

Databehandleravtale

Versjon 10.2026

Er inngått mellom:

KUBLAKAN AS

Organisasjonsnummer: 927 470 527

(heretter kalt Databehandler)

og

[Navn på skoleeier]

Organisasjonsnummer: [Behandlingsansvarlig organisasjonsnummer]

(heretter kalt Behandlingsansvarlig)

i fellesskap kalt Partene.

Avtaleparter

For Behandlingsansvarlig	For Databehandler
<p>Sted og dato:</p> <p>Underskrift</p> <p>[Navn]</p>	<p>Sted og dato:</p> <p>Underskrift</p> <p>Asbjørn Odin Aag</p>

Avtalen kan signeres elektronisk eller ved at hver part signerer og utveksler en skannet kopi. Hver part beholder ett eksemplar.

1. Formålet med denne Databehandleravtalen

- 1.1 Denne avtalen («Databehandleravtalen») fastsetter partenes rettigheter og plikter når Databehandleren behandler personopplysninger på vegne av den Behandlingsansvarlige som del av leveransene under Hovedavtalen. Databehandleravtalen har som formål å sikre at partene etterlever Gjeldende personvernregler.
- 1.2 Databehandleravtalen består av dette dokumentet, samt Bilag A, B, C og D.
- 1.3 Ved motstrid mellom Hovedavtalen og Databehandleravtalen, har Databehandleravtalen forrang når det gjelder forhold spesifikt knyttet til behandling av personopplysninger. Ved motstrid mellom Databehandleravtalen og dens bilag, har bilagene forrang.
- 1.4 Databehandleravtalens Bilag A inneholder nærmere beskrivelse av behandlingen som skal foretas, herunder om behandlingsformål, kategorier av personopplysninger og registrerte, regler for sletting og tilbakelevering, partenes kontaktpersoner, samt hvilken eller hvilke underliggende avtaler behandlingen av personopplysninger er knyttet til (se definisjonen av Hovedavtalen nedenfor).
- 1.5 Databehandleravtalens Bilag B inneholder betingelser for bruk av Underdatabehandlere, samt en oversikt over godkjente Underdatabehandlere.
- 1.6 Databehandleravtalens Bilag C inneholder spesifikke instruksjoner for behandling av personopplysninger under Hovedavtalen, herunder sikkerhetstiltak og Behandlingsansvarliges rett til innsyn og revisjon av Databehandler og eventuelle Underdatabehandlere, samt sektorspesifikke bestemmelser om behandling av personopplysninger.
- 1.7 Databehandleravtalens Bilag D inneholder endringer til standardteksten og eventuelle senere avtalte endringer i Databehandleravtalen.

2. Definisjoner

- 2.1 **Gjeldende personvernregler:** Den til enhver tid gjeldende versjon av EUs personvernforordning (2016/679) («personvernforordningen»), samt lov om behandling av personopplysninger av 15.06.2018 (personopplysningsloven) med tilhørende forskrifter mv., samt eventuell annen relevant lovgivning som gjelder behandling og vern av personopplysninger og som er angitt i Bilag C, punkt C.7.
- 2.2 **Hovedavtalen:** En eller flere avtaler mellom Behandlingsansvarlig og Databehandler om levering av tjenester som innebærer behandling av personopplysninger, som nærmere angitt i Bilag A. Databehandleravtalen kan gjelde flere underliggende avtaler.
- 2.3 **Underdatabehandler:** Annen virksomhet som benyttes av Databehandler som underleverandør til behandling av personopplysninger under Hovedavtalen.
- 2.4 For personvernbegreper som ikke er definert i denne Databehandleravtalen gjelder definisjonene i personvernforordningen artikkel 4.

3. Behandlingsansvarliges plikter og rettigheter

- 3.1 Behandlingsansvarlige har ansvaret for at behandlingen av personopplysninger skjer i samsvar med Gjeldende personvernregler. Behandlingsansvarlige skal i den forbindelse særskilt sørge for at:
 - a) behandlingen av personopplysninger er formålsbestemt og basert på et gyldig rettsgrunnlag;

- b) de registrerte har mottatt nødvendig informasjon om behandlingen av personopplysningene;
- c) Behandlingsansvarlig har gjennomført tilstrekkelige risikovurderinger; og
- d) Databehandler til enhver tid har tilstrekkelige instruksjoner og informasjon for å oppfylle sine plikter i henhold til Databehandleravtalen og Gjeldende personvernregler.

4. Behandlingsansvarliges instruksjoner til Databehandleren

- 4.1 Databehandleren skal behandle personopplysningene i samsvar med Gjeldende personvernregler og den Behandlingsansvarliges dokumenterte instruksjoner, jf. punkt 4.2. Hvis annen behandling er nødvendig for å oppfylle forpliktelser som Databehandler er underlagt i henhold til gjeldende rett, skal Databehandleren underrette den Behandlingsansvarlige så langt dette er tillatt ved lov, jf. personvernforordningen artikkel 28 (3) (a).
- 4.2 Behandlingsansvarliges instruksjoner fremgår av Hovedavtalen og Databehandleravtalen med bilag. Databehandler skal omgående underrette den Behandlingsansvarlige, dersom vedkommende mener at instruksene er i strid med Gjeldende personvernregler, jf. personvernforordningen artikkel 28 (3) (h).
- 4.3 Eventuelle endringer i instruksjoner skal varsles til Databehandler gjennom oppdatering av Bilag D, og skal implementeres av Databehandler innen det tidspunkt Partene avtaler eller, om ingen konkret frist er avtalt, innen rimelig tid. Databehandler kan kreve at Behandlingsansvarlig dekker dokumenterte kostnader som påløper i forbindelse med implementeringen av slike endringer eller forholdsmessig justering av vederlaget under Hovedavtalen dersom den endrede instruksjonen innebærer løpende ekstra kostnader for Databehandleren. Det samme gjelder merkostnader som følge av endring av Gjeldende personvernregler som gjelder den Behandlingsansvarliges virksomhet.

5. Konfidensialitet og taushetsplikt

- 5.1 Databehandleren skal sikre at ansatte og andre som har tilgang til personopplysninger er autorisert til å behandle slike personopplysninger på Databehandlers vegne. Dersom slik autorisasjon utløper eller trekkes tilbake, skal tilgangen til personopplysningene opphøre uten ugrunnet opphold.
- 5.2 Databehandleren skal kun autorisere personer som trenger tilgang til personopplysningene i forbindelse med arbeid for å kunne oppfylle Hovedavtalen, Databehandleravtalen og eventuelt annen behandling som er nødvendig for å oppfylle forpliktelser som Databehandler er underlagt i henhold til gjeldende rett, se punkt 4.1 siste setning.
- 5.3 Databehandleren skal sikre at personer som er autorisert til å behandle personopplysninger på vegne av den Behandlingsansvarlige er underlagt taushetsplikt gjennom avtale eller lov. Taushetsplikten skal bestå også etter avtalens og/eller ansettelsesforholdets opphør.
- 5.4 Databehandleren skal kunne dokumentere at de relevante personer er underlagt ovennevnte taushetsplikt på forespørsel fra den Behandlingsansvarlige.
- 5.5 Ved opphør av Databehandleravtalen plikter Databehandleren å avvikle alle tilganger til personopplysninger som behandles under avtalen.

6. Bistand til Behandlingsansvarlig

- 6.1 Databehandleren skal på forespørsel bistå Behandlingsansvarlig med oppfyllelse av de registrertes rettigheter etter personvernforordningens kapittel III gjennom egnede tekniske eller organisatoriske tiltak. Plikten til å bistå gjelder likevel bare i den utstrekning dette er

mulig og hensiktsmessig sett hen til karakteren og omfanget av behandlingen av personopplysninger under Hovedavtalen.

- 6.2 Databehandler skal uten ugrunnet opphold videresende alle henvendelser som Databehandler eventuelt mottar fra den registrerte vedrørende den registrertes rettigheter i henhold til Gjeldende personvernregler til Behandlingsansvarlig. Slike henvendelser kan kun besvares av Databehandler når dette er skriftlig godkjent av Behandlingsansvarlig.
- 6.3 Databehandleren skal bistå den Behandlingsansvarlige med å overholde kravene til personopplysningssikkerhet i personvernforordningen artikkel 32–36, herunder yte bistand ved personvernkonsekvensvurdering og forhåndsdrøftinger med Datatilsynet, sett hen til karakteren og omfanget av behandlingen av personopplysninger under Hovedavtalen.
- 6.4 Hvis Databehandler på Behandlingsansvarliges forespørsel yter bistand som nevnt i punkt 6.1 eller 6.3, og bistanden går ut over det som er nødvendig for at Databehandleren skal oppfylle sine egne forpliktelser etter Gjeldende personvernregler, kan Databehandler kreve dekket sine dokumenterte kostnader knyttet til bistanden. Arbeid dekkes i henhold til prisbestemmelsene i Hovedavtalen.

7. Sikkerhet ved behandlingen

- 7.1 Databehandler skal iverksette egnede tekniske og organisatoriske tiltak for å oppnå et tilfredsstillende sikkerhetsnivå sett hen til behandlingens karakter og omfang, den tekniske utviklingen, implementeringskostnader og aktuelle risikoer for fysiske personers rettigheter og friheter. Databehandleren skal som minimum iverksette de tiltak som er spesifisert i Databehandleravtalens Bilag C.
- 7.2 Databehandleren skal foreta risikovurderinger for å sikre at et egnet sikkerhetsnivå opprettholdes til enhver tid. Databehandleren skal herunder sørge for jevnlig testing, analyse og vurdering av sikkerhetstiltakene, særlig med hensyn til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemer og -tjenester, samt evne til raskt å gjenopprette tilgjengeligheten av personopplysningene ved hendelser.
- 7.3 Databehandler skal dokumentere risikovurderingen og sikkerhetstiltakene, og gjøre dem tilgjengelig for Behandlingsansvarlige på forespørsel, samt gi adgang til slik revisjon som er avtalt mellom partene, jf. Databehandleravtalens punkt 11.

8. Melding om brudd på personopplysningssikkerheten

- 8.1 Databehandler skal uten ugrunnet opphold skriftlig underrette den Behandlingsansvarlige om eventuelle brudd på personopplysningssikkerheten, samt for øvrig gi slik bistand og informasjon som er nødvendig for at den Behandlingsansvarlige skal kunne melde bruddet til tilsynsmyndigheter i tråd med Gjeldende personvernregelverk. Frist for underretning fremgår av Bilag C punkt C.4.
- 8.2 Underretning etter punkt 8.1 skal meddeles kontaktpunktet for Behandlingsansvarlig i henhold til Bilag C punkt C.9, og skal:
 - a) beskrive arten av bruddet på personopplysningssikkerheten, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt,
 - b) inneholde navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes,
 - c) beskrive de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten, og

- d) beskrive de tiltak som Databehandleren har truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.

Informasjonen kan i den grad det er nødvendig gis trinnvis uten ytterligere ugrunnet opphold.

- 8.3 Databehandler plikter å gjennomføre alle de tiltak som med rimelighet kan kreves for å utbedre og unngå tilsvarende brudd på personopplysningssikkerheten. Databehandler skal, så langt det er mulig, rådføre seg med Behandlingsansvarlig om de tiltak som skal gjennomføres, herunder vurdere Behandlingsansvarliges eventuelle forslag til tiltak.
- 8.4 Behandlingsansvarlig er ansvarlig for å underrette Datatilsynet og de berørte registrerte om brudd på personopplysningssikkerheten. Databehandler skal ikke informere tredjeparter om brudd på personopplysningssikkerheten med mindre noe annet er påkrevd etter gjeldende rett eller det følger av uttrykkelig skriftlig instruks fra Behandlingsansvarlig.

9. Bruk av Underdatabehandler

- 9.1 Databehandler kan kun benytte Underdatabehandler etter forutgående generell eller spesifikk skriftlig tillatelse fra Behandlingsansvarlig i samsvar med Databehandleravtalens Bilag B. Oversikt over godkjente Underdatabehandlere fremgår av Databehandleravtalens Bilag B.
- 9.2 Dersom en Databehandler engasjerer en Underdatabehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den Behandlingsansvarlige, plikter Databehandler å inngå skriftlig avtale med Underdatabehandleren som pålegger denne tilsvarende forpliktelser med hensyn til vern av personopplysninger som Databehandleren selv er underlagt etter denne Databehandleravtalen. Se punkt 9.7 med hensyn til bruk av standard tredjepartstjenester.
- 9.3 Databehandler skal kun engasjere Underdatabehandlere som gjennomfører egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene etter Gjeldende personvernregler. Databehandler skal gjennomføre kontroller av Underdatabehandlere for å verifisere at tilfredsstillende tiltak er iverksatt. Databehandler skal kunne fremlegge rapporter fra slike kontroller for Behandlingsansvarlig på forespørsel.
- 9.4 Dersom Behandlingsansvarlig motsetter seg endringer i bruken av Underdatabehandlere etter Databehandleravtalens Bilag B punkt B.1 skal Partene i god tro forhandle med sikte på å enes om en rimelig løsning på hvordan videre levering av tjenestene under Hovedavtalen skal gjennomføres, herunder om fordeling av eventuelle kostnader mellom Partene. Endringen i bruk av Underdatabehandlere kan ikke gjennomføres før Partene har kommet til enighet.
- 9.5 Dersom Underdatabehandleren ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger, skal Databehandleren overfor den Behandlingsansvarlige ha fullt ansvar på samme måte som om Databehandler selv sto for behandlingen.
- 9.6 Databehandler plikter å forelegge avtaler med Underdatabehandlere for Behandlingsansvarlig på forespørsel. Dette gjelder likevel bare de delene av avtalen som er relevant for behandlingen av personopplysningene og med de begrensninger som eventuelt måtte følge av lov eller forskrift. Rent kommersielle vilkår kan uansett ikke kreves fremlagt.
- 9.7 I den utstrekning Databehandleren benytter underleverandør som leverer standardiserte tredjepartstjenester som Behandlingsansvarlig uttrykkelig har akseptert at leveres på underleverandørens standardvilkår i henhold til Hovedavtalen, og som Databehandleren følger opp på Behandlingsansvarliges vegne, kan partene bli enige om at underleverandørens standard databehandleravtale legges til grunn og gjøres gjeldende

direkte overfor Behandlingsansvarlig som et direkte databehandlerforhold (altså ikke som Underdatabehandler) forutsatt at den oppfyller kravene i Gjeldende personvernregler. Databehandleren skal følge opp databehandleravtalen med underleverandøren på vegne av Behandlingsansvarlig med mindre annet er avtalt i det enkelte tilfellet.

10. Overføring av personopplysninger til land utenfor EØS-området

- 10.1 Personopplysninger kan bare overføres til et land utenfor EØS-området («Tredjestat») eller til internasjonal organisasjon hvis Behandlingsansvarlig skriftlig har godkjent slik overføring og vilkårene i punkt 10.3 er oppfylt. Som overføring regnes blant annet å:
- a) behandle personopplysningene i datasentre o.l. som er lokalisert i Tredjestat eller av personell som er lokalisert i Tredjestat (ved fjerntilgang);
 - b) overlate behandlingen av personopplysninger til Underdatabehandler i Tredjestat; eller
 - c) utlevere personopplysningene til en Behandlingsansvarlig i Tredjestat eller i en internasjonal organisasjon.
- 10.2 Databehandler kan likevel overføre personopplysninger dersom det kreves i henhold til gjeldende rett i EØS-området. I slike tilfeller skal Databehandler underrette Behandlingsansvarlig så langt dette er tillatt ved lov.
- 10.3 Overføring til Tredjestater eller internasjonale organisasjoner kan kun finne sted dersom det foreligger nødvendige garantier for et tilstrekkelig beskyttelsesnivå for personvern i henhold til Gjeldende personvernregler. Med mindre annet er avtalt mellom Partene kan slik overførsel kun finne sted med grunnlag i:
- a) en av EU-kommisjonens beslutninger om tilstrekkelig beskyttelsesnivå i henhold til personvernforordningen artikkel 45; eller
 - b) en Databehandleravtale som inkorporerer standard personvernbestemmelser som angitt i personvernforordningen artikkel 46 (2) (c) eller (d) (EU Model clauses); eller
 - c) bindende virksomhetsregler (Binding Corporate Rules) i henhold til personvernforordningen artikkel 47.
- 10.4 Den Behandlingsansvarliges eventuelle godkjennelse av at personopplysninger overføres til en Tredjestat eller internasjonal organisasjon skal fremgå av Databehandleravtalens Bilag B.

11. Generelt om revisjon

- 11.1 Databehandler skal på forespørsel gjøre tilgjengelig for den Behandlingsansvarlige all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i personvernforordningen artikkel 28 og denne Databehandleravtalen er oppfylt.
- 11.2 Databehandler skal muliggjøre og bidra ved inspeksjoner og revisjoner som gjennomføres av eller på oppdrag fra Behandlingsansvarlig. Databehandler skal også muliggjøre og bidra ved inspeksjoner fra aktuelle tilsynsmyndigheter. Den Behandlingsansvarliges tilsyn med eventuelle Underdatabehandler skal skje gjennom Databehandleren med mindre annet er særskilt avtalt. Nærmere rutiner for gjennomføring av revisjoner fremgår av Bilag C punkt C.5.
- 11.3 Dersom en revisjon avdekker avvik fra forpliktelsene i Gjeldende personvernregler eller Databehandleravtalen, skal Databehandler så snart som mulig utbedre avviket. Behandlingsansvarlig kan kreve at Databehandleren midlertidig stopper hele eller deler av behandlingsaktivitetene frem til utbedringen er godkjent av Behandlingsansvarlig.
- 11.4 Hver av Partene dekker sine egne kostnader forbundet med en årlig revisjon. Hvis en revisjon avdekker vesentlige brudd på forpliktelsene etter Gjeldende personvernregler eller

Databehandleravtalen, skal Databehandleren likevel dekke Behandlingsansvarliges rimelige kostnader forbundet med revisjonen.

12. Sletting og tilbakelevering av opplysninger

- 12.1 Ved opphør av denne Databehandleravtalen plikter Databehandler å tilbakelevere og slette alle personopplysninger som behandles på vegne av Behandlingsansvarlig under Databehandleravtalen i samsvar med bestemmelsene i Bilag C punkt C.6. Dette gjelder også eventuelle sikkerhetskopier.
- 12.2 Behandlingsansvarlig bestemmer hvordan en eventuell tilbakelevering av personopplysninger skal skje. Behandlingsansvarlig kan kreve at tilbakelevering skjer på et strukturert og alminnelig anvendt maskinlesbart format. Behandlingsansvarlig skal dekke Databehandlerens dokumenterte kostnader til tilbakelevering med mindre dette er inkludert i vederlaget under Hovedavtalen.
- 12.3 Hvis det benyttes delt infrastruktur eller backup der direkte sletting ikke er teknisk mulig, skal Databehandler sørge for at personopplysningene gjøres utilgjengelige inntil de er overskrevet.
- 12.4 Databehandler skal bekrefte skriftlig overfor Behandlingsansvarlig at sletting eller utilgjengeliggjøring er foretatt og skal på forespørsel dokumentere hvordan det er gjennomført.
- 12.5 Nærmere bestemmelser om sletting og tilbakelevering fremgår av Bilag C.

13. Mislighold og pålegg om stans

- 13.1 Ved brudd på Databehandleravtalen og/eller Gjeldende personvernregler, kan Behandlingsansvarlig og aktuelle tilsynsmyndigheter pålegge Databehandler å stoppe hele eller deler av behandlingen av opplysningene med øyeblikkelig virkning.
- 13.2 Dersom Databehandler ikke overholder sine plikter i henhold til denne Databehandleravtale og/eller Gjeldende personvernregler, vil dette anses som mislighold av Hovedavtalen, og de plikter, frister, sanksjoner og ansvarsbegrensninger som følger av Hovedavtalens regulering av Leverandørens mislighold kommer til anvendelse, med mindre annet er uttrykkelig avtalt mellom partene i Bilag D.

14. Varighet og opphør

- 14.1 Databehandleravtalen gjelder fra den er signert av begge Parter. Databehandleravtalen gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig. Den gjelder også for eventuelle personopplysninger som måtte finnes hos Databehandler eller noen av dennes Underdatabehandlere etter Hovedavtalens opphør.
- 14.2 Reglene om oppsigelse i Hovedavtalen gjelder tilsvarende for Databehandleravtalen, så langt det passer. Databehandleravtalen kan ikke sies opp så lenge Hovedavtalen består med mindre den avløses av en ny databehandleravtale.

15. Lovvalg og verneting

- 15.1 Avtalen er underlagt norsk rett. Tvister løses i samsvar med Hovedavtalens bestemmelser, herunder eventuelle bestemmelser om verneting.

Bilag A – Opplysninger om behandlingen

A.1 Hovedavtalen og formålet med behandlingen

Med Hovedavtalen menes avtalen mellom partene om kjøp av lisenser til KublaKan – videolærebok i norskfaget, slik den fremgår av tilbud, bestilling og faktura, inkludert senere fornyelser.

Databehandleravtalen gjelder for alle lisenser som Behandlingsansvarlig, eller skoler som Behandlingsansvarlig er skoleeier for, kjøper fra Databehandler.

Formålet med behandlingen er å opprette, administrere og avslutte brukerkontoer med lisens for lærere og elever, slik at de får tilgang til læreverket, samt å yte brukerstøtte og sikre stabil og sikker drift av tjenesten.

Avtalen gjelder kun skolekontoer som behandles på vegne av Behandlingsansvarlig. Databehandler er selv behandlingsansvarlig for privatpersoners kjøp av tilgang og for egen kunde-, kontakt- og regnskapsadministrasjon, for eksempel opplysninger om skolens kontaktpersoner og fakturering. Dette omfattes ikke av avtalen.

A.2 Behandlingens art

Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige omfatter:

- registrering og lagring av brukerkontoer basert på e-postadresser som Behandlingsansvarlig oversender;
- administrasjon av lisensperioder (opprettelse, fornyelse og avslutning);
- autentisering ved innlogging, og utsending av e-post for tilbakestilling av passord når brukeren selv ber om det;
- levering av læreverkets innhold, herunder videoer;
- logging av tekniske opplysninger for drift, feilsøking og sikkerhet;
- brukerstøtte; og
- sletting i henhold til Bilag C punkt C.6.

A.3 Typer av personopplysninger

Behandlingen omfatter følgende typer av personopplysninger om de registrerte:

- ☐ Særlige kategorier av personopplysninger i henhold til personvernforordningen artikkel 9 (1)
- ☐ Andre opplysninger med særlig behov for beskyttelse (f.eks. fødselsnummer, vurderinger eller karakterer)
- ☒ Andre personopplysninger:
 - **Kontoopplysninger:** e-postadresse, som også brukes som brukernavn; fornavn og etternavn dersom Behandlingsansvarlig oppgir dette; passord, som kun lagres som kryptografisk hash.
 - **Lisensopplysninger:** hvilken skole brukeren tilhører, samt lisensens startdato, sluttdato og status.
 - **Tekniske opplysninger om bruk av kontoen:** tidspunkt for opprettelse og for siste innlogging; aktive innloggingsøkter (IP-adresse og nettleser- eller enhetstype), som slettes når økten utløper.
 - **Tekniske logger:** serverlogger hos Underdatabehandler (IP-adresse, tidspunkt, forespurt side og nettlesertype) for drift, feilsøking og sikkerhet.

- **E-post og henvendelser:** e-post som sendes til brukeren ved tilbakestilling av passord, og henvendelser til brukerstøtte.
- **Informasjonskapsler,** se Bilag C punkt C.10.

Tidspunkt for siste innlogging og tekniske logger brukes kun til drift og sikkerhet. Det føres ikke lærings- eller progresjonsstatistikk for den enkelte bruker.

Følgende behandles **ikke**: posisjon (utover det som eventuelt kan utledes av IP-adressen), fødselsnummer, karakterer eller andre vurderinger, svar på quizer og oppgaver, eller lærings- og progresjonsdata for den enkelte bruker.

A.4 Kategorier av registrerte

Behandlingen omfatter følgende kategorier av registrerte: elever, lærere, bibliotekarer og andre ansatte ved skolene som bruker KublaKan som læreverk i undervisningen. Mange av elevene er under 18 år.

A.5 Varighet av behandlingen

Databehandlers behandling av personopplysninger under Hovedavtalen kan påbegynnes når Databehandleravtalen har trådt i kraft. Behandlingen har følgende varighet:

- ☒ Behandlingen er ikke tidsbegrenset, og varer frem til opphør av Hovedavtalen. Den enkelte brukerkonto behandles så lenge lisensen er aktiv, og slettes etter reglene i Bilag C punkt C.6.
- ☐ Behandlingen er tidsbegrenset.

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

Bilag B – Underdatabehandlere og andre leverandører

B.1 Godkjennelse og endring av Underdatabehandlere

Ved inngåelse av Databehandleravtalen godkjenner Behandlingsansvarlig bruk av de Underdatabehandlere som er oppført i punkt B.2.

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

- ☒ Databehandler kan gjennomføre endringer i bruken av Underdatabehandlere forutsatt at den Behandlingsansvarlige underrettes skriftlig og gis mulighet til å motsette seg endringene. Når endringen er Databehandlers eget valg, skal underretningen være mottatt senest 1 måned før endringen trer i kraft. Når endringen gjelder en Underdatabehandlers egne underleverandører, skal Databehandler videreformidle varselet uten ugrunnet opphold etter selv å ha mottatt det; fristen kan da være kortere (Kinsta gir for eksempel 14 dagers innsigelsesfrist, og kan ta i bruk nye underleverandører straks av sikkerhetshensyn). Behandlingsansvarlig kan motsette seg endringen med saklig grunn. Løsning ved uenighet fremgår av Bilag D punkt D.1 d). Endringer som medfører overføring av personopplysninger til land utenfor EØS-området krever uansett skriftlig godkjenning etter Databehandleravtalens punkt 10.
- ☐ Databehandler kan kun gjennomføre endringer i bruken av Underdatabehandlere etter spesifikk og forutgående skriftlig godkjennelse fra Behandlingsansvarlig.

B.2 Godkjente Underdatabehandlere

Den Behandlingsansvarlige har godkjent bruk av følgende Underdatabehandlere:

Underdatabehandler	Behandling	Behandlingssted	Overføringsgrunnlag	Kontakt
Kinsta Inc. West Hollywood, USA	Drift av nettstedet: databasen med brukerkontoer, sikkerhetskopier, tilgangsslogger, DNS og utsending av e-post fra nettstedet (tilbakestilling av passord).	Database og sikkerhetskopier: Finland (Google Cloud). Tilgangsslogger og IP-adresser: analyseres i USA (Google, Oracle, ClickHouse). E-post: MailChannels, USA og Canada. DNS: Amazon Web Services, USA. Kinstas personell kan ha fjerntilgang fra land utenfor EØS ved kundestøtte og drift.	EUs standardkontrakter (2021/914), modul 3 (databehandler til underdatabehandler), i Kinstas databehandleravtale. Canada: EU-kommisjonens beslutning om tilstrekkelig beskyttelsesnivå.	privacy@kinsta.com
Cloudflare, Inc. San Francisco, USA	Cloudflare Turnstile: beskyttelse av innlogging og skjemaer mot automatiserte angrep. Mottar IP-adresse og tekniske signaler fra nettleseren. Cloudflare bruker også signalene som selvstendig behandlingsansvarlig, se punkt B.3.	Cloudflares globale nettverk, herunder USA.	EU–US Data Privacy Framework. EUs standardkontrakter i Cloudflares databehandleravtale gjelder subsidiært.	cloudflare.com/privacypolicy

Underdatabehandler	Behandling	Behandlingssted	Overføringsgrunnlag	Kontakt
Google LLC / Google Ireland Ltd. (Google Workspace)	E-postkontoen post@kublakan.no: mottak av henvendelser fra brukere og skoler, og eventuelle delingslenker til brukerlister.	Googles datasentre, blant annet i EU og USA.	EU–US Data Privacy Framework. EUs standardkontrakter i Googles Cloud Data Processing Addendum gjelder subsidiært.	Via Admin-konsollen

Kinstas underleverandører fremgår av kinstas.com/legal/subprocessors. Kinstas øvrige underleverandører for kundestøtte, migrering og AI-verktøy behandler ikke personopplysninger om skolebrukerne, så lenge Databehandler ikke deler slike opplysninger i henvendelser til Kinstas.

Databehandler bruker ikke AI-tjenester til å behandle personopplysninger om skolebrukerne, for eksempel brukerlister eller kontoopplysninger.

B.3 Leverandører som er selvstendig behandlingsansvarlige

Læreverket leveres med enkelte komponenter fra tredjeparter som selv er behandlingsansvarlige for opplysningene de mottar. De er ikke Underdatabehandlere. Databehandler utleverer ikke navn, e-postadresse eller kontoopplysninger til dem. De mottar tekniske opplysninger direkte fra brukerens nettleser når siden lastes eller en video spilles av.

Leverandør	Hva den mottar og hvorfor	Behandlingssted	Overføringsgrunnlag
Vimeo.com, Inc. New York, USA	Videoavspilling. Mottar IP-adresse, nettleserinformasjon og opplysninger om avspillingen. Spilleren brukes med «Do Not Track» (dnt=1). Da settes bare Vimeos nødvendige sikkerhetsinformasjonskapsler (player_clearance, cf_clearance, __cf_bm og _cfuvid), men nettleseren kan sende informasjonskapsler fra Vimeo som brukeren har fått tidligere.	USA	Vimeo deltar i EU–US Data Privacy Framework.
Cloudflare, Inc.	Bruker signalene fra Turnstile til å forbedre botdeteksjonen.	Globalt, herunder USA	EU–US Data Privacy Framework.
Adobe Inc. (Adobe Fonts)	Levering av skrifttyper. Mottar IP-adressen og adressen til siden som laster skriften. Adobe oppgir at IP-adressen ikke lagres og at det ikke settes informasjonskapsler.	USA	EU–US Data Privacy Framework (Adobe er sertifisert). EUs standardkontrakter gjelder for øvrig.
Vipps MobilePay AS Oslo, Norge	Betalingsløsning i nettbutikken. Skriptet lastes fra Vipps MobilePays server og mottar IP-adresse og nettleserinformasjon.	Norge og Danmark (EØS)	Ikke relevant (innenfor EØS).

Ved signering godtar Behandlingsansvarlig at læreverket leveres med disse komponentene. Behandlingsansvarlig bør omtale dem i informasjonen til elevene. Databehandler skal begrense bruken av slike komponenter til det som er nødvendig for å levere læreverket, og varsle Behandlingsansvarlig om nye komponenter eller vesentlige endringer etter samme rutine som i punkt B.1.

B.4 Godkjenning av overføring til tredjeland

Ved signering godkjenner Behandlingsansvarlig de overføringene til USA og Canada som fremgår av punkt B.2, på de angitte overføringsgrunnlagene, jf. Databehandleravtalens punkt 10.

Behandlingsansvarlig godkjenner også at Databehandlers egne ansatte kan ha midlertidig fjerntilgang til systemene i punkt B.2 ved opphold utenfor EØS, for eksempel på reise. Tilgang skjer da over kryptert forbindelse, og personopplysninger om skolebrukerne lagres ikke lokalt.

Databehandler har dokumentert en vurdering av overføringene til tredjeland. Vurderingen gjøres tilgjengelig for Behandlingsansvarlig på forespørsel.

Bilag 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 og 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:

- ☐ Krever et høyt sikkerhetsnivå.
- ☒ Ikke krever et høyt sikkerhetsnivå. Begrunnelse: Behandlingen omfatter e-postadresse, eventuelt navn, og tekniske opplysninger om innlogging. Det behandles ingen særlige kategorier av personopplysninger, fødselsnummer, karakterer, vurderinger eller lærings- og progresjonsdata. Mange av de registrerte er under 18 år. Risikoen for den enkelte ved et brudd vurderes derfor som lav, men mulige følger av uautorisert tilgang til mange kontoer, og misbruk av e-postadresser til svindelforsøk, er tatt med i valget av tiltak i punkt C.2.2.

C.2.2 Sikkerhetstiltak

Databehandler har iverksatt følgende tiltak:

- all trafikk mellom bruker og nettsted krypteres (HTTPS/TLS);
- passord lagres kun som kryptografisk hash;
- antall samtidige innlogginger per konto er begrenset, og innlogging er beskyttet mot automatiserte angrep;
- administrativ tilgang er begrenset til Databehandlers ansatte, med personlige brukerkontoer og tofaktorautentisering;
- arbeidsmaskiner som brukes i administrasjonen har kryptert disk og automatisk skjermlås;
- nettstedet driftes på Kinstas plattform i Google Cloud, med isolerte containere, brannmur og daglige sikkerhetskopier.

Databehandler skal i tillegg:

- installere kritiske sikkerhetsoppdateringer for publiseringsløsningen og tilleggene uten ugrunnet opphold;
- ikke sende lister med personopplysninger om elever som vedlegg i vanlig e-post, og slette mottatte lister, også lokale kopier, når kontoene er opprettet;
- teste gjenoppretting fra sikkerhetskopi minst én gang i året.

C.2.3 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.

C.2.4 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 Behandlingsansvarlig eller tilsynsmyndigheter på forespørsel.

C.3 Lokasjon for behandling og tilgang

Behandling av de personopplysninger som avtalen omfatter kan ikke uten den Behandlingsansvarliges forutgående skriftlige godkjenning utføres på eller med tilgang fra andre lokasjoner enn de som er angitt i Bilag B. Med lokasjon menes sted det er mulig å få tilgang til personopplysningene fra (aksessering), sted hvor personopplysningene bearbeides (prosesserer) og sted hvor personopplysningene lagres.

Databasen med brukerkontoer og sikkerhetskopiene lagres i Kinstas datasenter i Finland. Tilgangsslogger, DNS og e-post fra nettstedet behandles også i USA og Canada, som angitt i punkt B.2. Databehandlers egne ansatte har tilgang fra Norge, og ved midlertidige opphold utenfor EØS etter punkt B.4.

Databehandleren skal på forespørsel fra den Behandlingsansvarlige redegjøre for hvor personopplysningene til enhver tid behandles.

C.4 Frist for varslings av brudd på personopplysningssikkerheten

Databehandler skal varsle Behandlingsansvarlig om brudd på personopplysningssikkerheten uten ugrunnet opphold og **senest 24 timer etter at Databehandler er blitt kjent med bruddet**, jf. Databehandleravtalens punkt 8. For brudd hos en Underdatabehandler regnes fristen fra Databehandler ble varslet av Underdatabehandleren. Er ikke all informasjon tilgjengelig innen fristen, sendes et foreløpig varsel, og resten ettersendes uten ugrunnet opphold. Varselet sendes til kontaktpunktet i punkt C.9.

C.5 Rutiner for revisjon og tilsyn

Behandlingsansvarlig har rett til revisjon, herunder inspeksjon, for å kontrollere at Databehandler etterlever Databehandleravtalen og Gjeldende personvernregler, jf. personvernforordningen artikkel 28 nr. 3 bokstav h og Databehandleravtalens punkt 11. Partene har avtalt følgende om hvordan revisjon gjennomføres:

C.5.1 Dokumentbasert revisjon

Revisjon gjennomføres i utgangspunktet skriftlig. Behandlingsansvarlig kan be om dokumentasjon, for eksempel svar på spørreskjema, beskrivelse av sikkerhetstiltak og rutiner, eller dokumentasjon på at Underdatabehandlere oppfyller sine forpliktelser. Databehandler skal besvare forespørselen innen 30 dager, eller innen en annen frist partene avtaler.

C.5.2 Inspeksjon

Behandlingsansvarlig kan kreve inspeksjon dersom den skriftlige dokumentasjonen etter punkt C.5.1 ikke er tilstrekkelig til å påvise etterlevelse, ved begrunnet mistanke om brudd på Databehandleravtalen eller Gjeldende personvernregler, eller etter et brudd på personopplysningssikkerheten hos Databehandler. Inspeksjon skal:

- a) varsles skriftlig minst 30 dager i forveien, med en beskrivelse av hva som skal kontrolleres, med mindre et brudd på personopplysningssikkerheten eller begrunnet mistanke om alvorlige brudd gjør kortere frist nødvendig;
- b) gjennomføres som digitalt møte med skjermdeling, med mindre særlige grunner tilsier fysisk oppmøte;
- c) gjennomføres maksimalt én gang i året, med mindre et brudd på personopplysningssikkerheten eller begrunnet mistanke gir grunn til hyppigere kontroll;

- d) foregå innenfor normal arbeidstid og ikke forstyrre Databehandlers virksomhet unødvendig;
- e) utføres av ansatte hos Behandlingsansvarlig eller av en uavhengig revisor som er underlagt taushetsplikt; og
- f) ikke gi tilgang til opplysninger om Databehandlers andre kunder eller forretningshemmeligheter.

C.5.3 Underdatabehandlere

For standardiserte tredjepartstjenester levert av Underdatabehandlere kan Databehandler oppfylle revisjonsretten ved å fremlegge Underdatabehandlers egne revisjonsrapporter eller sertifiseringer, for eksempel ISO/IEC 27001 eller SOC 2, utført etter alminnelig anerkjente standarder av uavhengig revisor. Dekker rapportene ikke det forholdet som skal kontrolleres, kan Behandlingsansvarlig kreve ytterligere dokumentasjon eller kontroll gjennom Databehandler, innenfor rammene i Underdatabehandlers vilkår.

C.5.4 Kostnader

Hver part dekker sine egne kostnader ved revisjon. Behandlingsansvarlig dekker kostnader til eventuell ekstern revisor. Dersom revisjonen avdekker vesentlige brudd på Databehandleravtalen eller Gjeldende personvernregler, dekker Databehandler Behandlingsansvarliges rimelige kostnader ved revisjonen.

Bestemmelsene i dette punktet begrenser ikke tilsynsmyndighetenes rett til tilsyn etter gjeldende rett.

C.6 Sletting og tilbakelevering av personopplysninger

Partene har avtalt følgende om sletting og tilbakelevering. Fristene er avtalte frister:

- a) **Utløpt lisens:** Brukerkontoen og tilhørende opplysninger slettes automatisk senest 90 dager etter at lisensen er utløpt, med mindre lisensen fornyes innen den tid. At en lisens utløper, er ikke i seg selv opphør av Hovedavtalen.
- b) **Elever og ansatte som slutter:** Brukerkontoen slettes senest 30 dager etter at Behandlingsansvarlig har bedt om det.
- c) **Opphør av Hovedavtalen:** Ved opphør slettes alle personopplysninger som behandles på vegne av Behandlingsansvarlig senest 90 dager etter opphør, etter Behandlingsansvarliges valg om eventuell tilbakelevering. Tilbakelevering skjer som en liste over brukerkontoene med e-postadresse, navn og lisensperioder i et maskinlesbart format (CSV). Dette er opplysningene som er knyttet til den enkelte konto. Tekniske logger og innloggingsøker tilbakeleveres ikke, men slettes etter lagringstidene i bokstav d.
- d) **Lagringstider for øvrige opplysninger:** Innloggingsøker slettes når de utløper, senest etter 14 dager. Mottatte brukerlister slettes når kontoene er opprettet. Henvendelser til brukerstøtte slettes senest 24 måneder etter at saken er avsluttet. Logg over gjennomførte slettinger, med maskert e-postadresse og domene, oppbevares i 24 måneder som dokumentasjon. Hos Underdatabehandlerne lagres serverlogger i 4 dager og tilgangsløgger og IP-adresser i Kinstas analysesystem i 32 dager (pluss 3 dager i sikkerhets kopi). E-post fra nettstedet lagres ikke hos MailChannels etter levering, og leveringslogger slettes etter 35 dager.
- e) **Sikkerhetskopier:** Kinsta tar daglige sikkerhetskopier som beholdes i 14 dager. Slettede opplysninger forsvinner fra sikkerhetskopiene når de roteres, senest 30 dager etter sletting. Inntil da er sikkerhetskopiene sperret for ordinær bruk og brukes bare til gjenoppretting etter feil. Gjenopprettes en sikkerhets kopi, gjennomføres slettinger som er utført etter kopiens tidspunkt på nytt før nettstedet tas i bruk.

- f) **Kopier hos Underdatabehandlere:** Sletting omfatter kopier hos Underdatabehandlere, i samsvar med deres sletterutiner.
- g) **Bekreftelse:** Databehandler bekrefter skriftlig at sletting etter bokstav b og c er gjennomført. Sletting etter bokstav a bekreftes skriftlig når Behandlingsansvarlig ber om det.

Fakturaer og ordreopplysninger om selve kjøpet (skolens navn, kontaktperson og beløp) er Databehandlers egne regnskapsopplysninger og oppbevares etter bokføringsloven. Disse inneholder ikke personopplysninger om elever.

C.7 Sektorspesifikke bestemmelser

Ingen sektorspesifikke bestemmelser er avtalt utover Gjeldende personvernregler.

C.8 Opprettelse av kontoer og overføring av brukerlistre

- Brukerkontoer opprettes med e-postadresser fra skolens eller skoleeiers domene. Andre adresser brukes bare etter skriftlig instruks fra Behandlingsansvarlig.
- Behandlingsansvarlig oversender brukerlistre via en sikker kanal: en delingslenke i skolens egen løsning (for eksempel OneDrive, Teams eller Google Disk) som er begrenset til post@kublakan.no, eller kryptert e-post. Lenker som er åpne for alle som har dem, og vedlegg i vanlig e-post, skal ikke brukes.

C.9 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 Databehandler
Navn: [Fyll ut]	Navn: Asbjørn Odin Aag
Telefon: [Fyll ut]	Telefon: 489 28 270
E-post: [Fyll ut]	E-post: post@kublakan.no

C.10 Informasjonskapsler og analyse

Databehandler bruker ikke annonse-, markedsførings- eller profileringsverktøy, og driver ikke individuell bruksanalyse av skolebrukere, verken før eller etter innlogging.

Nettstedet bruker:

- informasjonskapsler som er nødvendige for innlogging, sikkerhet og nettbutikk;
- informasjonskapsler fra samtykkeløsningen, som lagrer brukerens valg;
- sikkerhetsinformasjonskapsler fra Vimeo og Cloudflare, se punkt B.3.

Besøksstatistikk for nettstedet føres med anonymisert IP-adresse og uten informasjonskapsler. Innloggede skolebrukere registreres ikke i statistikken.

Nettbutikkens funksjon for kildesporing av bestillinger er slått av.

Bilag D – Endringer til Databehandleravtalens standardtekst og endringer etter avtaleinngåelsen

D.1 Endringer til standardteksten

Følgende gjelder foran Databehandleravtalens standardtekst, jf. punkt 1.3:

- a) **Punkt 6.1:** Bistandsplikten avgrenses av behandlingens art og hva som er mulig, jf. personvernforordningen artikkel 28 nr. 3 bokstav e. Ordene «og hensiktsmessig» gjelder ikke.
- b) **Punkt 6.2:** Databehandler kan, etter denne stående instruksen, bekrefte mottak av en henvendelse fra en registrert og henvise vedkommende til Behandlingsansvarlig. Selve kravet avgjøres av Behandlingsansvarlig.
- c) **Punkt 8.4:** Databehandler kan ha nødvendig og fortrolig kontakt med berørte Underdatabehandlere og rådgivere ved håndtering av et brudd på personopplysningssikkerheten.
- d) **Punkt 9.4:** Kommer partene ikke til enighet innen 30 dager etter at Behandlingsansvarlig har motsatt seg en endring, skal partene vurdere alternative løsninger. Finnes ingen akseptabel løsning, kan Behandlingsansvarlig si opp de berørte lisensene med virkning fra endringen, og Databehandler refunderer forholdsmessig forhåndsbetalt vederlag for gjenstående lisensperiode.
- e) **Punkt 9.7** benyttes ikke.
- f) **Punkt 13.1:** Behandlingsansvarliges rett etter avtalen til å kreve stans med øyeblikkelig virkning gjelder når stans er nødvendig for å hindre ulovlig behandling eller vesentlig risiko for de registrerte. Tilsynsmyndighetenes rettigheter etter gjeldende rett berøres ikke.

D.2 Tilleggsforpliktelser

Etter ønske fra skoleeiere har Databehandler i tillegg påtatt seg følgende, som er nærmere regulert i bilagene:

- ingen bruk av elevopplysninger til statistikk, markedsføring eller profilering, og ingen markedsførings- eller tredjepartsinformasjonskapsler for sporing (Bilag C punkt C.10);
- varsling av brudd senest 24 timer etter at Databehandler er blitt kjent med bruddet (Bilag C punkt C.4);
- automatisk sletting senest 90 dager etter at en lisens er utløpt (Bilag C punkt C.6);
- kun skolens e-postadresser og sikker overføring av brukerlister (Bilag C punkt C.8).

D.3 Endringer etter avtaleinngåelsen

Dato	Endring	Signatur