Mal for databehandleravtaler

Avtaleteksten må tilpasses hver enkelt tjeneste/system og tjenesteleverandør

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

mellom

Fauske kommune

…….

(behandlingsansvarlig)

og

Universitetet i Oslo

…….

(databehandler)

Innhold

1. Avtalens hensikt .....**Feil! Bokmerke er ikke definert.**
2. Definisjoner.....**Feil! Bokmerke er ikke definert.**
3. Formålsbegrensning.....**Feil! Bokmerke er ikke definert.**
4. Instrukser.....**Feil! Bokmerke er ikke definert.**
5. Opplysningstyper og registrerte .....**Feil! Bokmerke er ikke definert.**
6. De registrertes rettigheter.....**Feil! Bokmerke er ikke definert.**
7. Tilfredsstillende informasjonssikkerhet.....**Feil! Bokmerke er ikke definert.**

05.05.2021

8. Taushetsplikt .....**Feil! Bokmerke er ikke definert.**
9. Tilgang til sikkerhetsdokumentasjon .....**Feil! Bokmerke er ikke definert.**
10. Varslingsplikt ved sikkerhetsbrudd .....**Feil! Bokmerke er ikke definert.**
11. Underleverandører .....**Feil! Bokmerke er ikke definert.**
12. Overføring til land utenfor EU/EØS .....**Feil! Bokmerke er ikke definert.**
13. Sikkerhetsrevisjoner og konsekvensutredninger .....**Feil! Bokmerke er ikke definert.**
14. Tilbakelevering og sletting.....**Feil! Bokmerke er ikke definert.**
15. Mislighold .....**Feil! Bokmerke er ikke definert.**
16. Avtalens varighet.....**Feil! Bokmerke er ikke definert.**
17. Kontaktinformasjon .....**Feil! Bokmerke er ikke definert.**
18. Lovvalg og verneting.....**Feil! Bokmerke er ikke definert.**

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 Samtavla.

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 Samtavla.

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 Samtavla.

Personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig kan ikke brukes til andre formål enn levering og administrasjon av Samtavla 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 Samtavla som behandlingsansvarlig har bestemt skal gjelde.

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

- Kommentar: Dersom det er behov for det, kan detaljerte instrukser til databehandler legges ved som billag til databehandleravtalen.

b) Behandlingsansvarlig

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

- Kommentar: Gi en kort (gjerne punktvis) oversikt over hvilke hovedtyper personopplysninger som tjenesteleverandøren (databehandleren) forvalter på vegne av skoleeier (behandlingsansvarlig).
- Kommentar: Gi en kort oversikt over hvilke opplysninger som databehandler registrer og lagrer i forbindelse med bruk av tjenesten, for eksempel ved bruk av informasjonskapsler.

Personopplysningene gjelder følgende registrerte:

- Kommentar: Gi en kort oversikt over hvem opplysningene gjelder, for eksempel barn i barnehage, elever, ansatte og foreldre/foresatte.

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.

- Kommentar: retten til dataportabilitet vil mest sannsynlig ikke være aktuell for barnehage- og skoleeiere da det er en rett som først inntrer hvis det rettslige grunnlaget for behandlingen er samtykke, jf. GDPR artikkel 6 nr. 1 bokstav a) eller oppfyllelse av en avtale, jf. GDPR artikkel 6 nr. 1 bokstav b).

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.

- Kommentar: Her kan det være behov for å konkretisere de viktigste sikringstiltakene som databehandleren har iverksatt, eventuelt at det henvises til dokumenter eller publikasjoner som forklarer hvordan databehandleren jobber med informasjonssikkerhet og hvilke sikringstiltak som er etablert for den aktuelle tjenesten eller systemet. Konkretiseringene kan tas inn i selve avtaleteksten eller i billag til avtalen.

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 Samtavla.

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

9. Tilgang til sikkerhetsdokumentasjon

Databehandler plikter å gi behandlingsansvarlig tilgang til all sikkerhetsdokumentasjon som er nødvendig for at behandlingsansvarlig skal kunne ivareta sine forpliktelser i henhold til gjeldende norsk personopplysningslovgivning og GDPR.

Databehandler plikter å gi behandlingsansvarlig tilgang til annen relevant dokumentasjon som gjør det mulig for behandlingsansvarlig å vurdere om databehandler overholder vilkårene i denne avtalen.

Ansatte hos behandlingsansvarlig har taushetsplikt for konfidensiell sikkerhetsdokumentasjon som databehandler gjør tilgjengelig for behandlingsansvarlig.

10. Varslingsplikt ved sikkerhetsbrudd

Databehandler skal uten ubegrunnet opphold varsle behandlingsansvarlig dersom personopplysninger som forvaltes på vegne av behandlingsansvarlig utsettes for sikkerhetsbrudd som innebærer risiko for krenkelser av de registrertes personvern.

Varslet til behandlingsansvarlig skal som minimum inneholde informasjon som:

- beskriver sikkerhetsbruddet,
- hvilke registrerte som er berørt av sikkerhetsbruddet,
- hvilke personopplysninger som er berørt av sikkerhetsbruddet,
- hvilke strakstiltak som er iverksatt for å håndtere sikkerhetsbruddet og

- hvilke forebyggende tiltak som eventuelt er etablert for å unngå liknende hendelser i fremtiden.

Behandlingsansvarlig er ansvarlig for at varsler om sikkerhetsbrudd fra databehandler blir videreformidlet til Datatilsynet eller de registrerte.

11. Underleverandører

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

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 Samtavla 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 Samtavla:

……...
(navn på underleverandører).

Databehandler kan ikke engasjere andre underleverandører enn de som er nevnt ovenfor uten at dette på forhånd er godkjent av behandlingsansvarlig.

Databehandler er erstatningsansvarlig overfor behandlingsansvarlig for økonomiske tap som påføres behandlingsansvarlig og som skyldes ulovlig eller urettmessig behandling av personopplysninger eller mangelfull informasjonssikkerhet hos underleverandører til Samtavla.

12. Overføring til land utenfor EU/EØS

- Kommentar: Personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig kan bli overført til land utenfor EU/EØS (tredjeland). Slik overføring kan skje på visse vilkår og reglene om overføring til tredjeland finnes i GDPR artikkel 45-47 og 49. Disse reglene innebærer blant annet at overføringen vil være lovlig dersom den skjer til et EU-godkjente tredjeland, til amerikanske bedrifter i USA som har sluttet seg til Privacy Shield-ordningen eller på grunnlag av EUs standardkontrakter for overføring av personopplysninger til databehandlere i tredjeland. Reglene gjelder også for sikkerhetskopiering og annen overføring av personopplysninger som skjer i forbindelse med administrasjon av den aktuelle tjenesten, for eksempel support.

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

……...
(navn på mottakerland).

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

……...
(kort redegjørelse for overføringsgrunnlaget).

13. Sikkerhetsrevisjoner og konsekvensutredninger

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

Databehandler skal dokumentere sikkerhetsrevisjonene. Behandlingsansvarlig skal gis tilgang til revisjonsrapportene.

Dersom en uavhengig tredjepart gjennomfører sikkerhetsrevisjoner hos databehandler, skal behandlingsansvarlig informeres om hvilken revisor som benyttes og få tilgang til oppsummeringer av revisjonsrapportene.

- Kommentar: Partene kan avtale at behandlingsansvarlig selv utfører sikkerhetsrevisjoner hos databehandleren, eventuelt også hvordan kostnader som påløper i forbindelse med slike revisjoner skal fordeles.

Databehandler skal bistå behandlingsansvarlig dersom bruk av Samtavla medfører at behandlingsansvarlig har plikt til å utrede personvernkonsekvenser, jf. GDPR artikkel 35 og 36. Databehandler kan bistå behandlingsansvarlig ved iverksetting av personvernfremmende tiltak dersom konsekvensutredningen viser at dette er nødvendig.

14. Tilbakelevering og sletting

Ved opphør av denne avtalen plikter databehandler å slette og tilbakelevere alle personopplysninger som forvaltes på vegne av behandlingsansvarlig i forbindelse med levering og administrasjon av Samtavla. Behandlingsansvarlig bestemmer hvordan tilbakelevering av personopplysningene skal skje, herunder hvilket format som skal benyttes.

- Kommentar: Det kan være en fordel å konkretisere formatet i denne databehandleravtalen.

Databehandler skal slette personopplysninger fra alle lagringsmedier som inneholder personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig. Sletting skal skje ved at databehandler skriver over personopplysninger innen (fyll inn antall dager) etter avtalens opphør. Dette gjelder også for sikkerhetskopier av personopplysningene.

Databehandler skal dokumentere at sletting av personopplysninger er foretatt i henhold til denne avtalen. Dokumentasjonen skal gjøres tilgjengelig for behandlingsansvarlig.

Databehandler dekker alle kostnader i forbindelse med tilbakelevering og sletting av de personopplysninger som omfattes av denne avtalen.

- Kommentar: Partene kan eventuelt avtale nærmere hvordan kostnader som påløper i forbindelse med sletting eller tilbakelevering av personopplysninger skal fordeles.

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.

- Kommentar: Alternativt kan det bestemmes at avtalen gjelder til et bestemt tidspunkt (dato/år).

Avtalen kan sies opp av begge parter med en gjensidig frist på (fyll inn antall dager/måneder).

17. Kontaktinformasjon

Alle henvendelser vedrørende denne avtalen rettes til:

Hos behandlingsansvarlig:	Hos databehandler:
Skoleleder	Bård Henry Moum Jakobsen
[Behandlingsansvarlig telefon]	22852778
	b.h.m.jakobsen@usit.uio.no

18. Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar (fyll inn navn på tingrett) som verneting. Dette gjelder også etter opphør av avtalen.

***

Undertegning

For behandlingsansvarlig: For databehandler:

05.05.2021

_____	_____
Underskrift, Dato	Underskrift, Dato

Avtalen undertegnes i to eksemplarer, ett til hver part.