

(Erstatt med eigen kommune-logo)

Versjonsnummer: 2.0

**DATABEHANDLARAVTALE**

mellom

**Bærum kommune**

Org.nr.: 935 478 715

*Behandlingsansvarleg*

og

**[Namn på verksemda]**

Org.nr.: 000 000 000

*Databehandlar*

Datert: xx.xx.20xx

## Om avtalen

Denne databehandlaravtalen (heretter omtalt som "Avtalen") regulerer rettar og plikter mellom Behandlingsansvarleg og Databehandlar (heretter omtalt som "partane") etter gjeldande personvernlovgiving, her under Lov om behandling av personopplysningar av 15. juni 2018 nr. 38 (personopplysningsloven) og EUs personvernforordning 2016/679/EC av 27.april 2016 om vern av fysiske personar i samband med behandling av personopplysningar og om fri utveksling av slike opplysningar (General Data Protection Regulation) (heretter omtalt som "personvernforordninga");

Ved motstrid mellom regulering i Avtalen og dei rammene som følgjer av personvernforordninga eller annan relevant lovgiving, viker reguleringa i Avtalen.

Databehandlaravtalen erstattar eksisterande databehandlaravtale av DD.MM.ÅÅÅÅ

## Definisjonar

Omgrepa "personopplysningar", "behandling", "behandlingsansvarleg", "databehandlar" og "brot på personopplysningstryggleik" skal forståast slik dei er definerte i personvernforordninga artikkel 4.

"Avvik": brot på personopplysningstryggleik og bruk av informasjonssystemet i strid med fastlagte rutinar.

## Bakgrunn og føremål med Avtalen

Denne Avtalen er inngått mellom partane og skisserer dei generelle vilkåra for den behandlinga av personopplysningar som Databehandlar utfører på vegne av Behandlingsansvarleg.

Føremålet med Avtalen er å sikre behandlinga av personopplysningar på vegne av Behandlingsansvarleg slik at personopplysningane ikkje vert brukt ulovleg, urettmessig eller at opplysningane vert behandla på måtar som fører til uautorisert tilgang, endring, sletting, skade, tap eller gjort utilgjengelege.

## Omfang

Denne Avtalen vert å anvende på all behandling av personopplysningar som Databehandlar gjer på grunnlag av [*skriv namn på teneste/oppdragsavtale*] (heretter omtalt som "Teneste/oppdragsavtalen"). I tilfelle konflikt mellom denne Avtalen og Teneste/oppdragsavtalen, skal denne Avtalen gjelde.

Tenester som inngår i denne Avtalen er dei tenestene som inngår i Teneste/oppdragsavtalen og som inneber behandling av personopplysningar.

Denne Avtalen vil i tillegg gjelde for ytterlegare behandling av personopplysningar basert på eventuelle skriftlege avtalar mellom partane som vert inngått i løpet av denne Avtalen sin virkeperiode og som inneber at Databehandlar behandlar personopplysningar på vegne av Behandlingsansvarleg (heretter omtalt som "seinare skriftlege avtalar mellom partane").

Personopplysningar skal berre nyttast til dei føremåla som følgjer av denne Avtalen, Teneste/oppdragsavtalen, og seinare skriftlege avtalar mellom partane i den utstrekning det er strengt nødvendig for å gjennomføre og imøtekome krava i avtalane.

## Føremål med behandlinga, opplysningar og behandlingar

Føremålet med behandling av personopplysningar er [*hugs at ei kvar behandling må vere knytt til spesifikke og uttrykkeleg oppgjeve føremål*].

XX

Følgjande personopplysningar vert behandla: *[her listar ein opp kva personopplysningar som vert omfatta – sjå døme nedanfor].*

|  |  |
| --- | --- |
| **Type Personopplysningar** |  |
| Namn Telefonnummer Fødselsnummer Bustad  Helseopplysningar Fødselsnummer E-postadresser |  |

Følgjande kategoriar personar vert det behandla opplysningar om (registrerte): *[her listar ein opp kva kategoriar registrerte som vert omfatta – sjå døme nedanfor*

**Kategoriar av registrerte**

|  |  |  |
| --- | --- | --- |
| Innbyggjarar  Pasientar Born Elevar  Føresette | Tilsette  Tidlegare tilsette | Leverandørar  Tilsette i samarbeidande firma verksemder |

Behandlingsansvarleg har rett til å bestemme kva for hjelpemidlar som kan nyttast i behandlinga.

Følgjande behandlingar vert omfatta av Avtalen: *[her lister ein opp kva behandlingar av personopplysningar som vert omfatta – sjå døme nedanfor]*

|  |  |
| --- | --- |
| **Behandling** | **Behandlingsaktivitetar** |
| Innsamling | Databehandlar samlar inn opplysningar i eige system |
| Registrering | Innbyggjar-registreringar  Tilsett-registreringar |
| Lagring | Mellomlagring av ikkje ferdig utfylt skjema  Varig lagring av personopplysningar  Lagring i henhold til avgrensa lagringstid som angjeve i lov/forskrift eller avtale |
| Strukturering |  |
| Organisering |  |
| Tilpassing eller endring |  |
| Gjenfinning |  |
| Samanstilling |  |
| Sletting eller utradering |  |
| Utlevering |  |
|  |  |
|  |  |

Nærare beskriving av behandlinga, føremål med behandlinga og kva personopplysningar som vert omfatta, går fram av Teneste/oppdragsavtalen og seinare skriftlege avtalar mellom partane [*dersom relevant*].

## Rammene for behandling av personopplysningar

Databehandlaren skal berre behandle personopplysningane som er basert på dokumenterte instruksar frå den behandlingsansvarlege. Databehandlaren skal til ei kvar tid kunna dokumentere slike instruksar. Databehandlar skal varsle behandlingsansvarleg om instruksar og rutinar som Databehandlar meiner inneber brot på gjeldande lovgiving om behandling av personopplysningar.

Behandlingsansvarleg har til ei kvar tid full rådigheit over dei personopplysningane som databehandlar har høve til å behandle etter denne Avtalen. Databehandlar har ikkje sjølvstendig råderett over personopplysningane, og kan ikkje behandle desse til eigne føremål.

Behandlingsansvarleg har, med mindre anna er avtalt eller følgjer av lov, rett til tilgang til og innsyn i personopplysningar som vert behandla på vegne av Behandlingsansvarleg hos Databehandlaren.

## Behandlingsansvarleg sine plikter

Behandlingsansvarleg skal etterleve dei forpliktingar som kjem fram av personopplysningslova, personvernforordninga og annan særlovgiving, samt denne Avtalen.

## Databehandlar sine plikter

* 1. **Generelt**

Databehandlar forpliktar seg til å behandle personopplysningar kun i samsvar med all relevant lov og regelverk, denne Avtalen, Teneste/oppdragsavtalen, Behandlingsansvarleg sine dokumenterte instruksjonar og andre gjeldande avtalar mellom partane. Databehandlar skal ikkje med nokon handling eller unnlating, setje Behandlingsansvarleg i ein slik situasjon at Behandlingsansvarleg bryt nokon bestemming i gjeldande lov og regelverk.

Databehandlar skal ikkje:

1. behandle personopplysningar for andre føremål eller i større grad enn det som følgjer av denne Avtalen, Teneste/oppdragsavtale og eventuelle seinare skriftlege avtalar mellom partane;
2. behandle personopplysningar ut over det som er nødvendig for å oppfylle Databehandlar sine forpliktingar i henhold til dei til ei kvar tid gjeldande avtalar;
3. utlevere, overlate eller overføre personopplysningar i nokon form på eige initiativ med mindre det er avtalt på førehand med Behandlingsansvarleg eller Behandlingsansvarleg har godkjent dette skriftleg;
4. samle inn frå eller overføre personopplysningar til ein tredjepart;
5. behandle personopplysningar dei får tilgang eller adgang til gjennom oppdraget frå Behandlingsansvarleg på annan måte enn kva som er angjeve i denne Avtalen, Teneste/oppdragsavtale og eventuelle seinare skriftlege avtalar mellom partane.

Databehandlar skal:

1. ha eit internkontrollsystem som dekkjer alle behandlingsaktivitetar utført på vegne av Behandlingsansvarleg;
2. gi Behandlingsansvarleg tilgjenge til og innsyn i personopplysningar som vert behandla hos Databehandlaren;
3. dersom det er kravd etter personvernforordninga artikkel 50(5), føre og vedlikehalde oversyn over alle opplysningar og behandlingar eller, dersom det er relevant, protokoll over sine eigne behandlingsaktivitetar i henhold til personvernforordninga artikkel 30(2);
4. treffe alle rimelege tiltak for å sikre at personopplysningane til ei kvar tid er korrekte og oppdaterte;
5. etablere rutinar for å slette informasjon når den ikkje lenger er nødvendig ut frå føremålet med behandlinga og slette informasjon i henhold til fastsette rutinar og retningsliner;
6. ha rutinar for og teknisk moglegheit til å avgrense behandlinga av den registrerte sine personopplysningar dersom den registrerte ønskjer det med heimel i gjeldande lovgiving;
7. sjå til at samtlege personar som vert gitt tilgang til personopplysningar som vert behandla på vegne av Behandlingsansvarleg, er kjende med denne Avtalen og gjeldande avtalar mellom partane, og at dei er underlagt bestemmelsane i desse avtalane;
8. i rimeleg utstrekning og so langt det er mogleg, gi Behandlingsansvarleg nødvendig bistand slik at Behandlingsansvarleg skal kunne oppfylle sine forpliktingar ovafor dei registrerte;
9. so langt det er mogleg og der det er teke omsyn til arten av behandlinga, samarbeide med og bistå Behandlingsansvarleg når det gjeld å oppfylle dei registrerte sine rettar knytt til tilgang til opplysningar, her under å svare på oppmodingar frå den registrerte med det for auge å utøve sine rettar fastsett i personvernforordninga kapitel III;
10. omgåande underrette den Behandlingsansvarlege dersom Databehandlar meiner at ein instruks er i strid med personvernforordninga eller andre bestemmelsar om vern av personopplysningar;
11. i det ein tek omsyn til arten av behandlinga, bistå Behandlingsansvarleg for å sikre at pliktene i personvernforordninga artiklane 35-36 vert overhaldne, som omhandlar vurdering av personvernkonsekvensar og førehandsdrøftingar med Datatilsynet. Ved vurderingar av personvernkonsekvensar pliktar Databehandlar å vurdere tryggleikstiltak som kan bidra til å redusere risikoen behandlinga fører med seg for dei registrerte.

Databehandlar sin bistand i samband med ovannemnde skal gjerast kostnadsfritt dersom ikkje anna er avtalt.

## Tekniske, organisatoriske og tryggleiksmessige tiltak

Databehandlar pliktar å treffe og å gjennomføre alle nødvendige og adekvate planlagde og systematiske tekniske, organisatoriske og tryggleiksmessige tiltak slik at det til ei kvar tid er tilfredsstillande informasjonstryggleik ved behandling av personopplysningar.

Databehandlaren skal:

1. etablere og etterkome nødvendige tekniske og organisatoriske tiltak når det gjeld vedvarande konfidensialitet, integritet, tilgjenge og robustheit ved behandling av personopplysningar for å sikre tilfredsstillande informasjonstryggleik med visning til personvernforordninga artikkel 32. Dette omfattar mellom anna, alt etter kva som er relevant, nødvendige tiltak for å forhindre tilfeldig eller ulovleg øydelegging eller tap av data, ikkje-autorisert tilgang til eller spreiing av data og ein kvar annan bruk av personopplysningar som ikkje er i samsvar med denne Avtalen, og tiltak for å gjenopprette tilgjenge og tilgang til opplysningane ved hendingar;
2. ha gode og hensiktsmessige internkontrollrutinar;
3. ha rutinar for autorisasjon og styring som sikrar at berre dei hos Databehandlar sine medarbeidarar som har reelt behov for tilgang til system og opplysningane for å vareta nødvendige oppgåver for å gjennomføre Teneste/oppdragsavtalen, får slik tilgang. Tilgangsnivået skal vere i henhold til reelt behov knytt til å gjennomføre oppdraget. Databehandlar skal trekkje tilbake tilgangar dersom autorisasjonen løper ut eller av andre grunnar ikkje lenger gjeld for personen;
4. etablere nødvendige system og rutinar for å vareta informasjonstryggleiken, mellom anna rutinar for avviksmelding, og skal på førespurnad gi Behandlingsansvarleg tilgang til relevant tryggleiksdokumentasjon og systema som vert nytta for å behandle personopplysningar;
5. avdekke, registrere, rapportere og lukke avvik knytt til informasjonstryggleik, her under loggføre og dokumentere eit kvart forsøk på ikkje-autorisert tilgang og andre brot på personopplysningstryggleiken i datasystema. Slik dokumentasjon skal oppbevarast hos Databehandlar;
6. ved mistanke om eller konstatering av avvik, omgåande varsle Behandlingsansvarleg. I varselet vert å opplyse avviket med forklaring om årsak, tidsrom og tidspunktet avviket vart oppdaga, kategoriane av og omtrentleg tal registrerte som det vedkjem, kategoriane av og omtrentleg tal registreringar av personopplysningar som det vedkjem, namnet på og kontaktopplysningane til personvernombodet eller eit anna kontaktpunkt der meir informasjon hentast inn, antekne konsekvensar av avviket og kva umiddelbare tiltak som er sett i gong eller vert vurdert sett i gong for å handtere avviket;
7. dokumentere eit kvart avvik, her under dei faktiske forholda knytt til avviket, verknader av det og eventuelle iverksetje utbetringstiltak;
8. omgåande varsle Behandlingsansvarleg ved uautorisert utlevering av personopplysningar;
9. registrere all autorisert og uautorisert tilgang til informasjon. Alle oppslag som vert gjort skal registrerast slik at dei kan sporast til den enkelte brukar (dvs. tilsette hos Databehandlar, underleverandørar og Behandlingsansvarleg). Loggene skal oppbevarast til det ikkje lenger kan antakast å vere bruk for dei eller i henhold til det Teneste/oppdragsavtalen spesifiserer;
10. bistå Behandlingsansvarleg med å sikre at forplikting vert overhalden i personvernforordninga artiklane 32–34, dvs:
    * tryggleik ved behandlinga;
    * melding til tilsynsmynde om brot på personopplysningstryggleiken;
    * underretning av den registrerte om brot på personopplysningstryggleiken;
11. i samband med tryggleiksrevisjon som vert utført av Behandlingsansvarleg eller ein tredjepart utpeika av Behandlingsansvarleg, leggje fram interne revisjonsrapportar, interne prosedyrar, rutinar, tryggleiksarkitektur, risiko og sårbarheitsanalyser med tiltak og andre dokument av betydning for revisjonen. Behandlingsansvarleg eller tredjepart som behandlingsansvarleg peikar ut, kan utføre tilsyn etter behov eller XX (spesifikt) for å sikre at databehandlaravtalen vert overhalden.
12. varsle Behandlingsansvarleg om alle forhold som fører til endring i risikobiletet for behandling av personopplysningane;
13. hente inn godkjenning av Behandlingsansvarleg før gjennomføring av ei kvar endring av databehandlinga hos Databehandlar som har eller kan ha betydning for informasjonstryggleiken.

Nærare krav til Databehandlaren sin informasjonstryggleik er angjeve i **Vedlegg 1** om relevant. Dersom krava er dekka av kravspec eller annan avtale, kan vedlegg 1 utelatast.

Ved brot på denne Avtalen eller på bestemmelsane i forordninga eller personopplysningslova eller annan relevant lovgiving kan Behandlingsansvarleg krevje endringar i behandlingsmåten eller pålegge Databehandlar å stoppe den vidare behandlinga av opplysningane med øyeblikkeleg verknad.

Databehandlar skal dokumentere sine rutinar og alle tiltak som er trefte for å oppfylle krava gjevne ovanfor. Denne dokumentasjonen skal på førespurnad gjerast tilgjengeleg for Behandlingsansvarleg.

## Bruk av underleverandør

Behandlingsansvarleg tillet at Databehandlar nyttar underleverandørar for å oppfylle forpliktingane under Avtalen. Databehandlar nyttar underleverandørar som angjeve i **Vedlegg 2** for dei tenestene som er angjeve der og stadfestar at det er ingen andre underleverandørar som vert nytta. Databehandlar skal ikkje engasjere andre underleverandørar enn dei som er nemnt i Vedlegg 2 utan at dette på førehand er skriftlag godkjent av Behandlingsansvarleg.

Databehandlar skal:

1. sikre at underleverandøren tek på seg tilsvarande forpliktingar som Databehandlar under Avtalen og gjeldande lovgiving;
2. sørge for at underleverandørar kun behandlar personopplysningar i samsvar med denne Avtalen og ikkje i større utstrekning enn det som er nødvendig for å oppfylle den aktuelle tenesta som underleverandøren leverer;
3. halde ei oppdatert liste over identiteten og stadleg plassering av underleverandørar som angjeve i **Vedlegg 2**;
4. gjennomføre ei risikovurdering av bruken av underleverandør og betydninga for tenesta før det vert inngått avtale med underleverandør, og på Behandlingsansvarleg sin førespurnad, dele vurderinga med Behandlingsansvarleg;
5. på Behandlingsansvarleg sin førespurnad, leggje fram kopi av avtalen/avtalane som er inngått med underleverandørane (med unnatak av merkantile vilkår). Slike avtalar skal seinast vere inngått før underleverandørane startar med behandling av personopplysningar;
6. underrette Behandlingsansvarleg om eventuelle planar om å nytte andre underleverandørar eller skifte ut underleverandørar. Slike bytter skal varslast i god tid slik at Behandlingsansvarleg vert gitt høve til å motsetje seg endringa. Ved bytte av underleverandør skal **Vedlegg 2** oppdaterast og oversendast Behandlingsansvarleg sin kontaktperson. Oppdatert liste vert datert og underteikna av begge partar;
7. sikre at Behandlingsansvarleg og tilsynsmynde har same rett til innsyn og kontroll med behandling av personopplysningar hos ein underleverandør som Behandlingsansvarleg har ovafor Databehandlar etter Avtalen punkt 12;
8. ved opphøyr av Avtalen, sikre at underleverandørar oppfyller plikta til å slette eller forsvarleg destruere alle personopplysningane og alle eventuelle kopiar og tryggleikskopiar av opplysningane som går fram av Avtalen punkt 13 på same måte som Databehandlar, so langt det ikkje strir mot andre lovbestemmelsar.

Databehandlar er til ei kvar tid fullt ut ansvarleg ovafor Behandlingsansvarleg for alt arbeid som vert utført av underleverandørar og for underleverandørane sine etterlevingar av bestemmelsane i denne Avtalen.

Tilgang til personopplysningar for tredjepartar krev konkret avtale ut over denne Avtalen mellom partane for alle andre enn Databehandlar sine underleverandørar.

## Overføring av personopplysningar til utlandet

Hovudregelen er at ingen av dei personopplysningane som vert behandla under denne Avtalen skal førast ut av Norge. I tillegg skal personopplysningar vere plassert på serverar i Norge. Eventuelle unnatak som inneber overføring til utlandet skal godkjennast skriftleg av Behandlingsansvarleg før behandlinga startar.

Databehandlar bekreftar at ingen av underleverandørane overfører personopplysningar som vert omfatta av denne Avtalen til utlandet, med unnatak for slike overføringar som er angjeve i **Vedlegg 2**. Dette omfattar også fjerntilgang frå utlandet.

Bruk av underleverandørar som overfører personopplysningar til land utanfor EU/EØS (tredjeland) skal avtalast skriftleg med Behandlingsansvarleg på førehand. Ved overføring av personopplysningar til land utanfor EU/EØS (tredjeland) skal Databehandlar nytte godkjente EU-overføringsmekanismar.

Ved overføring til utlandet, uavhengig av om det er innanfor EU/EØS eller utanfor EU/EØS (tredjeland), skal Databehandlar gi nødvendig dokumentasjon om tryggleik, risiko og etterlevingsnivå knytt til aktuelle underleverandørar slik at Behandlingsansvarleg får nødvendig informasjon for å kunne gjennomføre ei særskilt risikovurdering. Behandlingsansvarleg kan nekte samtykke til den aktuelle overføringa basert på spesifikke risikoar som kjem fram av Behandlingsansvarleg si eiga risikovurdering.

## Teieplikt

Databehandlar sine tilsette og andre som opptrer på Databehandlar sine vegne i samband med behandling av personopplysningar i henhold til denne Avtalen, Teneste/oppdragsavtale og seinare skriftlege avtalar mellom partane (heretter omtalt som «personar som er autoriserte til å behandle personopplysningane), er underlagt teieplikt etter denne Avtalen og gjeldande regelverk. Personar som er autorisert til å behandle personopplysningane forpliktar seg til å behandle opplysningane fortruleg. Det same gjeld eventuelle underleverandørar.

Databehandlar skal sjå til at alle som behandlar personopplysningar under Avtalen er kjende med teieplikta.

Tilsette og andre som opptrer på Databehandlar sine vegne i samband med behandling av personopplysningar skal ha underteikna teieplikterklæring. Bestemmelsen gjeld tilsvarande for underleverandørar.

Partane har i tillegg teieplikt om konfidensiell informasjon knytt til kvar andre sine verksemder, som er formidla i samband med oppdraget, her under konfidensiell informasjon Behandlingsansvarleg eller tredjepart får tilgang til i samband med revisjon etter punkt 12 i Avtalen.

Partane pliktar å ta dei forholdsreglane som er nødvendige for å sikre at materiale eller opplysningar ikkje blir gjort kjent for andre i strid med dette punktet.

Teieplikta gjeld også etter opphøyr av Avtalen.

## Innsyn, verifikasjon og revisjon

Behandlingsansvarleg kan til ei kvar tid krevje innsyn i og verifikasjon av Databehandlar si behandling av personopplysningar som tilhøyrer Behandlingsansvarleg, her under innsyn i og verifikasjon av dokumentasjon for å oppfylle krava til informasjonstryggleik og Databehandlar sitt system for internkontroll.

Retten til innsyn gjeld alle tekniske, organisatoriske og administrative forhold som er relevante for tryggleiken ved behandlinga som vert utført av Databehandlar på vegne av Behandlingsansvarleg, og øvrige innsynsrettar nedfelt i lov. Dersom Behandlingsansvarleg ber om innsyn skal generell informasjon frå revisjonen gjerast tilgjengeleg for andre behandlingsansvarlege som nyttar same teneste hos Databehandlar.

Behandlingsansvarleg skal so vidt mogleg gi Databehandlar varsel i rimeleg tid ved krav om innsyn og kontroll, vanlegvis minst 30 dagars varsel. For krav om dokumentinnsyn bør det gis minst 14 dagars varsel. Behandlingsansvarleg skal medverke til at innsyn og kontroll kan koordinerast mellom fleire behandlingsansvarlege som får levert tenester frå Databehandlar. Innsyn og kontroll kan gjennomførast av Behandlingsansvarleg eller tredjepart som Behandlingsansvarleg utpeikar. Databehandlar kan krevje dekka dokumenterte meirkostnader som påløper ved slike revisjonar.

Databehandlar skal gi Datatilsynet og annan relevant tilsynsmynde tilgang og innsyn i behandlinga av personopplysningar slik det følgjer av relevant lovgiving.

Databehandlar skal utan ugrunna opphald korrigere eventuelle avvik. Avvik som skuldast Databehandlar eller underleverandørar til Databehandlar skal korrigerast utan kostnad for Behandlingsansvarleg. Databehandlar skal skriftleg gjere greie for korrektive tiltak og plan for å gjennomføre.

## Varigheit og opphøyr

Denne Avtalen gjeld frå han er signert av partane og gjeld til Avtalen og alle gjeldande avtalar mellom partane, som inneber at Databehandlar skal behandle personopplysningar på vegne av Behandlingsansvarleg, er opphøyrt.

Ved opphøyr av Avtalen skal Databehandlar leggje til rette for og medverke til tilbakeføring av alle opplysningar som Databehandlar har mottatt og behandla på vegne av Behandlingsansvarleg. Partane avtalar nærare korleis overføring konkret skal skje.

Etter at alle opplysningane er overførte til Behandlingsansvarleg og bekrefta mottekne av han, skal Databehandlar irreversibelt slette eller forsvarleg destruere alle opplysningane og alle eventuelle kopiar og tryggleikskopiar av opplysningane i sine system, med mindre ufråvikelege rettsreglar krev personopplysningane fortsatt lagra.

Vert det nytta delt infrastruktur der direkte sletting ikkje er teknisk mogleg, skal Databehandlar sørgje for at data vert gjort utilgjengeleg inntil desse dataene er overskrivne av systemet.

Databehandlaren sin bistand i samband med ovannemnde skal gjerast kostnadsfritt dersom ikkje anna er avtalt.

Databehandlar skal gi Behandlingsansvarleg skriftleg stadfesting på at opplysningane er overført og sletta som angjeve over.

## Endring av avtale

I tilfelle endringar i gjeldande lovverk, endeleg dom som gir ei anna tolking av gjeldande lov, eller endringar i tenester i Teneste/oppdragsavtalen som krev endringar av denne Avtalen, skal partane samarbeide for å oppdatere Avtalen tilsvarande.

## Meddelelsar

Meddelelsar, underretting, varsel eller annan kommunikasjon mellom Behandlingsansvarleg og Databehandlar skal gjevast skriftleg, eller stadfestast skriftleg til:

|  |  |
| --- | --- |
| **Behandlingsansvarleg** | **Databehandlar** |
| **[Verksemda sitt namn]** | **[Verksemda sitt namn]** |
| Att. Namn: Rolle:  E-post: | Att: Namn: Rolle:  E-post: |

## Lovval og verneting

Avtalen er underlagt norsk rett og partane vedtar Asker og Bærum tingrett som verneting. Dette gjeld også etter opphøyr av Avtalen.

## Underteikning

Denne Avtalen ligg føre i to originalar, der partane beheld eitt eksemplar kvar.

Stad og dato: XX, XX.XX.XX

På vegne av behandlingsansvarleg På vegne av databehandlar

……………………….. ………………………

(underskrift) (underskrift)

# VEDLEGG 1 – DETALJERTE KRAV TIL INFORMASJONSTRYGGLEIK

*Databehandlar har ei sjølvstendig plikt til å gjennomføre eigna tryggleikstiltak etter artikkel 32. Følgjande opplista tiltak er minimumskrav som må oppfyllast [her listar ein opp detaljerte krav til informasjonstryggleik – sjå dømer nedanfor]*

|  |  |  |  |
| --- | --- | --- | --- |
| Nr | **Krav** | **Ja/Nei/IR**  (angje IR dersom kravet ikkje er relevant i denne saman-hengen) | **Databehandlar si beskriving** Utdjup kort kvifor det er svart Ja eller Nei. Dersom det vert referert til andre dokument, må referansen vere nøyaktig m.o.t dokument, sidenr, avsnitt, URL, etc. |
| 1 | Har databehandlar inngåande kunnskap om, og opptrer databehandlar i henhold til alle relevante punkt i GDPR (personvernforordninga)? |  |  |
| 2 | Har databehandlar eit levande styringssystem (ISMS) for informasjons-tryggleik, basert på god praksis som t.d. angjeve i ISO27001/2? |  |  |
| 3 | Er ansvar og oppgåver for informasjonstryggleik dokumentert i eit organisasjonskart? |  |  |
| 4 | Er ansvar og oppgåver beskrivne på alle nivå? |  |  |
| 5 | Er ansvarsforholda gjort kjende for alle i organisasjonen? |  |  |
| 6 | Er alle tryggleikststiltak dokumenterte (organisatoriske, fysiske og tekniske)? |  |  |
| 7 | Er tryggleiksmål for verksemda fastsett? |  |  |
| 8 | Er tryggleiksstrategi for å nå tryggleiksmåla utarbeidd? |  |  |
| 9 | Er det utarbeidd rutinar for å gjennomføre risikovurderingar, inkludert oppfølging av tiltak? |  |  |
| 10 | Er alle medarbeidarar informerte om si teieplikt og klar over innhald i og omfang av den? |  |  |
| 11 | Er konsekvensar ved brot på teieplikta beskrivne? |  |  |
| 12 | Vert det jamleg gjennomført tryggleiksrevisjon og minimum årlig? |  |  |
| 13 | Dekkjer tryggleiks-revisjonen minimum: |  |  |
| a)Plassering av ansvar og organisering av tryggleiksarbeidet |  |  |
| b) Kvalitet på tryggleiksmål og tryggleiksstrategi |  |  |
| c) Overhalding av prosedyrar for bruk av informasjons-system og person-opplysningar |  |  |
| d) Resultat av opplæring |  |  |
| e) Forvaltning og bruk av personopplysningar |  |  |
| f) Tilgang til person-opplysningar og tiltak mot uautorisert innsyn? |  |  |
| h) Effekten av etablerte tryggleikstiltak? |  |  |
| i) Ivaretaking av informasjons-tryggleik hos kommunikasjons-partnarar, databehandlarar og leverandørar? |  |  |
| 14 | Er det etablert prosedyre for å følgje opp resultatet (avvik) av tryggleiksrevisjonar? |  |  |
| 15 | Er alle medarbeidarar klar over ansvaret dei har for å melde avvik? |  |  |
| 16 | Er det etablert prosedyre som sikrar at Behandlingsansvarleg vert varsla umiddelbart ved uautorisert utlevering eller endring av personopplysningar, eller andre tryggleiksbrot? |  |  |
| 17 | Vert det minimum årleg gjennomført og dokumentert leiinga sin gjennomgang av tryggleiken? |  |  |
| 18 | Er det iverksett tiltak for å hindre at teknisk personell misbrukar sin autorisasjon? |  |  |
| 19 | Er det etablert prosedyre for administrasjon av nøklar/adgangskort i adgangskontrollsystemet? |  |  |
| 20 | Er det iverksett tekniske og organisatoriske tiltak for sikker tilgang frå ikkje-sikra lokale (som t.dømes heimekontor, og via mobilt utstyr)? |  |  |
| 21 | Er det etablert tryggleikstiltak slik at kun autorisert personell får adgang til driftsutstyr (servere, nettverksutstyr, SAN, backupmedia med meir)? |  |  |
| 22 | Er det utarbeidd konfigurasjonskart over informasjonssystema? |  |  |
| 23 | Er det utarbeidd teknisk beskriving av konfigurasjonen? |  |  |
| 24 | Er kommunen sine data separert frå andre kundar sine data? |  |  |
| 25 | Har løysinga tilstrekkeleg kapasitet, uavhengig av den totale lasten leverandør har frå andre kunder |  |  |
| 26 | Har leverandøren beredskapsplanar for bortfall av løysning? |  |  |
| 27 | Har databehandlar forsvarlege backup- og restore-rutinar som vert testa regelmessig? |  |  |
| 28 | Har leverandøren gjennomført tekniske eller organisatoriske tiltak mot hacking? |  |  |
| 29 | Vert det gjort regelmessig penetrasjonstestar for å avdekke svakheiter? |  |  |
| 30 | Har databehandlar forsvarlege rutinar for autorisering og autentisering av brukarar? |  |  |
| 31 | Har databehandlar tekniske tiltak mot tenestenektangrep? |  |  |
| 32 | Har databehandlar gode løysinger for logging og sporbarheit? |  |  |
| 33 | Nyttar databehandlar eigne «dummy» testdata? |  |  |
| 34 | Vert data kryptert ved lagring? |  |  |
| 35 | Vert data kryptert i transit (kommunikasjon)? |  |  |
| 36 | Har løysninga moglegheit for å gi kommunen tilgang til logger, samt fortløpande eksportere loggdata til kommunen si SIEM løysning? |  |  |
| 37 | Ved bruk av IoT devices, har leverandøren eit godt regime for bruk av sterke passord, og regelmessig endring av desse? |  |  |

# VEDLEGG 2 – UNDERLEVERANDØRAR

*[her listar ein opp kva underleverandørar som vert nytta av Databehandlar – sjå døme nedenfor]*

|  |  |  |
| --- | --- | --- |
| **Namn på underleverandør** | **Verksemdstype/teneste som vert levert** | **Stadleg plassering** |
| ABC | Databehandlar sitt datasenter, hosting | Stockholm |
| XYZ | Tredjepart leverandør, IT- supporttenester | Paris |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |