ikke sensitive personopplysninger.

Personopplysninger som omfattes av denne databehandleravtalen, holdes logisk atskilt fra egne og andres opplysninger og tjenester.

Underleverandør Microsoft Azure er sertifisert følgende:

Certification	Azure
CSA STAR Certification	✓
ISO 27001:2013	✓
ISO 27017:2015	✓
ISO 27018:2014	✓
ISO 20000-1:2011	✓
ISO 22301:2012	✓
ISO 9001:2015	✓

Logging

- Databehandleren registrer all autorisert og uautorisert tilgang til personopplysninger.
- Alle endringer som gjøres på plattformnivå logges i Azure Activity Log.
- Loggene oppbevares til det ikke lenger antas å være bruk for dem, eller i henhold til det leveranseavtalen spesifiserer.

Fysisk sikkerhet

Prosedyrer etablert hos databehandler og underleverandør. Databehandler har rutiner for adgangskort.

Se ellers Microsoft sin informasjon om sikkerhet ved datasenter som dekkes av følgende ISO-sertifiseringer:

Certification	Azure
CSA STAR Certification	✓
ISO 27001:2013	✓
ISO 27017:2015	✓
ISO 27018:2014	✓
ISO 20000-1:2011	✓
ISO 22301:2012	✓
ISO 9001:2015	✓

Teknisk sikkerhet

Systemadministratorer i Campus Inkrement har to-faktorautentisering gjennom egne klientsertifikater.

Kundedata er logisk separert fra hverandre på applikasjonsnivå.

Servere og programvare for underliggende infrastruktur kontrolleres på månedlig basis. Relevante sikkerhetsoppdateringer installeres ved første kontroll og maksimalt en mnd etter at de er gjort tilgjengelige.

En leverandør av alle sertifikat. En person har ansvar for å holde oversikt over og vedlikehold sertifikater som er i bruk.