



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

ORGANIASJON

ORG NR

.....

(behandlingsansvarlig)

og

Ludenso AS

.....

(databehandler)

Innhold

Innhold	2
1. Avtalens hensikt	3
2. Definisjoner	4
3. Formålsbegrensning	5
4. Instruks	6
5. Opplysningstyper og registrerte	7
6. De registrertes rettigheter	9
7. Tilfredsstillende informasjonssikkerhet	10
8. Taushetsplikt	11
9. Tilgang til sikkerhetsdokumentasjon	12
10. Varslingsplikt ved sikkerhetsbrudd	13
11. Underleverandører	14
12. Overføring til land utenfor EU/EØS	15
13. Sikkerhetsrevisjoner og konsekvensutredninger	16
14. Tilbakelevering og sletting	17
15. Mislighold	18
16. Avtalens varighet	19
17. Kontaktinformasjon	20
18. Lovvalg og vernetting	21

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 Ludenso Create.

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 Ludenso AS.

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 Ludenso Create.

Personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig kan ikke brukes til andre formål enn levering og administrasjon av Ludenso Create 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. Instrukses

a) Databehandler

Databehandler skal følge de skriftlige og dokumenterte instrukses for forvaltning av personopplysninger i Ludenso Create som behandlingsansvarlig har bestemt skal gjelde.

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

b) Behandlingsansvarlig

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

1. Innloggingsinformasjon
 - a. Individuell innlogging: Selvdefinert brukernavn, dette kan være anonymt
 - b. Feide-innlogging. Navn og Feide-ID.
 - c. «Log in with» Google, Apple og Facebook. Navn og e-post.
 - d. Tidspunkt for opprettelse av konto
 - e. Innloggingstidspunkt
 - f. IP-adresse og enhets-ID
2. Modellinformasjon
 - a. 3D-modellen
 - b. Modellnavn
 - c. Tidspunkt for når modellen er endret/logret
 - d. Om modellen er koplet til en fellesvisning
3. Lærerportal (kun for lærere) (ikke fullt implementert per 10.3.21)
 - a. Data om bruk og opprettelse av oppgaver i lærerportalen
 - b. Data om innlogging til lærerportal gjennom informasjonskapsler

Personopplysningen gjelder følgende registrerte:

1. Elever (ikke tiltenkt bruk av lærerportal)
2. Lærere
3. Annet personell som lager bruker

Hva gjør databehandler med personopplysningene?

I Ludenso Create har vi ikke ønske som å samle inn mer personopplysninger enn nødvendig. Alle typene personopplysninger over er helt nødvendige for at all funksjonalitet skal fungere som det er tiltenkt.

1. a, b og c: For at bruker skal kunne logge seg ut og inn igjen, må vi ha en unik ID for at de skal komme tilbake til sine lagrede modeller. Dette gjør vi ved at brukeren selv velger en av disse alternativene.

1. d, e og f: Datostempling for konto, innlogging og modellagring er nødvendig for å holde orden i filsystemet vårt på serversiden. Det er også planlagt i fremtiden at bruker kan organisere modeller etter dato, når det blir mange modeller å holde oversikt over. Disse tre personopplysningene er også noe vi bruker til å holde en (anonym) oversikt over brukerveksten vår. Fra 1d) får vi oversikt over hvor mange nye brukere vi får, 1e) gir oss tall på hvor mange eksisterende brukere som logger seg inn. 1. f gir oss omtrentlig lokasjon som for eksempel Oslo, Kongsvinger, Berlin samt hva slags type enhet som logger seg på (nettleser, iPad, iPhone, Android-enhet). Med denne dataen skjønner vi omtrentlig hvor vi har brukervekst og hvilke type enheter som er mest brukt. Disse analysedataene kan vi ikke kople til enkeltbrukere.

2. Alle personopplysningene under punkt 2 handler spesifikt om data tilknyttet en bruker sin 3D-modell. Med unntak av 2e) er alle disse dataene nødvendige for at programmet fungerer som det gjør i dag. 2e) er lagt inn da lærere har bedt om å kunne gi tilbakemeldinger i app til eleven, men dette er enda ikke implementert per. 10.3.2021.

3. Hele punkt 3 går på Lærerportalen som per 10.3.2021 er en Web portal for lærere. Dataen her samles inn for at de skal kunne ha en bruker (3a), gi dem tilgang til relevante oppgaver (3b) og 3c til å analysere bruken av lærerportal for å kunne forbedre den. 3b og 3c er ikke implementert i dag.

6. De registrertes rettigheter

Databehandler plikter å bistå behandlingsansvarlig ved ivaretagelse 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.

De viktigste sikkerhetsrutinene for ansatte med tilgang til brukerdata:

1. Aldri last ned brukerdata til datamaskinen
2. Aldri la andre mennesker få tilgang til innloggingsdetaljer til skytjenesten Microsoft Azure, for eksempel ved å dele maskin eller brukerprofiler som har innloggingsdetaljer i nettleser.
3. Ansatte skal kun bruke brukerdata for å yte service til den spesifikke brukeren, feilsøking eller forbedring av produkt.

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 Ludenso Create.

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.

Hvordan få tilgang til dokumentasjon?

Send mail til harald@ludenso.com, her kan du få tilgang til oversikt over ansatte med tilgang til servere, deres signerte taushetsplikt og sikkerhetsprotokollgjennomgang, samt selskapets sikkerhetsprotokoll som helhet.

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 varslers om sikkerhetsbrudd fra databehandler blir videreformidlet til Datatilsynet eller de registrerte.

11. Underleverandører

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

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 Ludenso Create 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 Ludenso Create:

- Microsoft Norge
 - For bruk av skytjenesten Azure. Her lagres brukerens 3D-modeller.
- Unity Technologies
 - Spillmotoren vi bruker for å programmere applikasjonen. Identifiserbar persondata er ikke lagret her, men IP-adresse og en unik bruker-ID basert på enheten blir brukt for å se antall unike brukere som logger seg inn samt unøyaktig lokasjon (som for eksempel "Oslo", "Kongsvinger", ect.) Denne dataen kan vi ikke knytte opp mot person, men blir brukt av oss for å få vite antall unike brukere, cirka lokasjon på brukere, antall nye brukere og hva slags operativsystem som er mest brukt.

12. Overføring til land utenfor EU/EØS

Brukerdata overføres ikke til land utenfor EU/EØS.

Brukerdata er lagret på server i Norge.

13. Sikkerhetsrevisjoner og konsekvensutredninger

Databehandler skal jevnlig gjennomføre sikkerhetsrevisjoner av informasjonssikkerheten i Ludenso Create. 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 Ludenso Create. Det skal i tillegg omfatte rutiner for varsling av behandlingsansvarlig ved sikkerhetsbrudd og rutiner for testing av beredskaps- og kontinuitetsplaner.

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 Ludenso Create medfører at behandlingsansvarlig har plikt til å utrede personvernkonsekvenser, jf. GDPR artikkel 35 og 36. Databehandler kan bistå behandlingsansvarlig ved iverksetting av personvernforebyggende 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 Ludenso Create. Behandlingsansvarlig bestemmer hvordan tilbakelevering av personopplysningene skal skje, herunder hvilket format som skal benyttes.

Ved tilbakelevering av data, må behandlingsansvarlig levere bekreftelse fra bruker om at dette ønskes. Denne til dataen vil være som spesifisert i punkt 5.

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. 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.

Avtalen kan sies opp av begge parter med en gjensidig frist på 30 dager.

17. Kontaktinformasjon

Alle henvendelser vedrørende denne avtalen rettes til:

Hos behandlingsansvarlig:

Organisasjon

tlf

epost

Hos databehandler:

Harald Manheim

980 95 145

harald@ludenso.com

18. Lovvalg og verneting

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

Undertegning

For behandlingsansvarlig:

Underskrift, Dato

For databehandler:

Underskrift, Dato

Avtalen undertegnes i to eksemplarer, ett til hver part.