Databehandleravtale

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

(behandlingsansvarlig)

og

Tjenesteleverandør

H Aschehoug & CO W Nygaard AS (Aschehoug) og Unibok AS

(databehandler)

Innhold

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 Lokus, Unibok og Gan Aschehoug Digital (heretter kalt «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 Tjenesten.

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 Tjenesten.

Personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig kan ikke brukes til andre formål enn levering og administrasjon av Tjenesten uten at dette på forhånd er godkjent 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 Tjenesten som behandlingsansvarlig har bestemt skal gjelde, og som fremgår av denne databehandleravtalen.

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 som behandlingsansvarlig forplikter seg til å overholde alle plikter i henhold til gjeldende norsk personopplysningslovgivning som gjelder ved bruk av/behandling i Tjenesten 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 Tjenesten:

Personopplysninger hentet fra Feide:
Oversikt over Feide-attributter som mottas av Tjenesten kan Behandlingsansvarlig til enhver tid se i sin Feide-kundeportal (https://kunde.feide.no). For tiden er det følgende attributter som hentes inn. De attributter som er merket med * mottas i tjenesten når en bruker logger seg inn, men er ikke et krav for at tjenesten skal fungere.

- ✓ cn (Fullt navn)
- ✓ displayName (Navn som normalt vises)
- ✓ givenName (Fornavn)
- ✓ sn (Etternavn)
- ✓ eduPersonOrgDN:eduOrgLegalName (Organisasjonens/skoleeiers foretaksnavn)

- ✓ eduPersonOrgDN:norEduOrgNIN (Skoleeiers organisasjonsnummer)
- ✓ eduPersonOrgDN:o (Skolens navn)
- ✓ eduPersonOrgUnitDN:norEduOrgUnitUniqueIdentifier (Skolens unike id/ organisasjonsnummer/bedriftsnummer)
- ✓ feideSchoolList (Liste med skoler når det er flere enn én)
- ✓ eduPersonOrgUnitDN:ou (Organisasjoner brukeren er medlem av)
- ✓ eduPersonPrimaryAffiliation (primærrolle)
- ✓ eduPersonAffiliation (roller)
- ✓ eduPersonPrincipalName (Brukernes Feide-ID)
- ✓ eduPersonTargetedID (Persistent anonym ID)
- ✓ mail (epost)
- ✓ mobile (Telefon) *
- ✓ preferredLanguage (Målform/språk) *
- ✓ feideYearOfBirth (Fødselsår) *
- ✓ eduPersonEntitlement (Trinn, puppe) *

Det tas forbehold på at ev. nye FEIDE-attributter som tilkommer i FEIDE-katalogen, og som er relevante for tjenesten, kan legges til. Hvilke attributter som overføres kan til enhver tid gjenfinnes på https://kunde.feide.no.

Andre personopplysninger som lagres:

- Tidspunkt for første pålogging, tidspunkt for siste pålogging på Tjenesten
- Hvilke lisenser brukeren har, antall besøk og tidspunkt for første/siste besøk i spesifikke produkter.
- Logg av elevens resultater/progresjon i enkelte produkter.
- Bokmerker og notater i enkelte produkter, blant annet i unibøker.
- Brukerens preferanser for innhold og funksjonalitet (f.eks. relatert til målform, fag og trinn) lagrer vi på brukerens profil.
- Det lagres også at brukeren har samtykket til lagring av personopplysninger, samt en kode for hvilket samtykke dette gjelder.[1]
- Aschehoug bruker IP-adresser til å måle bruken av vår tjeneste, men alle IP-adresser blir anonymisert og ingenting blir lagret permanent. Vedrørende Google Analytics - les mer her om anonymisering av IP i Google Analytics.

Personopplysningene gjelder følgende registrerte:

- Primært elever og ansatte, og eventuelle andre som har en FEIDE-bruker tilknyttet behandlingsansvarlig. Alle som har en Feide-bruker utstedt av behandlingsansvarlig vil kunne logge inn på tjenesten og dermed bli behandlet.

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.

[1] Samtykkeerklæring for henholdsvis elev eller lærer kommer automatisk opp ved første gangs pålogging. Denne må godtas aktivt for at bruker skal kunne gå videre inn på Lokus og på Unibok og før data kan lagres på brukers profil. Elev over 15 år godkjenner samtykke på vegne av seg selv. For elever under 15 år må foresatt godkjenne samtykke.

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 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.

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 Tjenesten.

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

9. Tilgang til sikkerhetsdokumentasjon

Databehandler plikter å, på forespørsel, 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, på forespørsel, 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. Se også om håndteringen av sikkerhetshendelser under punkt 7., andre avsnitt.

11. Underleverandører

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

I avtaler mellom databehandler og underleverandører skal underleverandørene pålegges å ivareta alle plikter som databehandleren selv er underlagt i henhold til denne avtalen. Databehandler plikter å forelegge avtalene for behandlingsansvarlig etter forespørsel. Databehandler skal kontrollere at underleverandører til Tjenesten overholder sine avtalemessige plikter, spesielt at informasjonssikkerheten er tilfredsstillende og at ansatte hos underleverandører er kjent med sine forpliktelser og oppfyller disse. Dersom underdatabehandler ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger og kravene i Avtalen, skal Databehandleren overfor den Behandlingsansvarlige ha fullt ansvar for at underdatabehandler oppfyller sine forpliktelser.

Behandlingsansvarlig godkjenner at databehandler engasjerer følgende underleverandører i forbindelse med levering og administrasjon av Tjenesten:

Redpill Linpro AS, Norge, organisasjonsnummer 975 842 061 (Lokus)

Nagarro AS 980 394 573 (Lokus)

Cloubi Ltd., Finland, organisasjonsnummer 910 292 005 (Lokus og GAN Aschehoug Digital)

Cyberworld Adventure AB (Extransit), Sverige, organisasjonsnummer 556557-4778 (Lokus og GanAschehoug Digital)

Inspera AS, Norge, organisasjonsnummer 998 156 963 (Lokus)

Ravn Webveveriet AS, organisasjonsnummer 979 949 707 (Unibok)

WriteReader APS, Danmark, organisasjonsnummer 34892199 (GAN Aschehoug Digital)

Behandlingsansvarlig gir Databehandleren generell tillatelse til bruk av underdatabehandler for behandling av personopplysninger etter Avtalen. I tilfelle Databehandleren har planer om å benytte andre underdatabehandlere eller skifte ut underdatabehandlere, skal Databehandleren underrette den Behandlingsansvarlige om planene og dermed gi den Behandlingsansvarlige muligheten til å motsette seg slike endringer.

12. Overføring til land utenfor EU/EØS

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

13. Sikkerhetsrevisjoner og konsekvensutredninger

Databehandleren skal oppfylle de krav til sikkerhetstiltak som stilles etter personopplysningsloven med forskrifter, herunder personvernforordningen. Databehandleren skal kunne dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjonen skal være tilgjengelig på Behandlingsansvarliges forespørsel.

Databehandler skal bistå behandlingsansvarlig dersom bruk av Tjenesten 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. Sletting

Ved opphør av denne avtalen plikter databehandler å slette alle personopplysninger som forvaltes på vegne av behandlingsansvarlig i forbindelse med levering og administrasjon av Tjenesten.

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 30 dager etter avtalens opphør.

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 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. 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.

Avtalen kan sies opp av begge parter med en gjensidig frist på 3 måneder.

17. Kontaktinformasjon

Alle henvendelser vedrørende denne avtalen rettes til:

Hos behandlingsansvarlig		Hos databehandler	
Navn	Nils-Erik Buck	Navn	Kristine Nøklestad
Telefon	56 37 5449	Telefon	46 41 60 08
e-post	nils-erik.buck@lindas.kommune.no	e-post	kristine.noklestad@aschehoug.no

18. Lovvalg og verneting

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

***

Undertegning

For behandlingsansvarlig			For databehandler	
04.02.19	Nils E Buck	15.01.19	Svein Skarheim	
Dato	Underskrift	Dato	Underskrift	
	IKT-lærar, Lindås kommune		Svein Skarheim, Forlagsdirektør Utdanning	

Avtalen undertegnes i to eksemplarer, ett til hver part.