

SKOOLER



Databehandleravtale

mellom

Skooler AS

Org.nr: 896901702

(Databehandler)

og

Tana kommune

Org.nr: 943505527

(Behandlingsansvarlig)

1. AVTALENS BAKGRUNN OG FORMÅL

1.1 Det er et krav etter Gjeldende personvernrett at det inngås en skriftlig databehandlingsavtale mellom en behandlingsansvarlig og en databehandler om behandlingen av personopplysninger.

1.2 Partene har inngått avtale datert 11.01.2017 («Hovedavtalen»). Gjennomføring av Hovedavtalen innebærer at Databehandler vil Behandle Personopplysninger på vegne av Behandlingsansvarlig.

1.3 Denne databehandleravtalen («Databehandleravtalen») regulerer partenes rettigheter og plikter etter Gjeldende personvernrett for blant annet å sikre at Personopplysninger om de Registrerte ikke brukes urettmessig eller kommer uberettigede i hende.

2. DEFINISJONER

«Gjeldende personvernrett»	EUs personverndirektiv 95/46/EC, eller annen fremtidig EU-lovgivning, nasjonale eller internasjonalt bindende personvernlover eller forskrifter, og som regulerer den Behandlingsansvarlige eller Databehandleren. «Gjeldende personvernrett» inkluderer bindende veiledninger, avgjørelser eller vedtak myndigheter, domstoler eller andre relevante organer, i tillegg til EUs personvernforordning (heretter kalt «GDPR») når den trer i kraft den 25. mai 2018;
«Datasubjekt»	Betyr en identifisert eller identifiserbar fysisk person
«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;
«Sikkerhetsbrudd»	Et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til Personopplysninger som er overført, lagret eller på annen måte behandlet;
«Behandling»	Enhver operasjon eller rekke av operasjoner som gjøres med Personopplysninger, enten automatisert eller ikke, som f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrenning, sletting eller tilintetgjøring;
«Pseudonymisering»	Behandling av Personopplysninger på en slik måte at Personopplysningene ikke lenger kan knyttes til en bestemt Registrert uten bruk av tilleggsopplysninger, forutsatt at nevnte tilleggsopplysninger lagres atskilt og omfattes av tekniske og organisatoriske tiltak som sikrer at Personopplysningene ikke kan knyttes til en identifisert eller identifiserbar fysisk person;
«Underleverandør»	En tredjeparts underleverandør som er tilsatt av Databehandleren for å bistå i Behandlingen av Personopplysninger på vegne av den Behandlingsansvarlige;

3. BEHANDLING AV PERSONOPPLYSNINGER

3.1 **Garanti.** Databehandler garanterer at all Behandling av Personopplysninger i medhold av denne Databehandleravtalen til enhver tid skjer i overensstemmelse med Gjeldende personvernrett, herunder at Databehandler har implementert tekniske og organisatoriske tiltak egnet til å sikre (i) at Behandlingen av Personopplysninger oppfyller kravene i Gjeldende personvernrett og (ii) vern av den Registrertes rettigheter.

3.2 **Instruks.** Databehandleren skal kun Behandle Personopplysninger i henhold til dokumenterte instruks fra den Behandlingsansvarlige, med mindre annet kreves etter til Gjeldende personvernrett. Databehandleren skal til enhver tid kunne dokumentere konkrete instruks fra Behandlingsansvarlig. Behandlingsansvarliges instruks gitt til Databehandler og som gjelder ved inngåelse av Databehandleravtalen fremgår av Vedlegg 1. Databehandler skal umiddelbart underrette Behandlingsansvarlig dersom (i) Databehandler mener at en instruks gitt av Behandlingsansvarlig er i strid med Gjeldende personvernrett, og (ii) Databehandler mangler instruks om hvordan Personopplysninger skal behandles i en bestemt situasjon. Databehandler godtar at Behandlingsansvarlig kan endre sine instruks til Databehandler, og dessuten at Behandlingsansvarlig kan foreta eventuelle endringer i denne Databehandleravtalen som følge av endringer i Gjeldende personvernrett.

3.3 **Bistand til Behandlingsansvarlig.** Databehandler skal bistå Behandlingsansvarlig med å oppfylle sine forpliktelser etter Gjeldende personvernrett. Slik bistand omfatter blant annet Behandlingsansvarliges plikt til svare på forespørslers fra Registrerte om innsyn, korrigering, begrensning av Behandlingen, sletting, og retten til å få oversendt kopi av de Personopplysninger som Behandles.

3.4 **Personvernrådgiver.** Dersom Databehandler er forpliktet til det etter Gjeldende personvernrett, skal Databehandler utpeke en personvernrådgiver.

3.5 **Innebygd personvern og dataportabilitet.** Dersom Databehandler designer systemene mv. hvor Behandlingen av Personopplysninger i medhold av denne Databehandleravtalen finner sted, skal Databehandler påse at systemene mv. er designet i overensstemmelse med kravene til innebygd personvern og dataportabilitet etter Gjeldende personvernrett.

3.6 **Forespørslers fra tredjeparter.** Dersom den Registrerte, myndigheter eller andre ber om informasjon fra Databehandleren vedrørende Behandlingen av Personopplysninger i medhold av denne Databehandleravtalen, skal Databehandleren henvise forespørselen til Behandlingsansvarlig. Databehandleren skal ikke, uten forutgående instruksjoner fra Behandlingsansvarlig, overføre eller på annen måte utlevere Personopplysninger eller annen informasjon knyttet til Behandlingen av Personopplysninger til en tredjepart. Hvis

Databehandleren i henhold til Gjeldende personvernrett er pålagt å utlevere Personopplysninger som Databehandleren Behandler på vegne av den Behandlingsansvarlige, må Databehandleren umiddelbart informere Behandlingsansvarlig om dette, og be om konfidensialitet i forbindelse med utleveringen av informasjonen. Databehandler kan ikke handle på vegne av eller opptre som representant for Behandlingsansvarlig.

3.7 **Bistand.** Databehandler skal bistå Behandlingsansvarlig med å oppfylle kravene under Gjeldende personvernrett, inkludert men ikke begrenset til bistand til oppfyllelse av Behandlingsansvarliges plikt til å etterkomme forespørslers fra Datasubjektene om innsyn i egne Personopplysninger, og adgang til retting og sletting av disse.

3.8 **Ytterligere tiltak.** Dersom Behandlingsansvarlig innen rimelighetens grenser etterspør ytterligere tekniske og organisatoriske sikkerhetstiltak og tilpasninger av

behandlingsaktivitetene, skal dette implementeres av Databehandleren uten ekstra kostnad for Behandlingsansvarlig. Behandlingsansvarlig skal varsle Databehandleren om eventuelle endringer av den Behandlingsansvarliges sikkerhetsinstruksjoner og Behandling av Personopplysninger innen rimelig tid slik at Databehandleren rekker å gjøre de nødvendige endringer i de prosedyrene som må implementeres.

3.9 Dokumentasjon på overensstemmelse med Gjeldende personvernrett. Databehandler skal til enhver tid kunne dokumentere overholdelse av denne Databehandleravtalen og Gjeldende personvernrett

3.10 Revisjon. Databehandleren skal gi Behandlingsansvarlig all informasjon og nødvendig assistanse for å påvise at forpliktelsene i denne Databehandleravtalen og Gjeldende personvernrett er overholdt. Databehandler skal videre muliggjøre og bidra til revisjoner, herunder inspeksjoner på stedet av Behandlingsansvarlig eller annen inspektør med fullmakt fra den Behandlingsansvarlige.

3.11 Årlig revisjonsrapport. Databehandleren forplikter seg til å levere en årlig revisjonsrapport til Behandlingsansvarlig som redegjør for hvorvidt Databehandlerens tekniske og organisatoriske tiltak samsvarer med Gjeldende personvernrett.

3.12 Sletting. Databehandleren skal, i tråd med den Behandlingsansvarliges forespørsel eller instruks, slette eller returnere alle Personopplysninger som Databehandler har Behandlet på vegne av Behandlingsansvarlig etter denne Databehandleravtalen. Dette gjelder med mindre Gjeldende personvernrett krever lagring av Personopplysningene.

4. BRUK AV UNDERLEVERANDØR

4.1 Samtykke. Databehandler kan ikke benytte seg av Underleverandør uten først å ha innhentet generell eller spesifikk skriftlig godkjenning fra Behandlingsansvarlig. I den grad Databehandler ønsker å benytte underleverandører for å oppfylle sine forpliktelser i henhold til vilkår for bruk av Tjenesten må dette skriftlig godkjennes av den Behandlingsansvarlige før behandling av personopplysninger i henhold til denne Databehandleravtalen påbegynnes. Det samme gjelder dersom Databehandler ønsker å foreta et skifte av Underleverandør. Eventuelle godkjenninger gitt av Behandlingsansvarlig ved inngåelse av denne Databehandleravtalen følger av Vedlegg 1.

4.2 Avtale med Underleverandør. Ansvar. Databehandleren skal sørge for at eventuelle godkjente Underleverandører inngår skriftligere avtaler som pålegger dem de samme forpliktelsene med hensyn til vern av Personopplysninger som er fastsatt i denne Databehandleravtalen. Databehandleren er fullt ut ansvarlig overfor den Behandlingsansvarlige hva gjelder utførelsen av Underleverandørenes forpliktelser.

4.3 Revisjon. Behandlingsansvarlig kan kreve at Databehandleren reviderer Underleverandøren eller bekrefter at en slik revisjon er gjennomført, eller, når mulig, innhenter eller bistår Behandlingsansvarlig med å innhente en tredjemanns revisjonsrapport om Underleverandørens drift for å sikre samsvar med Gjeldende personvernrett. Behandlingsansvarlig har også rett til, etter skriftlig forespørsel, å motta kopier av de relevante vilkårene i Databehandlerens avtale med Underleverandører som skal Behandle Personopplysninger på vegne av Behandlingsansvarlig.

5. OVERFØRING TIL TREDJELAND

5.1 **Krav om samtykke.** Enhver overføring av Personopplysninger til en stat utenfor EØS krever skriftlig forhåndsgodkjent samtykke fra Behandlingsansvarlig. Et samtykke fra Behandlingsansvarlig forutsetter at vilkårene for overføring til tredjestater eller internasjonale organisasjoner etter Gjeldende personvernrett er oppfylt.

5.2 **Tilbaketrekking av samtykke.** Behandlingsansvarlig kan til enhver tid trekke tilbake sitt samtykke om overføring av Personopplysninger til ett eller flere tredjeland. Ved slik tilbaketreking skal Databehandleren umiddelbart slutte med overføringen av Personopplysninger. På forespørsel fra Behandlingsansvarlig skal Databehandler skriftlig bekrefte at overføringen har opphørt.

6. INFORMASJONSSIKKERHET OG KONFIDENSIALITET

6.1 **Generelt.** Databehandleren skal, for å bistå Behandlingsansvarlig med å oppfylle sine forpliktelser etter Gjeldende personvernrett når det gjelder blant annet sikkerhetstiltak og konsekvensutredninger, være forpliktet til å gjennomføre hensiktsmessige tekniske og organisatoriske tiltak for å beskytte de Personopplysningene som Behandles. Databehandler skal følge Behandlingsansvarliges eventuelle og til enhver tid gjeldende skriftlige krav eller retningslinjer knyttet til informasjonssikkerheten.

6.2 **Plikt til å opprettholde tilstrekkelig sikkerhetsnivå.** Databehandleren skal opprettholde et sikkerhetsnivå for Behandlingen av Personopplysningene som er tilstrekkelig i forhold til risikoen ved Behandlingen. Databehandleren skal beskytte Personopplysningene fra ødeleggelse, endring, ikke-autorisert utlevering, eller ikke-autorisert tilgang. Med hensyntagen til den tekniske utviklingen og gjennomføringskostnadene, Behandlingens art, omfang, formål og i hvilken sammenheng den utføres, i tillegg til den varierende sannsynlighets- og alvorlighetsgraden for fysiske personers rettigheter og friheter, skal Databehandleren gjennomføre følgende tekniske og organisatoriske tiltak:

- a) Pseudonymisering og kryptering av Personopplysninger;
- b) Muligheten til å sikre vedvarende fortrolighet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene som behandler Personopplysninger;
- c) Muligheten til å gjenopprette tilgjengeligheten og tilgangen til Personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse; og
- d) En prosess for regelmessig testing, analysering og vurdering av hvor effektive tekniske og organisatoriske sikkerhetstiltak er med hensyn til sikkerheten ved Behandlingen; og
- e) opprettholde et sikkerhetsnivå som minst er i overensstemmelse med beste bransjepraksis.

6.3 **Ytterligere krav.** I tillegg til de tekniske og organisatoriske tiltakene nevnt ovenfor skal Databehandler implementere følgende tiltak:

- a) Tilgangskontroll hvor tilgang til Personopplysningene styres gjennom et teknisk system for autorisasjonskontroll. Det skal være prosedyrer for tildeling og fjerning av godkjenninger.
- b) Bruker-ID og passord som brukes til å få tilgang til Personopplysninger skal være personlige og skal ikke deles.

- c) Sikker kommunikasjon hvor eksterne datakommunikasjonsforbindelser skal beskyttes ved hjelp av tekniske funksjoner som sikrer at tilkoblingen er autorisert og kryptert for Personopplysninger i transitt, i kommunikasjonskanaler utenfor systemer som styres av Databehandleren.
- d) Det skal være mulig å følge opp tilgangen til Personopplysningene i ettertid gjennom en logg eller lignende informasjonsbase. Loggene skal være beskyttet og kun være tilgjengelig gjennom autorisert personell. Det skal være mulig for Databehandleren å kontrollere informasjonen og rapportere tilbake til Behandlingsansvarlig.
- e) En prosess for å sikre sikker datadestruksjon, når faste eller flyttbare lagringsmedier ikke lenger brukes for sitt formål.
- f) Datautstyr og flyttbare lagringsmedier som inneholder Personopplysninger i Databehandlerens lokaler skal låses inn når de ikke er under oppsyn for å beskytte mot uautorisert bruk og tyveri.
- g) Rutiner for inngåelse av konfidensialitetsavtaler med leverandører som reparerer og tilbyr service på utstyr som brukes til å lagre Personopplysninger.
- h) Rutiner for tilsyn med leverandører som utfører tjeneste i Databehandlerens lokaler. Lagringsmedier som inneholder Personopplysninger skal være låst inn hvis tilsyn ikke er mulig.

6.4 Protokoll. Databehandleren skal føre en protokoll over alle kategorier av Behandlingsaktiviteter som er utført på vegne av Behandlingsansvarlig. Databehandleren skal utarbeide og holde oppdatert en beskrivelse av sine tekniske, organisatoriske og fysiske tiltak for å opprettholde og være i overensstemmelse med Gjeldende personvernrett.

6.5 Konfidensialitet. Databehandleren skal ikke, uten den Behandlingsansvarliges skriftlige forhåndsgodkjenning, utlevere eller på annen måte gjøre Personopplysninger Behandlet i medhold av denne Databehandleravtalen tilgjengelig for tredjeparter. Dette med unntak for de Underleverandører som eventuelt er engasjert i samsvar med Databehandleravtalen.

Databehandleren skal være forpliktet til å sikre at det kun er personer som direkte trenger tilgang til Personopplysninger for å oppfylle Databehandlerens forpliktelser i samsvar med Hovedavtalen som har tilgang til slik informasjon. Databehandleren skal sørge for at alle personene som er involvert i Behandlingen av Personopplysningene har forpliktet seg til konfidensialitet eller er underlagt lovbestemt taushetsplikt.

Ovennevnte konfidensialitetsplikt gjelder også etter at denne Databehandleravtalen har opphørt

7. HÅNDTERING AV SIKKERHETSBRUDD

7.1 Ved Sikkerhetsbrudd som involverer Personopplysninger som Behandles på vegne av Behandlingsansvarlig, skal Databehandleren bistå Behandlingsansvarlig med å sikre overholdelse av den Behandlingsansvarliges forpliktelser i henhold Gjeldende personvernrett, herunder GDPR artikkel 33. Databehandleren varsle Behandlingsansvarlig uten ugrunnet opphold, og senest 24 timer etter at Databehandler har fått kunnskap om Sikkerhetsbruddet. Varselet skal som et minimum:

- a) Beskrive typen Sikkerhetsbrudd, herunder, hvis mulig, kategoriene av og omtrentlig antall
- b) Registrerte og personopplysningsposter som er berørt;
- c) Inneholde navnet og kontaktopplysningene til vedkommende som kan kontaktes for merinformasjon;
- d) Beskrive sannsynlige konsekvenser av Sikkerhetsbruddet;
- e) Beskrive de tiltak som er tatt eller foreslås tatt av den Behandlingsansvarlige for å håndtere Sikkerhetsbruddet, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av Sikkerhetsbruddet.

8. AVTALENS VARIGHET

8.1 **Varighet.** Med mindre annet fremgår gjelder denne Databehandleravtalen så lenge Databehandler Behandler Personopplysninger på vegne av Behandlingsansvarlig etter Hovedavtalen.

8.2 **Opphør.** Hvis en part vesentlig misligholder sine forpliktelser etter denne Databehandleravtalen kan den andre parten heve avtalen. Den part som ønsker å heve avtalen skal gi den andre parten skriftlig varsel med en angivelse av hva misligholdet består i, og en 10 (ti) dagers frist til å rette misligholdet. Hvis misligholdet ikke er rettet innen fristen angitt i varselet anses avtalen for opphørt ved utløpet av fristen. Databehandlerens manglende oppfyllelse av Gjeldende personvernrett eller garantiene i punkt 3 skal alltid anses som et vesentlig mislighold, og vesentlig mislighold av Databehandleravtalen skal også anses som et vesentlig mislighold av Hovedavtalen.

8.3 **Stans av videre Behandling.** Uavhengig av bestemmelsene om opphør kan Behandlingsansvarlig ved Databehandlers brudd på Gjeldende personvernrett, Databehandleravtalen eller instruks gitt i eller i medhold av denne Databehandleravtalen pålegge Databehandler og eventuelle Underleverandør å stoppe den videre behandlingen av Personopplysningene med øyeblikkelig virkning.

9. KONSEKVENNS VED OPPHØR

9.1 Ved opphør av denne Databehandleravtalen skal Databehandler (i) avslutte alle Behandling av Personopplysninger og (ii) etter Behandlingsansvarliges valg, tilbakelevere og/eller slette alle Personopplysninger og kopier av slike Personopplysninger som er mottatt på vegne av den Behandlingsansvarlige og som omfattes av denne Avtalen. Plikten til sletting gjelder i den utstrekning ikke Gjeldende personvernrett krever at Personopplysningene lagres.

9.2 Uavhengig av årsaken til opphøret av Databehandleravtalen skal Databehandler på skriftlig forespørsel fra Behandlingsansvarlig akseptere å utsette opphøret av Databehandleravtalen med inntil 90 dager slik at Behandlingsansvarlig får sikret dataene sine før de tilbakeleveres og/eller slettes.

9.3 Databehandler skal innen 2 (to) uker etter Databehandleravtalens opphør, på eget initiativ skriftlig dokumentere ovenfor Behandlingsansvarlig at sletting og/eller destruksjon er foretatt i henhold til ovennevnte.

10. VEDERLAG

10.1 Databehandlers krav på godtgjørelse er fullt ut regulert i Hovedavtalen. Databehandler har derfor ikke krav på ytterligere godtgjørelse for å gjennomføre sine forpliktelser etter denne Databehandleravtalen.

11. DIVERSE

11.1 **Overdragelse.** Databehandler kan ikke overdra Databehandleravtalen helt eller delvis, eller delegere noen av sine plikter herunder til en tredjepart uten Behandlingsansvarliges skriftlige forhåndsgodkjenning.

11.2 **Ugyldighet.** Dersom en eller flere bestemmelser i denne Databehandleravtalen av domstolene blir kjent å være ugyldige, forblir de resterende bestemmelsene i Databehandleravtalen gyldige og skal tolkes i samsvar med partenes intensjon.

11.3 **Varighet.** Eventuelle forpliktelser som enten uttrykkelig eller av deres art fortsetter etter oppsigelsen eller utløpet av denne Databehandleravtalen, skal forbli gyldige selv etter Databehandleravtalens opphør.

12. MEDDELELSER

Meddelelser etter denne Databehandleravtalen skal sendes skriftlig til:

- **For Databehandler:**
Navn: Vibekke Holme
Rolle: Customer Success Manager
E-post: vh@skooler.com
- **For Behandlingsansvarlig:**
Navn: Trond Are Anti
Rolle: Kommunalsjef for oppvekst
E-post: taa@tana.kommune.no


12. LOVVALG OG VERNETING

Databehandleravtalen er underlagt norsk rett og partene vedtar Oslo tingrett som verneting. Dette gjelder også etter opphør av Databehandleravtalen.

Moss, 06.02.2019


Dato og sted

På vegne av Databehandler

DocuSigned by:

3C1AAB093420466...

Navn: Klaus H. Hansen
Rolle: CFO, Skooler AS
E-post: kh@skooler.com

På vegne av Behandlingsansvarlig

DocuSigned by:

44C35918C5E840D...

Navn: Trond Are Anti
Rolle: Kommunalsjef for oppvekst
E-post: taa@tana.kommune.no