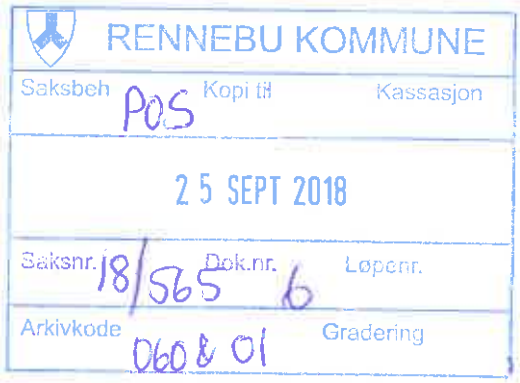
Databehandleravtale til tjenesteavtale (SSA-L)

Avtalen omhandler også håndtering av taushetsbelagt informasjon og data.

mellom virksomhet Rennebu kommune
org. nr. 940 083 672
.....
som Behandlingsansvarlig

og virksomhet KS
org. nr. 971 032 146
.....
som Databehandler



Denne avtalen inngår som bilag 3 i «Avtale om bruk av KS FIKS-Meldingsformidler», senere kalt «Leveranseavtalen», og erstatter tidligere bilag 3.

Denne avtale er i 2 – to eksemplarer, hvorav partene har hvert sitt.

For Databehandler/Hovedleverandør
Sted: Oslo
Dato: 1. september 2018

Astrid Øksenvåg

Versjon: 1.0

For Behandlingsansvarlig/Kunde:
Sted: Berkåk
Dato: 12. Sept. 18

Rådmann - Per Øivind Sundell

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
- Personopplysningsloven av 2018-06-15

I det følgende vil disse lovverkene 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 behandling 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 Leveranseavtalen, herunder avtaler mellom Databehandler og dennes underleverandører eller tredjeparter/samarbeidspartnere og eventuelle personvernvilkår disse måtte ha.

Ved eventuell motstrid i denne avtalen skal den generelle avtaleteksten gå foran bilagene, med følgende unntak:

- Bilag med endringer til den generelle avtaleteksten gis forrang
- Bilag med sikkerhetsbestemmelser gis forrang

3 Omfanget av behandlingen

3.1 Typer personopplysninger som behandles iht. denne databehandleravtalen

KS SvarUt formidler korrespondanse mellom kunden og dens part. Nær alltid i PDF format. Korrespondansen kan potensielt inneholde alle typer personopplysinger.

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.

Det behandles:

- Korrespondanse mottas elektronisk fra kunden og videreformidles elektroniske til en part
- Korrespondanse mottas elektronisk fra kunden og sendes til trykking og forsendelse på papir til parten og parten ikke kan motta elektronisk
- Om parten (innbygger/virksomhet) ønsker og samtykker til et samlet elektronisk arkiv over all korrespondanse opprettes et arkiv i KS-FIKS kalt MinSide
- Korrespondanse mottas elektronisk fra en part og videreformidles elektroniske kunden

Det forutsettes videre at Databehandler bruker fiktive testdata til utvikling og feilsøking så langt dette er mulig. Brukes skarpe data eller pseudonymiserte data gjelder bestemmelsene i denne databehandleravtalen uavkortet.

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 Behandlingsansvarlig utarbeide et endringsbilag hvor instruksen som beskriver endringen i behandlingsformålet legges inn.

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

4 Partenes plikter og rettigheter

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 Leveranseavtalen.

4.2 Databehandler skal ikke:

a. behandle personopplysninger for andre formål eller i større grad enn det som følger av denne Avtalen, Tjeneste/oppdragsavtale og eventuelle senere skriftlige avtaler mellom partene;

b. behandle personopplysninger utover det som er nødvendig for å oppfylle Databehandlers forpliktelser i henhold til de til enhver tid gjeldende avtaler;

c. utlevere, overlate eller overføre personopplysninger i noen form på eget initiativ med mindre det er avtalt på forhånd med Behandlingsansvarlig eller Behandlingsansvarlig har godkjent dette skriftlig;

d. samle inn fra eller overføre personopplysninger til en tredjepart;

e. behandle personopplysninger de får tilgang eller adgang til gjennom oppdraget fra Behandlingsansvarlig på annen måte enn hva som er angitt i denne Avtalen, Tjeneste/oppdragsavtale og eventuelle senere skriftlige avtaler mellom partene.

4.3 Databehandler skal:

a. ha løpende kontroll på alle kategorier av behandlingsaktiviteter utført på vegne av Behandlingsansvarlig;

b. gi Behandlingsansvarlig tilgang til og innsyn i personopplysninger som behandles hos Databehandleren;

c. føre og vedlikehold en oversikt over alle opplysninger og behandlinger eller dersom det er relevant, protokoll over sine egne behandlingsaktiviteter i henhold til personvernforordningen artikkel 30;

d. treffe alle rimelige tiltak for å sikre at personopplysningene til enhver tid er korrekte og oppdaterte;

e. etablere rutiner for å slette informasjon når den ikke lenger er nødvendig ut fra formålet med behandlingen og slette informasjon i henhold til fastsatte rutiner og retningslinjer;

f. ha rutiner for og teknisk mulighet til å begrense behandlingen av den registrertes personopplysninger dersom den registrerte ønsker det med hjemmel i gjeldende lovgivning;

g. påse at samtlige personer som gis tilgang til personopplysninger som behandles på vegne av Behandlingsansvarlig er kjent med denne Avtalen og gjeldende avtaler mellom partene, og er underlagt disse avtalenes bestemmelser;

h. sikre at krav til innebygd personvern og personvern som standardinnstilling innfris i Databehandlers løsninger. Dette inkluderer å bygge inn funksjonalitet for å oppfylle personvernprinsipper samt funksjonalitet for å sikre den registrertes rettigheter;

i. gi Behandlingsansvarlig nødvendig bistand slik at Behandlingsansvarlig skal kunne oppfylle sine forpliktelser overfor de registrerte;

j. samarbeide med og bistå Behandlingsansvarlig ved oppfyllelse av de registrertes rettigheter knyttet til tilgang til opplysninger, herunder å svare på anmodninger fra den registrerte med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III;

k. omgående underrette den Behandlingsansvarlige dersom Databehandler mener at en instruks er i strid med personvernforordningen eller andre bestemmelser om vern av personopplysninger;

l. bistå Behandlingsansvarlig for å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 35-36 som omhandler vurdering av personvernkonsekvenser og forhåndsdrøftinger med Datatilsynet.

4.4 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.

4.5 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 Leveranseavtalen 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.

4.6 Internkontrollsystem / sikkerhetsdokumentasjon

Databehandler skal oppfylle de krav til sikkerhetstiltak som stilles i Rettsgrunnlaget.

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 Leveranseavtalen innen rimelig tid.

4.7 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 som er lovlig i henhold til Rettsgrunnlaget.

4.8 Ivaretakelse av de registrertes rettigheter

Databehandler plikter å bistå den Behandlingsansvarlige ved ivaretakelse av den registrertes rettigheter etter Rettsgrunnlaget.

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.

Ved bruk av underleverandør og/eller tredjepart blir også underleverandør / tredjepart/samarbeidspartnere å anse som Databehandler etter denne databehandleravtalen.

Oversikt over aktuelle underleverandører / tredjeparter/samarbeidspartnere ved avtalens oppstart, som er godkjent av Behandlingsansvarlig, ligger som bilag 1 til denne databehandleravtalen.

Databehandler kan ikke benytte underleverandører og 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 Leveranseavtalen og fremlegge denne for Behandlingsansvarlig på forespørsel.

Underleverandør / tredjeparter/samarbeidspartnere plikter å oppfylle alle krav i denne Databehandleravtale og skal signere Databehandleravtalens bilag 2. Databehandleravtalens bilag 2 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 2 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 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 databehandleravtale, 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 Leveranseavtalen.

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 *(maks intervall er hver tolvte måned)*. Resultatet av risikovurderinger overleveres Behandlingsansvarlig uten ugrunnet opphold.

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 ved 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.

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 Databehandleravtale, 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 og senest innen 24 timer 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 skal benyttes uavhengig tredjepartsrevisor til gjennomføringen av revisjonen.

Revisjon skal minimum gjennomføres 1 ganger per år *(maks intervall er hver tolvte måned)*, 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 databehandleravtale. Dette omfatter alle deler av Databehandlers virksomhet som kan være av betydning for Behandlingsansvarliges informasjonssikkerhet i de leveranser som Databehandler i henhold til Leveranseavtalen 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 gjennom bruk av uavhengig revisor å foreta revisjoner hos Databehandler og dennes underleverandører og tredjeparter/samarbeidspartner for å kontrollere etterlevelsen av Rettsgrunnlaget / denne databehandleravtalen.

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

Etter nærmere avtale kan Behandlingsansvarlig akseptere revisjonsrapport fra revisjon gjennomført av Databehandler, gjennom 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 eventuelle Informasjon som måtte forefinnes hos Databehandler etter Leveranseavtalens avtalens opphør.

12 Mislighold og pålegg om stans

Ved brudd på denne databehandleravtale 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 Leveranseavtalen med øyeblikkelig virkning.

Ved et vesentlig mislighold, kan Behandlingsansvarlig uansett heve Leveranseavtalen med øyeblikkelig virkning.

13 Erstatning

Behandlingsansvarlig har krav på erstatning for tap som følge av at Databehandler ikke har overholdt sine forpliktelser i henhold til denne databehandleravtalen.

Dette omfatter også Behandlingsansvarliges rett til å få tilbakebetalt eventuell utbetalt erstatning til den skadelidte ved et solidarisk ansvar og evt. overtredelsesgebyrer e.l. som Behandlingsansvarlig blir pålagt av aktuelle tilsynsmyndigheter og som kan tilbakeføres til forhold på Databehandlers hånd.

14 Ved opphør av Leveranseavtalen

Ved opphør av Leveranseavtalen plikter Databehandler å tilbakelevere all Informasjon som er mottatt på vegne av den Behandlingsansvarlige og som omfattes av Leveranseavtalen og denne Databehandleravtalen, til Behandlingsansvarlig, eller den som den Behandlingsansvarlige utpeker. Dette skal gjøres snarest, og senest innen 30 dager etter opphøret.

Ved utløpet av Leveranseavtalen 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.

14.1 Sletting

Databehandler skal, etter overlevering av Informasjon ved Leveranseavtalens 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 Leveranseavtalen/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 Leveranseavtalens opphør.

Meddelelse om sletting og destruksjon skal sendes til Behandlingsansvarlig.

Ved opphør av avtalen plikter Leverandøren å avvikle alle tilganger til Behandlingsansvarliges data.

15 Meddelelser

Meddelelser etter denne databehandleravtalen skal sendes skriftlig til virksomheten og merkes «Databehandleravtale for «Avtale om bruk av KS SvarUt Meldingsformidler»,

16 Lovvalg og verneting

Avtalen er underlagt norsk rett og Behandlingsansvarliges verneting. Dette gjelder også etter opphør av avtalen.

Bilag 1 Oversikt over Databehandlers underleverandører og tredjeparter/samarbeidspartnere

Det er inngått avtale med følgende underleverandører:

- Bergen kommune for drift av applikasjonen.
- Grafisk Digital AS for utskrift, konvoluttering, frankering og postlegging av forsendelser som skal sendes som brevpost.
- Brønnøysundregistrene for bruk av Altinn som meldingsformidler
- Linus AS for forsendelser av SMS
- Difi for bruk av ID-porten
- Difi for bruk av Sikker Digital Post
- Difi for bruk av eSignering