Ski kommune

Databehandleravtale til driftsavtale

Avtalen omhandler håndtering av taushetsbelagt informasjon og data

mellom

Ski kommune Org. nr. 960 507 878

som behandlingsansvarlig

og

firma Org. nr. xxxxxxxx

som databehandler

()

Denne avtalen er elektronisk signert sammen med øvrige kontraktsdokumenter mellom partene, saksnummer xx/xxxx, senere kalt «kontrakten».

Versjon: mai 2019 PL/UL

1. Formålet med denne databehandleravtalen

Formålet med denne databehandleravtalen er å regulere partenes rettigheter og plikter i forbindelse med databehandlers behandling av personopplysninger og annen taushetsbelagt informasjon på vegne av behandlingsansvarlig iht.:

- Europaparlaments- og rådsforordning (EU) 2016/679 (heretter omtalt som «GDPR»)
- Personvernlovgivningen

I det følgende vil disse lovverkene i fellesskap bli betegnet som «rettsgrunnlaget».

Avtalen regulerer også partenes rettigheter og plikter ved behandling av data og informasjon som er underlagt taushetsplikt i medhold av annen lov eller avtale.

Avtalen skal sikre at personopplysninger eller annen taushetsbelagt informasjon, ikke brukes urettmessig eller kommer uberettigede i hende.

Avtalen regulerer databehandlers bruk av personopplysninger og annen taushetsbelagt informasjon på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse, m.m.

1.1.Definisjoner

I denne avtalen gjelder de definisjoner som fremkommer av rettsgrunnlaget. I tilfelle motstrid har definisjonene i Europaparlaments- og rådsforordning (EU) 2016/679 forrang.

2. Rangordning

Databehandleravtalens bestemmelser har rang foran databehandlers eventuelle egne personvernvilkår, eller eventuelle andre vilkår som måtte inngå i eller påvirke avtaleforholdet i denne databehandleravtalen og/eller kontrakten, herunder avtaler mellom databehandler og dennes underleverandører eller tredjeparter/samarbeidspartnere og eventuelle personvernvilkår disse måtte ha.

3. Omfanget av behandlingen

3.1. Opplysninger som behandles iht. denne databehandleravtalen

Behandlingens formål, type opplysninger og annen behandling er nærmere beskrevet i bilag D1.

3.2. Behandlingstyper omfattet av denne databehandleravtalen

Avtalen skal sikre at databehandler har tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av informasjon som blir utført på vegne av den behandlingsansvarlige, og at databehandler behandler informasjonen i samsvar med den behandlingsansvarliges dokumenterte rutiner.

3.3. Rådighet over data

Databehandler skal behandle informasjonen på vegne av behandlingsansvarlig.

Databehandler har ikke råderett over informasjonen, og kan dermed heller ikke behandle disse til egne formål.

Informasjonen skal utelukkende behandles for å ivareta de formål som er beskrevet i denne databehandleravtalen eller som fremkommer av senere skriftlige instrukser fra behandlingsansvarlig.

Utarbeider behandlingsansvarlig slike instrukser, skal det utarbeides et endringsbilag hvor endringene beskrives.

Informasjonen kan kun utleveres til behandlingsansvarlig og til den/de han skriftlig bemyndiger som mottaker.

4. Partenes plikter og rettigheter

Behandlingsansvarlig er ansvarlig for at personopplysninger blir behandlet i samsvar med personvernforordningen og personopplysningsloven (GDPR artikkel 24). Den behandlingsansvarlige har både en rett og en forpliktelse til å bestemme hvilke formål, og hvilke hjelpemidler som kan brukes i behandlingen (GDPR artikkel 4 nr. 7).

Databehandler skal følge de rutiner og instrukser for behandlingen som behandlingsansvarlig til enhver tid har bestemt at skal gjelde, med mindre lov eller forskrift som databehandler er underlagt tilsier behandling er i strid med instruks. Dersom databehandler behandler personopplysninger uten eller i strid med instruks på grunn av krav i lov eller forskrift, skal databehandleren underrette den behandlingsansvarlige om nevnte rettslige krav før behandlingen, med mindre denne rett av hensyn til viktige allmenne interesser forbyr en slik underretning.

Dersom databehandler mottar instruks som databehandler mener bryter rettsgrunnlaget, skal databehandler umiddelbart informere behandlingsansvarlig.

Databehandler plikter, uten ugrunnet opphold, å bistå behandlingsansvarlig, slik at behandlingsansvarlig kan oppfylle de krav som fremkommer i rettsgrunnlaget slik dette fremkommer til enhver tid, herunder å sikre overholdelse av forpliktelsene i henhold til GDPR artikkel 32–36, idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for databehandleren

4.1. Databehandlers ansatte/andre som opptrer på vegne av databehandler

Samtlige aktører som på vegne av databehandler utfører oppdrag der bruk av/ tilgang til informasjon inngår, skal være kjent med databehandlers avtalemessige og lovmessige forpliktelser overfor behandlingsansvarlig og påta seg å etterleve disse.

Databehandler plikter å ha kontrolltiltak for å forebygge og forhindre at databehandlers medarbeidere, tredjeparter eller systemer, bevisst eller ubevisst, medvirker til uønskede sikkerhetshendelser i databehandlers egen virksomhet eller hos andre virksomheter eller privatpersoner som etter avtale med databehandler medvirker til oppfyllelse av kontrakten.

4.2. Rett til innsyn og tilgang

Behandlingsansvarlig har, med mindre annet er avtalt eller følger av lov, direkte eller gjennom bruk av uavhengig tredjepartsrevisor, rett til tilgang til og innsyn i:

- Den behandling av personopplysninger og taushetsbelagt informasjon som databehandler foretar
- De systemer som benyttes til denne behandlingen

Databehandler plikter å gi nødvendig bistand til slik tilgang/slikt innsyn innen rimelig tid.

Retten gjelder tilsvarende for aktuelle tilsynsmyndigheter.

4.3. Databehandlers taushetsplikt

Databehandler har taushetsplikt om informasjonen og all annen relevant dokumentasjon, som databehandler får tilgang til iht. denne databehandleravtalen.

Taushetsplikten gjelder også etter opphør av kontrakten og denne databehandleravtalen.

Databehandler skal innhente taushetserklæring fra egne ansatte og andre som gis tilgang til behandlingsansvarliges informasjon og annen relevant dokumentasjon i anledning oppdrag disse utfører for behandlingsansvarlig, før tilgang til informasjonen gis. Taushetserklæringen må oppfylle kravene i relevante lovkrav.

Taushetserklæringene skal gjøres tilgjengelig for behandlingsansvarlig på forespørsel.

4.4. Internkontrollsystem / sikkerhetsdokumentasjon

Databehandler skal oppfylle de krav til sikkerhetstiltak som stilles i rettsgrunnlaget, herunder treffe alle tiltak som er nødvendige i henhold til artikkel 32.

Databehandleren skal ha et internkontrollsystem som ivaretar informasjonssikkerheten i tjenesten og som dokumenterer databehandlerens rutiner og tiltak for internkontroll. Databehandler plikter å gi behandlingsansvarlig tilgang til sitt internkontrollsystem og sin sikkerhetsdokumentasjon, alternativt å gi uavhengig tredjepartsrevisor og relevante tilsynsmyndigheter tilgang.

Databehandler plikter å informere behandlingsansvarlig hvis det foretas endringer i internkontrollsystemet eller sikkerhetsdokumentasjonen, av betydning for kontrakten innen rimelig tid.

4.5. Overføring av data til utlandet

Informasjonen kan ikke uten skriftlig godkjennelse fra behandlingsansvarlig overføres til land utenfor EØS (med unntak for EU-godkjente mottakerland utenfor EØS-området). Ved inngåelse av avtale om slik overføring skal behandlingsansvarliges «EUs Model Clause» benyttes.

Begrepet overføring omfatter tilsvarende tilgang til/aksessering til informasjonen av personer/systemer fra land utenfor EØS og overføring av driftsoperasjoner som kan muliggjøre tilgang til informasjonen.

Etter nærmere skriftlig avtale kan eksport skje ved hjelp av andre mekanismer for lovlig eksport i henhold til rettsgrunnlaget.

4.6. Ivaretakelse av de registrertes rettigheter

Databehandler plikter å bistå den behandlingsansvarlige ved ivaretakelse av den registrertes rettigheter etter rettsgrunnlaget (jf. bl.a. GDPR kapittel III), herunder ved hjelp av egnede tekniske og organisatoriske tiltak.

Databehandler skal ikke gi de registrerte innsyn i informasjonen eller etterkomme de registrertes anmodning om retting eller sletting av informasjonen, uten at dette er avtalt skriftlig med behandlingsansvarlig. Databehandler skal, senest innen 2 virkedager, videresende henvendelsen(e) eller henvise de(n) registrerte til behandlingsansvarlig.

5. Bruk av underleverandør

Dersom databehandler benytter seg av underleverandør eller tredjeparter/samarbeidspartner forblir databehandler ansvarlig for deres behandling av informasjonen.

Oversikt over aktuelle underleverandører/ tredjeparter/ samarbeidspartnere ved avtalens oppstart, som er godkjent av behandlingsansvarlig, ligger som bilag 2 til denne databehandleravtalen.

Databehandler kan ikke benytte underleverandører/ tredjeparter/ samarbeidspartnere til oppfyllelse av avtaler med behandlingsansvarlig uten skriftlig forhåndsgodkjennelse fra behandlingsvarlig. Behandlingsansvarlig har rett til å underkjenne valg av nye underleverandører og tredjeparter/ samarbeidspartnere på saklig grunnlag.

Den enkelte databehandleren plikter fortløpende å føre en oversikt over alle underleverandører / tredjeparter/samarbeidspartnere som benyttes i kontrakten og fremlegge denne for behandlingsansvarlig på forespørsel.

Dersom databehandler engasjerer en underleverandører/ tredjeparter/samarbeidspartnere for å utføre spesifikke behandlingsaktiviteter på vegne av behandlingsansvarlig, skal nevnte andre databehandler pålegges de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i databehandleravtalen eller i et annet rettslig dokument mellom behandlingsansvarlig og databehandleren, ved hjelp av en avtale eller et annet rettslig dokument i henhold til lov eller forskrift. Det skal særlig gis tilstrekkelige garantier for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i GDPR.

Underleverandør/ tredjeparter/ samarbeidspartnere plikter å oppfylle alle krav i denne databehandleravtalen og skal signere bilag D2 og D3 dersom relevant. Bilag D2 og dersom relevant bilag D3 skal være mottatt og skriftlig godkjent av behandlingsansvarlig før data kan overføres til/ behandles av den aktuelle underleverandør/ tredjepart/ samarbeidspartner.

Etter nærmere skriftlig avtale kan underleverandørers forpliktelser oppfylles på andre måter som er lovlig i henhold til rettsgrunnlaget.

Bestemmelsen gjelder tilsvarende for den enkelte underleverandørs eller tredjeparters/ samarbeidspartneres underleverandører eller tredjeparter/ samarbeidspartnere.

6. Informasjonssikkerhet

Databehandler skal ha tilfredsstillende informasjonssikkerhet for å oppfylle kravene som fremkommer av rettsgrunnlaget.

Eventuelle nye krav til informasjonssikkerhet som måtte følge av endringer i rettsgrunnlaget, skal oppfylles. Databehandleren plikter å implementere eventuelle endringer/ tillegg etc. som er nødvendig for å oppfylle nye krav før endringene trer i kraft.

Databehandler skal fortløpende ved hjelp av planlagte og systematiske, organisatoriske og tekniske tiltak, sikre tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet i forbindelse med behandling av informasjonen.

Databehandler kan ikke endre avtalte, normale informasjonssikkerhetstiltak uten at den behandlingsansvarlige er blitt skriftlig informert og skriftlig har godkjent endringen. Endringer kan kun nektes på saklig grunnlag.

Må databehandler foreta endring i sine informasjonssikkerhetstiltak som følge av akutte endringer i risiko/trusselbildet, skal behandlingsansvarlig varsles om dette uten ugrunnet opphold. Databehandler skal skriftlig informere behandlingsansvarlig om endringen(e) som er foretatt og hvordan risiko/ trusselbildet er endret, innen 3 virkedager fra endring er foretatt.

6.1. Autorisasjon, autentisering og logging

Databehandler skal ha rutiner for autorisering og avvikling av autorisasjon av alt personell som skal ha tilgang til behandlingsansvarliges informasjon. Som et minimum skal autorisasjonen angi hvilke IKT-systemer leverandørens personell, til enhver tid har lovlig tilgang til og hvilke operasjoner disse har lov til å utføre.

Databehandler skal i tillegg til enhver tid ha en oppdatert oversikt over hvilke medarbeidere hos databehandleren og eventuelle underleverandører og tredjeparter/ samarbeidspartnere som har tilgang til den informasjon som behandles. Denne oversikten skal på forespørsel forelegges den behandlingsansvarlige innen rimelig tid.

Alle med tjenstlig tilgang til den informasjon som lagres, skal autentiseres med en unik identitet, og alle oppslag, editeringer, endringer og sletting av informasjon, skal logges.

Også andre hendelser av betydning for informasjonssikkerheten og eventuelle forsøk på uautorisert tilgang skal logges.

Tilsvarende skal logger beskyttes mot uautoriserte endringer.

Loggene skal oppbevares i minst 12 måneder.

6.2. Konfidensialitet

For å sikre konfidensialitet skal databehandler sikre at informasjonen kun er tilgjengelig for de som etter avtale mellom behandlingsansvarlig og databehandler skal ha tilgang. Herunder skal det etableres funksjonalitet som hindrer uautorisert tilgang til systemer og informasjon og/eller utlevering av informasjon.

Det skal kun gis tilgang til den del av informasjonen som den aktuelle person har tjenstlig behov for å se/ha tilgang til.

Databehandler skal hindre uautorisert tilgang til fysiske lokasjoner og utstyr som brukes til behandling av informasjon på vegne av behandlingsansvarlig.

6.2.1. Ulike behandlingsansvarlige / separasjon

Databehandler skal sikre at informasjonen ikke sammenblandes med informasjon som behandles på vegne av andre behandlingsansvarlige.

6.3. Integritet

For å sikre integritet skal databehandler sikre at informasjon ikke uautorisert eller utilsiktet endres eller slettes.

Databehandler skal benytte og vedlikeholde anerkjente mekanismer for beskyttelse mot ondsinnet kode- og datainnbrudd.

6.3.1. Retting

Databehandler plikter å rette informasjon etter skriftlig pålegg fra behandlingsansvarlig.

6.4. Tilgjengelighet

Databehandler plikter å sikre tilgang til informasjonen, herunder å iverksette tiltak som forhindrer tilfeldig eller ulovlig ødeleggelse eller tap av informasjonen.

6.4.1. Sikkerhetskopiering og speiling av informasjon

Databehandler skal ta sikkerhetskopi daglig, ukentlig og månedlig av all informasjon som lagres, herunder informasjon som har betydning for informasjonssikkerheten (f.eks. konfigurasjonsdata, logger o.l.).

Databehandler skal lagre sikkerhetskopiene på en annen fysisk lokasjon enn originaldataene.

6.4.2. Sletting

Sletting av informasjon skal utføres av databehandler, etter skriftlig avtale med den behandlingsansvarlige, og etter avtalte rutiner.

Det skal finnes funksjonalitet som sikrer mulighet for tilgangsstyring til informasjonen i ulike tidshorisonter for ulike brukergrupper, ut fra de forskjellige brukergruppenes ulike tjenstlige behov for å se informasjonen over tid.

Det skal finnes funksjonalitet som muliggjør sletting av data på grunnlag av dataens alder, ut fra rettslig plikt til å lagre informasjon i visse tidsintervall/ slette informasjon det ikke lengre finnes tjenstlig behov for å behandle og derved har plikt til å slette.

7. Dokumentasjon

Databehandler skal dokumentere alle rutiner og alle tiltak som er iverksatt for å oppfylle kravene som fremkommer av rettsgrunnlaget og av denne databehandleravtalen, herunder kravene til informasjonssikkerhet.

Databehandler plikter skriftlig å varsle behandlingsansvarlig når det foretas endringer i dokumentasjonen som kan ha betydning for informasjonssikkerheten. Samtlige versjoner av dokumentasjonen skal i hele avtaleperioden være tilgjengelig på forespørsel fra behandlingsansvarlige eller aktuelle tilsynsmyndigheter.

All dokumentasjon med betydning for informasjonssikkerhet skal lagres i minst 5 år fra utløpet av kontrakten.

8. Håndtering av risiko og avvik

8.1. Risikohåndtering

Databehandler skal regelmessig og minimum hver 12 måned dokumentere eget fastsatt akseptabelt risikonivå. Dokumentasjonen skal fremlegges for behandlingsansvarlig på oppfordring.

Databehandler skal videre gjennomføre og dokumentere utført risikovurderinger minimum 1 gang per år. Resultatet av risikovurderinger overleveres behandlingsansvarlig på oppfordring.

Avdekker risikovurderingene avvik/brudd på personopplysningssikkerheten i henhold til rettsgrunnlaget, forsvarlig informasjonssikkerhet og/eller annen gjeldende norsk rett som omhandler informasjonssikkerhet, plikter databehandler for egen regning og på eget initiativ å utbedre disse snarest.

Databehandler plikter tilsvarende å oppdatere/dokumentere eget fastsatt akseptabelt risikonivå og gjennomføre/dokumentere ny risikovurdering etter hendelser, endringer av betydning for informasjonssikkerheten og/eller hvis det avdekkes nye sårbarheter mv. som er av betydning for informasjonssikkerheten.

8.2. Avvikshåndtering/brudd på personopplysningssikkerheten

Databehandler skal kontinuerlig registrere og rapportere avvik/brudd på personopplysningssikkerheten/sikkerhetshendelser iht. kravene i rettsgrunnlaget.

Ved alvorlige avvik/brudd på personopplysningssikkerheten/sikkerhetshendelser, eller ved begrunnet mistanke om dette, skal behandlingsansvarlig varsles umiddelbart. Databehandler skal omgående underrette behandlingsansvarlig dersom vedkommende mener at en instruks er i strid med rettsgrunnlaget eller andre bestemmelser om vern av personopplysninger.

Avviksmelding/ melding om brudd på personopplysningssikkerheten skal skje ved at databehandler melder avviket til behandlingsansvarlig. Behandlingsansvarlig har ansvaret for at avviksmelding/ melding om brudd på personopplysningssikkerheten sendes Datatilsynet.

Enhver bruk av informasjonssystemet som er i strid med databehandlers rutiner, denne databehandleravtalen, behandlingsansvarliges instrukser og/eller rettsgrunnlaget, samt ethvert sikkerhetsbrudd, skal behandles som et avvik/ brudd på personopplysningssikkerheten.

Databehandler skal ha på plass rutiner og systematiske tiltak for å avdekke og følge opp avvik/ brudd på personopplysningssikkerheten, herunder tiltak for å gjenopprette normaltilstand, fjerne årsaken til avviket/ bruddet på personopplysningssikkerheten og forhindre gjentakelse.

Databehandler skal, uten ugrunnet opphold etter at avviket /brudd på personopplysningssikkerheten/ sikkerhetshendelsen eller mistanke om avvik/ brudd på personopplysningssikkerheten/ sikkerhetshendelse ble oppdaget, rapportere avviket/ bruddet på personopplysningssikkerheten skriftlig til behandlingsansvarlig. Rapporten skal omfatte en beskrivelse av avviket/ bruddet på personopplysningssikkerheten, samt opplysninger om hvilke tiltak databehandler har iverksatt for å gjenopprette normaltilstand, fjerne årsaken til avviket/ bruddet på personopplysningssikkerheten og forhindre gjentakelse.

Databehandler skal gi behandlingsansvarlig alle nødvendige opplysninger for å kunne gi avviksmelding/ melding om brudd på personopplysningssikkerheten til aktuell tilsynsmyndighet(er), samt for å kunne besvare eventuelle spørsmål fra og etterleve eventuelle pålegg fra denne/ disse. Tilvarende skal det gis nødvendige opplysninger for å kunne gjennomføre varsling til de registrerte.

9. Revisjoner

9.1. Sikkerhetsrevisjoner

Databehandler plikter å gjennomføre sikkerhetsrevisjoner på infrastruktur, hardware og software, samt på andre enheter, funksjoner, systemer og lignende som omfattes av denne databehandleravtalen. Testene skal omfatte så vel tekniske tester som gjennomgang av dokumentasjon etc.

Det kan benyttes uavhengig tredjepartsrevisor til gjennomføringen av revisjonen.

Revisjon skal minimum gjennomføres 1 gang per år, samt i forbindelse med utbedring etter alvorlige hendelser, større endringer av betydning for informasjonssikkerheten, avdekking av nye alvorlige sårbarheter mv.

Sikkerhetsrevisjonen skal minimum omfatte gjennomgang av alle punkter i databehandlers virksomhet som er relevant for å avdekke om databehandler har et forsvarlig sikkerhetsnivå som oppfyller alle relevante krav i rettsgrunnlaget/ denne databehandleravtalen. Dette omfatter alle deler av databehandlers virksomhet som kan være av betydning for behandlingsansvarliges informasjonssikkerhet i de leveranser som databehandler i henhold til kontrakten utfører på vegne av behandlingsansvarlig.

Resultatet av revisjonen skal forelegges behandlingsansvarlig umiddelbart etter gjennomføring av revisjonen.

Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som ikke oppfyller ovenstående krav, skal dette behandles som avvik/ brudd på personopplysningssikkerheten.

Avdekker revisjonen at databehandler ikke oppfyller kravene i denne databehandleravtalen, plikter databehandleren å foreta nødvendige utbedringer umiddelbart.

Revisjonen skjer for databehandlers regning.

9.2. Revisjoner av etterlevelse av rettsgrunnlaget/denne databehandleravtalen

Behandlingsansvarlig har rett til for å kontrollere etterlevelsen av rettsgrunnlaget/denne databehandleravtalen. Dette gjelder både behandlingsansvarliges egne undersøkelser/kontroll og gjennom bruk av uavhengig revisor å foreta revisjoner hos databehandler og dennes underleverandører og tredjeparter/ samarbeidspartnere mv.

Databehandler plikter i denne sammenheng å fremlegge interne og eksterne revisjonsrapporter, interne prosedyrer, rutiner, sikkerhetsdokumentasjon mv.

Partene bærer sine egne kostnader i forbindelse med slik revisjon.

Etter nærmere avtale kan behandlingsansvarlig akseptere revisjonsrapport fra revisjon gjennomført av databehandler, gjennom f.eks. bruk av anerkjent uavhengig tredjepartsrevisor.

10. Særlig om taushetsbelagt informasjon

For annen taushetsbelagt informasjon som ikke er personopplysninger, plikter databehandler å sikre at behandling skjer i henhold til de retningslinjene i rettsgrunnlaget som gjelder for behandling av sensitive personopplysninger (så langt disse passer). Dette gjelder så vel taushetsplikt som følger av lov som taushetsplikt som følger av avtale.

11. Avtalens varighet

Avtalen gjelder så lenge databehandler og dennes underleverandører / tredjeparter/samarbeidspartnere behandler informasjon på vegne av behandlingsansvarlig. Den gjelder også for eventuell informasjon som måtte forefinnes hos databehandler etter kontraktens/avtalens opphør.

12. Mislighold og pålegg om stans

Ved brudd på denne databehandleravtalen og/ eller rettsgrunnlaget, kan behandlingsansvarlig og aktuelle tilsynsmyndigheter pålegge databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning

Hvis det foreligger mislighold av denne databehandleravtalen, kan den behandlingsansvarlige ved skriftlig varsel kreve at databehandler utbedrer forholdet innen en rimelig frist satt av behandlingsansvarlig.

Dersom forholdet ikke bringes i orden innen fristens utløp, vil behandlingsansvarlig ha adgang til å heve kontrakten med øyeblikkelig virkning.

Ved et vesentlig mislighold, kan behandlingsansvarlig uansett heve kontrakten med øyeblikkelig virkning.

13. Erstatning

Partene er enige om at det generelle prinsippet om ansvarsfordeling mellom partene i forbindelse med overtredelsesgebyr eller tvangsmulkt pålagt av relevante tilsynsmyndigheter eller krav reist av de registrerte under denne databehandleravtalen, er basert på at hver enkelt part må oppfylle sine egne forpliktelser i henhold til rettsgrunnlaget.

En part som blir idømt erstatningsansvar på grunn av brudd på personopplysningsloven eller annet regelverk som gjennomfører eller presiserer personvernforordningens (forordning 2016/679), kan uten hinder av ansvarsbegrensningen kreve regress i samsvar med personvernforordningen artikkel 82.

Partene er hver for seg ansvarlige for overtredelsesgebyr ilagt i henhold til personvernforordningens art. 83.

14. Opphør av Kontrakten

Ved opphør av kontrakten plikter databehandler, etter den behandlingsansvarliges valg, å tilbakelevere og/eller slette all informasjon som er mottatt på vegne av den

behandlingsansvarlige og som omfattes av kontrakten og denne databehandleravtalen. Dette skal gjøres snarest, og senest innen 2 dager etter opphøret.

Ved utløpet av kontrakten skal sikkerhetskopier og nødvendig programvare for å lese disse overlates til behandlingsansvarlig uten ytterligere krav på vederlag. Forutsetter avlesing flere generasjoner programvare, skal alle aktuelle versjoner medfølge.

Dersom behandlingsansvarlig initierer endring av databehandleravtalen og dette medfører kostnader for databehandler, dekkes kostnadene av behandlingsansvarlig.

14.1. Sletting

Databehandler skal, etter overlevering av informasjon ved kontraktens opphør og etter at behandlingsansvarlig har bekreftet mottak, foreta sikker sletting eller forsvarlig destruering av all informasjon og alle dokumenter, data, disketter, cd-er mv, som inneholder informasjon som omfattes av kontrakten/denne databehandleravtalen. Dette gjelder også for eventuelle sikkerhetskopier.

Sletting skal foregå ved hjelp av verktøy godkjent av Nasjonal sikkerhetsmyndighet eller med mekanismer som gir tilsvarende sikkerhet.

Databehandler skal skriftlig dokumentere at sikker sletting og/eller destruksjon er foretatt i henhold til denne databehandleravtalen innen rimelig tid etter kontraktens opphør.

Meddelelse om sletting og destruksjon skal sendes til:

personvernombud.ski@ski.kommune.no, merket «Meddelelse om sletting av data, saksnummer xx/xxxx».

Ved opphør av avtalen plikter dataleverandøren å avvikle alle tilganger til behandlingsansvarliges data.

15. Meddelelser

Meddelelser etter denne databehandleravtalen skal sendes skriftlig til: personvernombud.ski@ski.kommune.no

og merkes «Databehandleravtale avtale saksnr. xx/xxxx».

16. Lovvalg og verneting

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

***

Denne avtale er elektronisk signert sammen med øvrige kontraktsdokumenter.

Ski kommune

Bilag D1 Behandlingens formål, opplysninger og behandlinger

Typer personopplysninger og taushetsbelagt informasjon som behandles iht. denne databehandleravtalen

Tabellene oppdateres fortløpende.

[*dato/måned/år*]

Formål

Formålet med databehandlers behandling av personopplysninger på vegne av Ski kommune er:

- [beskriv formålet eller hensikten med behandlingen]

- Her bør det også vises til relevant, kommersiell avtale [kontrakten eller hovedavtalen]

Navn på tjeneste	Formålet med behandlingen	Varigheten av behandlingen

Behandlingens lovlighet

Personopplysningene er samlet med utgangspunkt i:

Vilkår	Kryss
Samtykke	
Oppfylle en avtale	
Rettslig forpliktelse	
Verne om en persons vitale interesser	

Allmenn interesse eller pålagt oppgave	
Nødvendig iht den registrertes interesse	
Opplysninger som personen selv har offentliggjort	
Forebyggende medisinsk formål	
Allmenn folkehensyn	
Arkivformål	

Type behandling

Behandlingen av personopplysninger på vegne av den behandlingsansvarlige vil primært gjelde:

- [beskriv behandlingen]

Følgende behandlinger omfattes av avtalen: *[her listes opp hvilke behandlinger av personopplysninger som omfattes – se eksempler nedenfor]*

Behandling	**Behandlingsaktiviteter**
Innsamling	
Registrering	
Organisering	
Strukturering	
Lagring	
Tilpasning eller endring	
Gjenfinning	
Sammenstilling	
Sletting eller tilintetgjøring	
Utlevering/Overføring	

Typer av personopplysninger

Behandlingen omfatter følgende typer av personopplysninger om de registrerte:

- [beskriv de personopplysningene/type som behandles]

[Det er ikke nødvendig å være veldig detaljert i beskrivelsen av hvilke opplysninger som skal behandles, men kun type/kategori av opplysninger]. [1]

I forordningen, art. 9 nr. 2 og 3 gis en oversikt over når visse opplysninger kan behandles.

Personopplysninger	Helseopplysninger
Navn, alder og fødselsnummer Adresse Telefonnummer og e-postadresse Opplysninger om elevenes underveis- og sluttevalueringer Fravær og anmerkninger Faglig progresjon Spesielle undervisningsbehov Atferdsmønstre og sosiale evner Kommunikasjon mellom elever Kommunikasjon mellom lærer og elev Kommunikasjon mellom barnehage og hjem Informasjon om allergier Logg fra elevenes bruk av skolens nettverk Bilder, videoer eller lydfiler av elever IP adresse	

D. Kategorier av registrerte

Kategorier av registrerte

Behandlingen omfatter følgende kategorier av registrerte:

[1] Listen er ikke uttømmende, men som ett forslag for kommunens tjenesteproduksjon

- [beskriv kategorien av registrerte]

Følgende kategorier av personer behandles det opplysninger om (registrerte): [her listes opp hvilke kategorier av registrerte som omfattes – se eksempler nedenfor]

Kategorier av registrerte		
Pasienter	Helsepersonell	Leverandører
Barn	Ansatte	Nøkkelpersoner
Foreldre	Tidligere ansatte	Medlemmer
Innbyggere	Ansatte i samarbeidende firma	
Fullmektiger	Kunder til kommunal tjenesteleveranser	

2

Varighet

Databehandlers behandling av personopplysninger på vegne av Ski kommune kan ikke påbegynnes før ikrafttredelse av denne avtalen. Behandlingen har følgende varighet:

- [beskriv hvor lang varighet behandlingen har]

[2] Listen er ikke uttømmende, men som ett forslag for kommunens tjenesteproduksjon

Ski kommune

Bilag D2 Oversikt over databehandlers underleverandører og tredjeparter/samarbeidspartnere

Selskap	Rolle	Org. nr.	Leveranseområde	Adresse	Kontaktperson	Epost kontakt-person

Ski kommune

Bilag D3 Tiltredelseserklæring til databehandleravtale inngått mellom hovedleverandør/ databehandler og behandlingsansvarlig.

Som underleverandør/ tredjepart/ samarbeidspartner til hovedleverandør/ databehandler eller noen av dennes underleverandører, bekrefter vi å ha påtatt oss ansvar og forpliktelser i henhold til vilkårene i databehandleravtale inngått xx.xx.xxxx.

Dersom våre evt. underleverandører/ tredjeparter/ samarbeidspartnere skal behandle informasjon, blir underleverandøren/ tredjeparten/ samarbeidspartneren også databehandler i databehandleravtalens forstand og skal tilsvarende undertegne på et likelydende bilag til databehandleravtale. Databehandleren i databehandleravtalen vil da bli behandlingsansvarlig overfor underleverandøren/ tredjeparten/ samarbeidspartneren, og sistnevnte gruppering blir databehandler overfor databehandler i databehandleravtalen.

Alle evt. underleverandører/ tredjeparter/ samarbeidspartnere har selvstendig ansvar og identiske forpliktelser for å oppfylle kravene i databehandleravtalen som vi bekrefter å ha fått utlevert en kopi av.

Denne avtale er elektronisk signert.
eller
Denne avtale er i 3 – tre eksemplarer, hvorav partene har hvert sitt og hvor et eksemplar oversendes behandlingsansvarlig i kontrakten.

Sted:	Sted:
Dato:	Dato:
Dataeksportør/ Databehandler	Dataimportør/ Underleverandør / Tredjepart/Samarbeidspartner
_____	_____
Navn	Navn