DATABEHANDLERAVTALE

mellom
Trondheim kommune
……
som Behandlingsansvarlig
og
XX
…….
Som Databehandler

Denne avtalen er knyttet til xxxxxx avtale av xxxxxxx mellom partene (Leveranseavtalen)

Versjon: XX

<MERKNAD: ALL TEKST I RØDT MÅ TILPASSES DET ENKELTE AVTALEFORHOLDET>

Mal sist oppdatert: 24.01.2019

1. Formålet med Databehandleravtalen

Formålet med denne databehandleravtalen er å regulere Databehandlers behandling av personopplysninger på vegne av den Behandlingsansvarlige i tråd med kravene i personopplysningsloven og personvernforordningen.. Avtalen skal være et ledd i oppfyllelsen av art. 28 i personvernforordningen. I det følgende vil disse regelverkene bli betegnet som ”Personvernreglene”.

Avtalen regulerer også partenes rettigheter og plikter ved behandling av data og informasjon som er underlagt taushetsplikt i medhold av annet regelverk eller avtale. Avtalen skal sikre at personopplysninger eller annen taushetsbelagt informasjon ikke brukes urettmessig eller kommer uvedkommende 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.

2. Definisjoner

Følgende definisjoner, som gjøres gjeldende i denne avtalen, fremgår av personvernforordningens art 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 onlineidentifikator 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.

Nr 12. “Brudd på personopplysningssikkerheten” - et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagre
t, eller på annen måte behandlet.

3. 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 skal den generelle avtaleteksten gå foran bilagene, med følgende unntak:

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

4. Avtalens omfang

Avtalen gjelder levering av oppdrag / tjenester med behandling av personopplysninger.

4.1 Typer personopplysninger og taushetsbelagt informasjon som behandles iht. denne databehandleravtalen

(Her må avtalepartene liste opp aktuelle typer informasjon som behandles – denne listen må tilpasses de opplysningene som behandles - opplysningene skal også være registrert i Trondheim kommunes oversikt over behandlinger av personopplysninger.

- ***Personopplysninger:***
  - ***Kategorier av registrerte***
    - ***eks: Ansatte***
    - ***eks: Elever***
    - ***eks: personer som søker jobb***
  - ***Kategorier av personopplysninger***
    - ***Eks: kontaktinformasjon som navn, epostadresse, telefon***
    - ***Eks: finansielle opplysninger, som lønn, kontonummer, kredittkortnummer***
    - ***Eks: dokumenter (den behandlingsansvarlige er ansvarlig for at dokumenter behandles iht. gjeldende regelverk***
    - ***Eks: helseopplysninger***
    - ***Eks: ip-adresser, nettverksadresser***
    - ***Eks: lokalisering av personer***
  - ***Særlige kategorier av personopplysninger (databehandler skal behandle følgende typer sensitive personopplysninger)***
    - ***Rase, etnisitet, politisk eller filosofisk tilhørighet eller***
    - ***religion***
    - ***At en person har vært eller er siktet/dømt for kriminalitet***
    - ***Helseopplysninger (hvis Kunden registrerer det)***
    - ***Seksuell orientering***
    - ***Fagforeningsmedlemskap***
    - ***Genetisk eller biometrisk data***
  - ***Informasjon underlagt taushetsplikt:***
    - *Lovbestemt taushetsplikt, Informasjon som kan unntas offentlighet – Offentlighetsloven kap. 3, Avtalefestet taushetsplikt*
  - ***Sikkerhetsgradert informasjon***
  - ***Intern informasjon uten restriksjoner/uten innsynsrett***
  - ***Informasjon som kun kan lagres i nærmere angitte land – må beskrives nærmere hva som omfattes og aktuelle land***
  - ***Informasjon som må lagres i Norge – må beskrives nærmere hva som omfattes***

Ovennevnte typer informasjon vil i det følgende bli benevnt som ”Informasjonen”, med mindre aktuelt avtalepunkt bare berører enkelte av informasjonstypene.

4.2 Behandlingstyper omfattet av denne databehandleravtalen

(Her beskrives hva slags behandling som er aktuell i de applikasjoner som utvikles/driftes, vedlikeholdes, f.eks:

Transport, innsamling, registrering, sammenstilling, lesing, oppslag, bearbeiding, lagring, kobling, sletting og utlevering til databehandler av opplysninger/data. Disse behandlingstypene kan også gjennomføres i kombinasjon.
Om opplysningene skal kunne kobles med andre registre
.

5. 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.

Databehandler har ikke anledning til å overlate Informasjonen på noen måte til andre, dersom det ikke er en del av oppdraget/tjenesten, uten at det er avtalt skriftlig med Behandlingsansvarlig på forhånd.

6. Partenes plikter og rettigheter

Databehandler skal følge de rutiner og instrukser for behandlingen som Behandlingsansvarlig til enhver tid har bestemt skal gjelde.

Dersom Databehandler mottar instruks som Databehandler mener bryter med Personvernreglene, skal Databehandler umiddelbart informere Behandlingsansvarlig.

Databehandler plikter uten ugrunnet opphold å bistå Behandlingsansvarlig, slik at behandlingsansvarlig kan oppfylle de krav som fremkommer i Personvernreglene slik dette fremkommer til enhver tid.

6.1 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.

6.2 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 og innsyn i:

- 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.

6.3 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 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.

Taushetserklæringene skal gjøres tilgjengelig for Behandlingsansvarlig på forespørsel.

6.4 Internkontrollsystem / sikkerhetsdokumentasjon

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, plikten gjelder tilsvarende for uavhengig revisor og tilsynsmyndigheter.
Databehandler plikter å informere Behandlingsansvarlig dersom det foretas endringer i internkontrollsystemet eller sikkerhetsdokumentasjonen av betydning for Leveranseavtalen innen rimelig tid.

6.5 Overføring av data til utlandet

Informasjonen kan ikke uten skriftlig godkjenning fra Behandlingsansvarlig overføres til land utenfor EØS. Ved inngåelse av avtale om slik overføring skal Databehandler inngå ”EUs Model Contract Clauses” med Behandlingsansvarlig som eksportør, og overføringene være i henhold til disse bestemmelsene.

Dersom det avtales at deler eller hele oppdraget/tjenesten utføres i land utenfor EØS, skal Databehandleren på forhånd gi en skriftlig garanti for at det ikke foreligger noen myndighetskrav som hindrer oppfyllelse av kravene i denne avtalen.

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

6.6 Ivaretakelse av de registrertes rettigheter
Databehandler plikter å bistå den Behandlingsansvarlige ved ivaretakelse av den registrertes rettigheter etter Personvernreglene.

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

7. Bruk av underleverandør

Dersom Databehandler benytter seg av underleverandør eller tredjeparter / samarbeidsparter forblir Databehandler ansvarlig for deres behandling av Informasjonen.

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

Oversikt over aktuelle underleverandører og/eller 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 Behandlingsansvarlig. Behandlingsansvarlig har rett til å underkjenne valg av nye underleverandører og tredjeparter/samarbeidspartnere på saklig grunnlag.

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

Underleverandør/ tredjepart/ samarbeidspartner plikter å oppfylle alle krav i denne Databehandleravtale og skal signere Databehandleravtalens bilag 2. Dette bilag 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 Personvernreglene.

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

8. Informasjonssikkerhet

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

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.

Må databehandler foreta endring i sine informasjonssikkerhetstiltak som følge av akutte endringer i risikobildet/trusselbildet, skal Behandlingsansvarlig varsles om dette uten ugrunnet opphold.

Nærmere sikkerhetsbestemmelser følger av bilag 3 - Sikkerhetsbestemmelser.

9. Dokumentasjon

Databehandler skal dokumentere alle rutiner og alle tiltak som er iverksatt for å oppfylle kravene som fremkommer av Personvernreglene 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.

10. Håndtering av risiko og avvik

10.1 Risikohåndtering

Databehandler skal regelmessig og minimum hver **XX** måned, dokumentere eget fastsatt akseptabelt risikonivå. Dokumentasjonen skal fremlegges for Behandlingsansvarlig på oppfordring.

Databehandler skal videre, gjennomføre og dokumentere utførte risikovurderinger minimum en gang per år (vurder hyppigere intervall). Resultatet av vurderingene overleveres Behandlingsansvarlig uten ugrunnet opphold.

Avdekker risikovurderingene avvik/brudd på personopplysningssikkerheten i forhold til Personvernreglene, taushetsplikt, forsvarlig informasjonssikkerhet og/eller annen gjeldende rett som omhandler informasjonssikkerhet, plikter Databehandler for egen regning og på eget initiativ å utbedre disse snarest.

Medfører endringer i Personvernreglene eller endringer i risikobildet behov for tilpasninger/utbedringer som medfører kostnader på mer enn **XX%** av leveranseavtalens totale pålydende, dekkes **XX** av det overskytende av Behandlingsansvarlig..

Databehandler plikter tilsvarende å oppdatere/dokumentere eget fastsatt akseptabelt risikonivå og gjennomføre/dokumentere ny risikovurdering etter hendelser, endringer av betydning for informasjonssikkerheten.

10.2 Avvikshåndtering/ brudd på personopplysningssikkerheten

Enhver bruk av informasjonssystemet som er i strid med Databehandlers rutiner, denne databehandleravtale, Behandlingsansvarliges instrukser og/ eller Personvernreglene, samt ethvert sikkerhetsbrudd, skal behandles som et avvik

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

Ved alvorlige avvik/ brudd på personopplysningssikkerhet/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.

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/sikkerhetshendelsen ble oppdaget, rapportere avviket/bruddet 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 og forhindre gjentakelse.

Databehandler skal gi Behandlingsansvarlig alle nødvendige opplysninger for å kunne gi avviksmelding/melding om brudd på personopplysningssikkerheten til aktuell tilsynsmyndighet(er) i henhold til personvernforordningen art. 33, samt for å kunne besvare eventuelle spørsmål fra - og etterleve eventuelle pålegg fra denne/disse. Tilsvarende skal det gis nødvendige opplysninger for å kunne gjennomføre varsling til de registrerte.

11. Revisjoner

11.1 Sikkerhetsrevisjoner

Databehandler plikter å gjennomføre sikkerhetsrevisjoner på hardware og software, samt på andre enheter, funksjoner, systemer og lignende som omfattes av denne databehandleravtalen. Revisjonene skal omfatte så vel tekniske tester som gjennomgang av dokumentasjon etc. Plikten gjelder ikke i de tilfellene hvor arbeidene kun utføres på Kundens/Databehandlers eget utstyr.

Det skal benyttes uavhengig revisor til gjennomføringen av revisjonen.

Revisjon skal minimum gjennomføres **XX** ganger per år samt i forbindelse med utbedring etter alvorlige hendelser, større endringer av betydning for informasjonssikkerheten, avdekking av nye, alvorlige sårbarheter m.v.

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 Personvernreglene / 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.

11.2 Revisjoner av etterlevelse av Personvernreglene / denne databehandleravtalen

Behandlingsansvarlig har rett til å gjennomføre sikkerhetsrevisjoner hos Databehandler og dennes underleverandører og tredjeparter/ samarbeidspartner for å kontrollere etterlevelsen av Personvernreglene/ denne databehandleravtalen. Databehandler plikter i denne sammenheng å fremlegge interne og eksterne revisjonsrapporter, interne prosedyrer, rutiner, sikkerhetsdokumentasjon mv.

Revisjon kan utføres av Behandlingsansvarlig selv eller en uavhengig revisor utpekt av Behandlingsansvarlig.

Det kan særskilt avtales at revisjon gjennomføres av Databehandler, gjennom bruk av uavhengig revisor.

12. 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 Personvernreglene som gjelder for behandling av sensitive personopplysninger så langt det passer. Dette gjelder også for så vidt gjelder taushetsplikt som følger av lov og avtale.

13. 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 Leveranseavtalens opphør.

14. Mislighold, sanksjoner og pålegg om stans

Ved brudd på denne databehandleravtale og/eller Personvernreglene, 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 Behandlingsansvarlig 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 vesentlig mislighold kan Behandlingsansvarlig uansett heve Leveranseavtalen med øyeblikkelig virkning.

15. Erstatning

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

Partenes erstatningsansvar for skade som rammer den registrerte eller andre fysiske personer og som skyldes overtredelse av personvernforordningen (forordning 2016/679), personopplysningsloven med forskrifter eller annet regelverk som gjennomfører personvernforordningen, følger av bestemmelsene i personvernforordningen artikkel 82.

Erstatningsbegrensninger i Leveranseavtalen kommer ikke til anvendelse for ansvar som følger av personvernforordningen artikkel 82. Partene er hver for seg ansvarlige for overtredelsesgebyr ilagt i henhold til personvernforordningens (forordning 2016/679) art. 83.

16. 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 **XX** dager etter opphøret.

16.1 Sletting

Databehandler skal, etter overlevering av informasjon ved opphør og etter at Behandlingsansvarlig har bekreftet mottak, foreta sikker sletting eller forsvarlig destruering av all lagret informasjon og alle dokumenter, elektroniske lagringsmedier m.v., som inneholder Informasjon som som omfattes av Leveranseavtalen/denne databehandleravtalen. Dette gjelder også for eventuelle sikkerhetskopier.

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

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

17. Meddelelser

Meddelelse etter denne databehandleravtalen skal sendes skriftlig til **XXX** og merkes **XXX**

Varsel om avvik og brudd på personopplysningssikkerheten skal meldes til Trondheim kommunes personvernombud.

18. Lovvalg og verneting

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

***

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

For Databehandler/Hovedleverandør: For Behandlingsansvarlig/Kunde:
Sted: Sted:
Dato: Dato:

Bilag 1

Oversikt over Databehandlers underleverandører og tredjeparter/samarbeidspartnere

Selskap	Rolle	Org.nr.	Leveranseområde	Adresse	Kontaktperson	Epost kontaktperson

Bilag 2

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.XX.

Dersom våre eventuelle underleverandører / tredjeparter / samarbeidspartnere skal behandle Informasjon, blir underleverandøren / tredjeparter / samarbeidspartnere også Databehandler i Databehandleravtalens forstand og skal tilsvarende undertegne på et likelydende bilag til Databehandleravtalen.

Samtlige av eventuelle underleverandører / tredjeparter / samarbeidspartnere har selvstendig ansvar og identiske forpliktelser til å oppfylle i Databehandleravtalen som vi bekrefter å ha fått utlevert en kopi av.

***

Denne avtale er i 3 - tre - eksemplarer, hvorav partene har hvert sitt og hvor ett eksemplar oversendes behandlingsansvarlig/oppdragsgiver i Leveranseavtalen.

Sted:	Sted:
Dato:	Dato:
Databehandler:	underleverandør/tredjepart/ samarbeidspartner:
---	---
Navn:	Navn:

Bilag 3 - Sikkerhetsbestemmelser

<følgende sikkerhetskrav er tilpasset en enkel avtale med behandling av ikke-sensitive personopplysninger, hvor databehandler behandler eller har tilgang til opplysningene i egne systemer - for andre typer avtaler, eksempelvis service- og vedlikeholdsavtaler, sensitive opplysninger mv., - må egne kravsett benyttes.>

1. Autorisasjon, Autentisering og logging

Databehandler skal ha rutiner for autorisering og avvikling av autorisasjon av alt personell som skal ha tilgang til Behandlingsansvarliges/Kundens 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 tjenestelig tilgang til den informasjon som lagres, skal autentiseres med 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.
Logger skal oppbevares i minst **12** måneder.

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.

Leverandøren plikter å holde Kundens data atskilt fra eventuelle tredjeparters data for å redusere faren for beskadigelse av data og/eller innsyn i data. Med atskilt forstås at nødvendige tekniske tiltak som sikrer data mot uønsket endring og innsyn, er iverksatt og opprettholdt. Som uønsket endring og innsyn anses også tilgang fra

ansatte hos Leverandøren eller andre som ikke har behov for informasjonen i sitt arbeid for Kunden.

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

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

3 Integritet

For å ivareta nødvendig integritet skal Databehandler sikre at Informasjon ikke utilsiktet endres eller slettes.

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

4 Retting

Databehandler plikter å rette opp Informasjon etter skriftlig pålegg fra Behandlingsansvarlig.

5 Tilgjengelighet

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

6 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 (for eksempel, konfigurasjonsdata, logger o.l).

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

7 Sletting

Sletting av Informasjon skal utføres av Databehandler i samsvar med Personvernreglene etter den Behandlingsansvarliges skriftlige instruks/rutiner.

Leverandøren skal sikre at informasjonen kan slettes i tråd med forpliktelser i Personvernregelverket.

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