

 HELSE FØRDE Organisasjon Forskning og innovasjon Malar	Mal for databehandlaravtale		Dokument-id: D25108		
			Avtale		
	Utarbeidd av Anette Susanne Bøe Wolff, Marianne Schiefloe Myklebust		Versjon 1.01	Gyldig frå 31.10.2024	Rev. innan 31.10.2026
	Godkjent av Kleiven, Anne Kristin		EK-ansvarleg Hovland, Runar Tengel		

Mal:

Databehandlaravtale

i samsvar med personopplysningslova og EU personvernforordning
2016/679

om behandling av person- og helseopplysningar

mellom

Dataansvarlig, org.nr.
("dataansvarlege")

og

Databehandler, org. nr.
("databehandlar")

1. Bakgrunn og føremål til avtalen

Denne avtalen gjeld for tenesteoppdrag som inkluderer behandling av person- og helseopplysningar som er tilgjengeleg på utstyr og/eller løysing som er eigd, leigd eller på anna måte blir disponert av den dataansvarlege. Avtalen skal regulere rett og plikt mellom dataansvarleg og databehandlar. Føremålet er å regulere korleis databehandlar skal behandle person- og helseopplysningar på vegner av den dataansvarlege, jf. personopplysningslova § 1, jf. personvernforordninga art 28 nr. 3. Avtalen skal vidare sikre at partane tek vare på tilfredstillande informasjonstryggleik og omfattar vern av den registrerte sine rettar. Avtalen skal sikre at opplysningane ikkje vert brukt urettmessig og at konfidensialitet, integritet -, tilgjenge og robustheit blir teke i vare på i behandlingssystema under oppdraget.

2. Forholdet til andre avtalar

Bransjenorm for informasjonstryggleik og personvern i helse- og omsorgstenesta ("Normen") er bindande for databehandlar som omhandlar helseopplysningar (Dette avsnittet kan strykast dersom det ikkje skal behandlast helseopplysningar).

Denne avtalen supplerer andre avtalar som er inngått mellom partane, for eksempel kjøps- og leigeavtalar, tenestenivåavtalar (SLA), serviceavtalar, oppdragsavtalar og avtale om tilgang til utstyr. I tilfelle konflikt mellom denne avtalen og avtalar som nemnt i avsnitt ovanfor, skal denne avtalen gjelde ved behandling av personopplysningar.

3. Tilgang til person- og helseopplysningar

Databehandlar får tilgang til person- og helseopplysningar anten ved personleg oppmøte og bruk av utstyret til den dataansvarlege eller ved fjerntilgang. I begge tilfelle gjeld tilgangen for eit spesifisert databehandlaroppdrag. Tilgangen skal ikkje brukast til andre føremål.

Helse Vest IKT AS er ansvarleg for etablering og drift av fjerntilgang over datanettverket. Leverandøren skal følgje dei krav Helse Vest IKT AS stiller til brukarar av fjerntilgang.

4. Skildring av behandling av personopplysningar

Teneste-/oppdragsavtalen (sett inn namn) medfører at databehandlar behandlar personopplysningar på vegner av dataansvarleg. I vedlegg 1 til denne avtalen kjem det nærare fram kva sjølv behandlinga som databehandlar utfører på vegne av dataansvarleg.

Personopplysningar skal berre brukast 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 imøtekomme krava i avtalane.

Føremålet med og varigheita av behandlinga er nærare skildra i vedlegg 1. Vidare skildrar dette vedlegget sjølv behandlinga som blir utført, kva helse- og personopplysningar som skal behandlast, kategoriar av dei registrerte og behandlinga sin art. Eventuelt seinare endringar skal framgå av vedlegg 1.

Databehandlar skal ikkje behandle person- og helseopplysningar på anna måte enn det som er avtalt skriftleg med den dataansvarlege.

Databehandlar kan ikkje bruke tredjepart (underleverandører) i sin behandling av personopplysningar utan at dette på førehand er skriftleg avtalt med Databehandlingsansvarleg. Dersom tredjepart blir engasjert, er Databehandlar ansvarleg for utføringa på same måte som om han sjølv stod for utføringa.

5. Omfang for behandling av helse- og personopplysningar

Behandlingsansvarleg har til ein kvar tid full rådigheit over dei helse- og personopplysningane som Databehandlar har anledning til å behandle etter denne avtalen. Databehandlar har ikkje sjølvstendig råderett over helse- og personopplysningane, og kan ikkje behandle desse til egne føremål.

Behandlingsansvarleg har, med mindre anna er avtalt eller følgjer av lov, rett til tilgang til og innsyn i helse- og personopplysningane som blir behandla hjå Databehandlar.

6. Dataansvarleg/dataansvarlege sine pliktar

Behandlingsansvarleg skal etterleve dei pliktene som kjem fram av personopplysningslova, personvernforordninga, relevant helselovgjevnad og anna særlovgjevnad, samt denne avtalen.

7. Databehandlar sine plikter

7.1 Generelt

Databehandlar plikter å behandle helse- og personopplysningar berre i samsvar med all relevant lov og regelverk, denne Avtalen, Teneste/oppdragsavtalen, Dataansvarlege sine dokumenterte instruksjonar og andre gjeldande avtalar mellom partane, samt Norm for informasjonstryggleik og personvern i helse og omsorgstenesta» "Normen". Databehandlar skal ikkje ved nokon handling eller unnlating, setje Behandlingsansvarleg i ein slik situasjon at Behandlingsansvarleg bryt nokon føresegn i gjeldande lov og regelverk.

Databehandlar skal ikkje:

- a. behandle helse- og personopplysningar for andre føremål eller i større grad enn det som følgjer av denne Avtalen med vedlegg;
- b. behandle helse- og personopplysningar utover det som er nødvendig for å oppfylle Databehandlar sine plikter i samsvar med dei til ein kvar tid gjeldande avtalar;
- c. utlevere, overlate eller overføre helse- og personopplysningar i nokon form på eige initiativ med mindre det er avtalt på førehand med Behandlingsansvarleg eller Behandlingsansvarleg har godkjent dette skriftleg;
- d. samle inn frå eller overføre helse- og personopplysningar til ein tredjepart;
- e. behandle helse- og personopplysningar dei får tilgang eller adgang til gjennom oppdraget frå Behandlingsansvarleg på annan måte enn kva som er angitt i denne Avtalen med vedlegg.
- f. gjere kjent personopplysningar for nokon tredjepart viss dette ikkje er godkjent av dataansvarleg eller lova krev det. Dersom ein offentleg myndigheit eller tilsynsmyndigheit krev tilgang til personopplysningar, skal databehandlar varsle dataansvarleg før utleveringa med mindre dette er forbode ved lov. Databehandlar krev at all personell som er autorisert for å behandle dataansvarlege sine personopplysningar, plikter seg til konfidensialitet og ikkje behandlar dataansvarlege sine personopplysningar til noko anna føremål, unntake på instruksjon frå databehandlar eller at gjeldande lov krev det.

Databehandlar skal:

- a. ha løpande kontroll på alle kategoriar av behandlingsaktivitetar utført på vegne av Behandlingsansvarleg;
- b. gje Behandlingsansvarleg tilgang til og innsyn i helse- og personopplysningar som blir behandla hos Databehandlar;
- c. føre og vedlikehalde ei oversikt over alle opplysningar og behandlingar eller dersom det er relevant, protokoll over sine eigne behandlingsaktivitetar i samsvar med personvernforordninga artikkel 30;
- d. treffe alle rimelege tiltak for å sikre at helse- og personopplysningane til ein kvar tid er korrekte og oppdaterte;
- e. 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 retningslinjer frå den dataansvarlege;
- f. ha rutinar for og teknisk moglegheit til å begrense behandlinga av den registrerte sine helse- og personopplysningar dersom den registrerte ynskjer det med heimel i gjeldande lovgjevnad;

- g. sørge for at samtlige personar som får tilgang til personopplysningar som vert behandla på vegner av Behandlingsansvarleg er kjent med denne Avtalen og gjeldande avtalar mellom partane, og er underlagt desse avtalene sine bestemmingar
- h. sikre at krav til innebygd personvern og personvern som standardinnstilling vert innfridd i Databehandlar sine løysningar. Dette inkluderer å bygge inn funksjonalitet for å oppfylle personvernprinsipp samt funksjonalitet for å sikre den registrerte sine rettar;
- i. gje Behandlingsansvarleg nødvendig bistand slik at Behandlingsansvarleg skal kunne oppfylle sine plikter ovanfor dei registrerte;
- j. samarbeide med og bistå Behandlingsansvarleg med å oppfylle dei registrerte sine rettar knytt til tilgang til opplysningar, herunder å svare på oppmoding frå den registrerte med innblikk på å utøve sine rettar fastsett i personvernforordninga kapittel III;
- k. omgåande underrette den Dataansvarlege dersom Databehandlar meiner at ein instruks er i strid med personvernforordninga eller andre føresegn om vern av personopplysningar;
- l. bistå Behandlingsansvarleg for å sikre at pliktene og ansvar i personvernforordninga artiklane 35-36 som omhandlar vurdering av personvernkonsekvensar og førehandsdrøftingar med Datatilsynet blir overhalde.

7.2 Tekniske, organisatoriske og tryggleiksmessige tiltak

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

Databehandlar skal:

- a. etablere og etterkomme nødvendige tekniske og organisatoriske tiltak med omsyn til vedvarande konfidensialitet, integritet, tilgjenge og robustheit ved behandling av helse- og personopplysningar for å sikre tilfredsstillande informasjonstryggleik etter føresegn i personopplysningslovgjevnaden, herunder krava etter personvernforordninga artikkel 32, og gjeldande helselovgjevnad. Dette omfattar blant 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 i tillegg til ein kvar annan bruk av helse- og personopplysningar som ikkje er i samsvar med denne Avtalen, og tiltak for å gjenopprette tilgjenge og tilgang til opplysningane ved førespurnad;
- b. ha gode og hensiktsmessige internkontrollrutinar;
- c. ha rutinar for autorisasjon og styring som sikrar at berre dei av Databehandlar sine medarbeidarar som har reelt behov for tilgang til system og opplysningane for å ta vare på nødvendige oppgåver for gjennomføring av Teneste/oppleggsavtalen får slik tilgang. Tilgangsnivået skal vere i samsvar med reelt behov knytt til å gjennomføre oppdraget;
- d. etablere nødvendige system og rutinar for å ta vare på informasjonstryggleiken og følge opp avvik, som skal omfatte blant anna rutinar for avviksmelding, gjenoppretting av normalsituasjonen, fjerne årsaken til avviket og hindre gjentaking. På førespurnad, skal Databehandlar gje Behandlingsansvarleg tilgang til relevant tryggleiksdokumentasjon og systema som blir brukt for behandling av helse- og personopplysningar;
- e. avdekke, registrere, rapportere og lukke avvik knytt til informasjonstryggleik, herunder loggføre og dokumentere eitkvart forsøk på ikkje-autorisert tilgang og andre brot på opplysningstryggleiken i datasystema. Slik dokumentasjon skal bli oppbevart hos Databehandlar;
- f. ved mistanke om eller konstatering av avvik, omgåande varsle Behandlingsansvarleg. I varselet skal det bli opplyst om avviket med forklaring om årsak, tidsrom og tidspunktet avviket blei oppdaga, kategoriane av og omtrentleg tal registrerte som er berørt, kategoriane av og omtrentleg tal registreringar av personopplysningar som er berørt, namnet på og kontaktopplysningane til personvernombodet eller eit anna kontaktpunkt der meir informasjon

- kan verte innhenta, antatte konsekvensar av avviket og kva direkte tiltak som er igangsett eller er vurdert igangsett for å handtere avviket;
- g. dokumentere eitkvart avvik, herunder dei faktiske forhold knytt til avviket, verknader til avviket og eventuelle iverksette forbetringstiltak;
 - h. omgåande varsle Behandlingsansvarleg ved uautorisert utlevering av personopplysningar;
 - i. registrere all autorisert og uautorisert tilgang til informasjon. Alle oppslag som blir gjort skal verte registrert slik at dei kan sporast til den enkelte brukar (dvs. tilsette hos Databehandlar, underleverandører og Behandlingsansvarleg). Loggane skal oppbevarast til det ikkje lenger er anteke å vere bruk for dei eller i samsvar med det Teneste/oppdragsavtalen spesifiserer;
 - j. bistå Behandlingsansvarleg med å sikre at ein rettar seg etter personvernforordninga artikkel 32–34, dvs:
 - tryggleik ved behandlinga;
 - melding til tilsynsmyndigheita om brot på personopplysningstryggleiken;
 - underretting av den registrerte om brot på personopplysningstryggleiken;
 - k. i samband med tryggleikssrevisjon som blir utført av Behandlingsansvarleg eller ein tredjepart utpeika av Behandlingsansvarleg, framlegger interne revisjonsrapportar, interne prosedyrar, rutinar, tryggleiksarkitektur, risiko og sårbarheitsanalysar med tiltak og andre dokumentar av betyding for revisjonen;
 - l. varsle Behandlingsansvarleg om alle forhold som medfører endring i risikobiletet;
 - m. innhente godkjenning av Behandlingsansvarleg før gjennomføring av ein kvar endring av databehandlinga hos Databehandlar som har eller kan ha betyding for informasjonstryggleiken.

Nærare krav til Databehandlaren sin informasjonstryggleik er oppgitt i **Vedlegg 2 (dersom relevant)**. Ved brot på denne avtalen eller på føresegna i personopplysningslovgjevnaden, helselovgjevnaden eller annan relevant lovgjevnad kan Behandlingsansvarleg krevje endringar i behandlingsmåten eller pålegge Databehandlar å stoppe den vidare behandlinga av opplysningane med umiddelbar verknad. Databehandlar skal dokumentere sine rutinar og alle tiltak som er bestemt for å oppfylle krava som er gitt ovanfor. Denne dokumentasjonen skal på førespurnad bli gjort tilgjengeleg for Behandlingsansvarleg.

8. Bruk av underleverandør

Behandlingsansvarleg tillèt at Databehandlar brukar underleverandører for å oppfylle forpliktingar under Avtalen. Databehandlar brukar underleverandører som angitt i **Vedlegg 3** for dei der angitte tenester og bekreftar at det er ingen andre underleverandører som blir brukt.

Databehandlar skal:

- a. sikre at underleverandøren påtar seg tilsvarende pliktar som Databehandlar under Avtalen og gjeldande lovgjevnad;
- b. sørge for at underleverandører berre 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;
- c. holde ei oppdatert liste over identiteten og plassering av underleverandører som angitt i **Vedlegg 3**. Oppdatert liste skal vere tilgjengeleg for Behandlingsansvarleg;
- d. gjennomføre ei risikovurdering av bruk av underleverandør og konsekvensen for tenesta før det blir inngått avtale med underleverandør og på Dataansvarlige sin førespurnad, dele vurderinga med Behandlingsansvarleg;
- e. på Dataansvarlige sin førespurnad, legge fram kopi av avtalen(e) som er inngått med underleverandørene (med unntak av merkantile stadfestingar). Slike avtalar skal seinast vere inngått før underleverandørene startar med behandling av helse- og personopplysningar;
- f. underrette Behandlingsansvarleg om eventuelle planar om å bruke andre underleverandører eller skifte ut underleverandører. Slike byte skal varslast i god tid slik at Behandlingsansvarleg får

høve til å motsette seg endringa. Ved byte av underleverandør skal **Vedlegg 3** bli oppdatert og oversendt til Dataansvarleg sin kontaktperson;

- g. sikre at Behandlingsansvarleg og tilsynsmyndene har same rett til innsyn og kontroll med behandling av personopplysningar hos ein underleverandør som Behandlingsansvarleg har ovanfor Databehandlar etter Avtalen punkt 11;
- h. ved opphøyr av Avtalen, sikre at underleverandører oppfyller plikten til å slette eller forsvarleg destruere alle helse- og personopplysningane og alle eventuelle kopiar og tryggleikskopiar av opplysningane som framgår av Avtalens punkt 12 på same måte som Databehandlar så langt det ikkje strider mot andre lovbestemmelsar.

Databehandlar er til ein kvar tid fullt ut ansvarleg ovanfor Behandlingsansvarleg for alt arbeid som vert utført av underleverandører og for underleverandørane sin etterleving av føresegna i denne Avtalen.

Tilgang til helse- og personopplysningar for tredjepartar krev konkret avtale utover denne Avtalen mellom partane for alle andre enn Databehandlar sine underleverandører.

9. Overføring av personopplysningar til utlandet

Partane i denne Avtalen er einige om at ingen av helse- og personopplysningane som behandlast under denne Avtalen skal førast ut av Norge, med mindre det er særskilt avtalt mellom partane. I tillegg skal helse- og personopplysningar vere plassert på servere i Norge (jf. arkivloven § 9 bokstav b). Eventuelle unntak som inneberer overføring til utlandet skal bli godkjent eksplisitt av Behandlingsansvarleg før behandlinga startar.

Databehandlar stadfester at ingen av underleverandørane overfører helse- og personopplysningar som er omfatta av denne Avtalen til utlandet, med unntak for slike overføringer som er angitt i Vedlegg 3. Dette omfattar også fjerntilgang frå utlandet.

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

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

10. Teieplikt

Databehandlar sine tilsette og andre som opptre på vegne av Databehandlar i samband med behandling av personopplysningar i denne Avtalen med vedlegg og Teneste/oppdragsavtale (heretter omtalt som «personar som er autorisert til å behandle personopplysningane»), er underlagt teieplikt etter denne Avtalen og gjeldande regelverk. Personar som er autorisert til å behandle personopplysningane plikter å behandle opplysningane fortruleg. Det same gjeld eventuelle underleverandører.

Databehandlar skal sjå til at alle som behandlar personopplysningar under avtalen er kjent med teieplikta. Tilsette og andre som opptre på vegne av Databehandlar i samsvar med behandling av personopplysningar skal ha underteikna teiepliktserklæring. Føresegna gjeld tilsvarande for underleverandører.

Teieplikta gjeld og etter opphøyr av Avtalen.

11. Innsyn, verifikasjon og revisjon

Behandlingsansvarleg kan til ein kvar tid krevje innsyn i og verifikasjon av Databehandlar si behandling av personopplysningar tilhøyrande Behandlingsansvarleg, inkludert innsyn i og verifikasjon av

dokumentasjon for oppfylling av krav til informasjonstryggleik og Databehandlar sine system for internkontroll.

Retten til innsyn gjeld alle tekniske, organisatoriske og administrative forhold som er relevante for tryggleiken ved behandlinga som blir utført av Databehandlar på vegne av Behandlingsansvarleg, og øvrige innsynsrettigheter nedfelt i lov. Dersom Behandlingsansvarleg ber om innsyn skal generell informasjon frå revisjonen bli gjort tilgjengeleg for andre dataansvarlege som brukar same teneste hos Databehandlar.

Behandlingsansvarleg skal så vidt mogleg gje Databehandlar varsel i rimeleg tid ved krav om innsyn og kontroll, vanlegvis minst 30 dagars varsel. For krav om dokumentinnsyn bør det bli gitt minst 14 dagars varsel. Behandlingsansvarleg skal medverke til at innsyn og kontroll kan koordinerast mellom fleire dataansvarlege som får levert tenester frå Databehandlar. Innsyn og kontroll kan gjennomførast av Behandlingsansvarleg eller tredjepart som blir utpeika av Behandlingsansvarleg. Databehandlar kan krevje dekkja dokumenterte meirkostnader som kjem ved slike revisjonar.

Databehandlar skal gje Datatilsynet og annan relevant tilsynsmynde tilgang og innsyn i behandlinga av helse- og personopplysningar slik det følgjer av relevant lovgjevnad.

Databehandlar skal utan ugrunna opphald korrigere eventuelle avvik. Avvik som skuldast Databehandlar eller deira underleverandører skal bli korrigerte utan kostnad for Behandlingsansvarleg. Databehandlar skal skriftleg gjere greie for korrektive tiltak og plan for gjennomføring.

12. 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 tilsvarende.

13. Varigheit og opphøyr

Denne avtalen gjeld frå den er signert av begge partar og til behandlinga av helse- og personopplysningar opphøyrer. Når behandling av helse- og personopplysningar opphøyrer skal Databehandlar legge til rette for og medverke til overføring av alle opplysningar som Databehandlar har behandla på vegne av dataansvarleg. Partane avtalar nærmare korleis overføring konkret skal skje.

Etter at alle opplysningane er overført til og bekrefta mottekne av Databehandlingsansvarleg, skal Databehandlar slette opplysningane og alle eventuelle kopiar og tryggleikskopiar av opplysningane i sine system.

Databehandlar skal gje Databehandlingsansvarleg skriftleg stadfesting på at opplysningane er overført og sletta som skrive over.

14. Avtalebrot(mishald) og erstatning for økonomiske utlegg

Avtalebrot føreligg dersom ein part ikkje oppfyller sine plikter etter avtalen, og dette ikkje skuldast forhold som den andre parten har ansvar eller risiko for. Den som vil påkalle seg avtalebrot må melde dette til den andre parten med skriftleg grunngjevnad, utan ugrunna opphald etter at det aktuelle forholdet vart kjent. Dersom ein part i vesentleg grad misheld sine plikter etter avtalen kan den andre parten heve avtalen.

Den som ynskjer å heve skal i skriftleg varsel setje ein rimeleg frist for retting av forholdet. Av varselet skal det framgå at avtalen vil bli heva dersom forholdet ikkje er retta innan fristen.

Brot på teieplikt vil alltid bli sett som vesentleg mishald.

Dersom avtalebrot fører til økonomisk tap i form av auka utgifter eller reduserte inntekter, kan den skadelidte parten krevje at motparten dekkar tapet.

15. Kunngjering og kontaktpersonar

Alle kunngjeringar som blir gitt i samsvar med denne avtalen skal vere skriftlege. Andre språk enn norsk kan berre brukast dersom det er avtalt.

Avsendar pliktar å vurdere om kunngjeringa har eit slikt innhald at den skal vere unnateke offentlegheit på grunn av personopplysningar eller næringsopplysningar, jf. forvaltningslova §§ 13 flg.

Følgjande kontaktpersonar er oppnemnt i avtalen.

For den dataansvarlege: Namn, rolle, kontaktinformasjon

For databehandlararen: Namn, rolle, kontaktinformasjon

Skifte av kontaktperson skal så snart som mogleg kunngjerast skriftleg til den andre parten.

16. Rettsval og verneting

Dette er nærmare regulert i tenesteavtalen mellom dataansvarleg og databehandlar punkt

17. Underteikning

Denne avtalen underteiknast i to eksemplar og partane får kvar sitt eksemplar.

Stad og dato

Stad og dato

Databehandlingsansvarleg

Helse Førde
(klinikk-/stabs-direktør
Stilling og namn

Databehandlar

Stilling og namn

VEDLEGG 1 – FØREMÅL TIL BEHANDLINGA OG OPPLYSNINGAR

Tabellane skal oppdaterast fortløpande og daterast.

[dato/månad/år]

A. Føremålet med og varigheita av behandlinga

Føremålet med og varigheita av behandling av helse- og personopplysningar er: [hugs at kvar behandling må vere knytt til spesifikke og uttrykkeleg gitte føremål – sjå eksempel nedanfor. Fjern det som ikkje er aktuelt.]

OBS- Fjern denne boksen med rettleiingstekst.

Kvifor gjer underleverandøren denne databehandlinga? Kvifor treng vi ekstern hjelp i drifta?

Dersom føremålet ikkje kjem klart fram av driftsavtalen skal dette vere klart for kunden(e)/dei dataansvarlege for systemet, så spør gjerne der.

Dato (frå/til)	Navn på teneste	Føremålet med behandlinga	Varigheita av behandlinga
<Fyll ut>	Filoverføringstenesta	Overføre større datamengder	Til føremålet er oppnådd
<Fyll ut>	Vedlikehald av system	Drift og forvaltning	I avtaleperioden
<Fyll ut>	Produktutvikling	Betre funksjonalitet etc	I avtaleperioden
<Fyll ut>	Hjelp ved feilretting	Hjelp ved feilretting – gjennomrette og stabilisere drift	I avtaleperioden
<Fyll ut>	Fillagring	Lagring av filer og databaser	I avtaleperioden
<Fyll ut>	<Fyll ut>	<Fyll ut>	<Fyll ut>

B. Behandling av helse- og personopplysningar

Det følgjer av personvernforordninga art 4 nr.2 at med «behandling» tyder dette: «kvar ein operasjon eller rekke av operasjonar som blir gjort med personopplysningar, enten automatisert eller ikkje, til dømes innsamling, registrering, organisering, strukturering, lagring, tilpassing eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spreiding eller alle andre former for tilgjengeleggjering, samanstilling eller samkøyring, avgrensing eller sletting»

Følgjande behandling av personopplysningar blir omfatta av Avtalen: [sjå eksemplar nedanfor – stryk det som ikkje passer]

OBS- Fjern denne boksen med rettleiingstekst.

Korleis gjennomfører underleverandøren denne databehandlinga? Kva er det denne underleverandøren konkret utfører av oppgåver og handlingar knytt til lagra personopplysningar?

Dette kan komme fram av avtalene med underleverandøren, bør vere kjent for forvaltninga og gjerne også for kundane/ dei dataansvarlege av løysinga.

1.1 Databehandling

1.2 Nærmare beskriving av databehandlingsaktiviteter

1.3	Tilgang til lagra personopplysningar for feilretting	1.4	<Særleg relevant – forslag til tekst: Leverandøren har behov for tilgang til lagra personopplysningar for feilsøking og feilretting. >
1.5	Tilgang til lagra personopplysningar for support oppdatering	1.6	<Særleg relevant – forslag til tekst: Leverandøren har behov for tilgang til lagra personopplysningar for oppdatering>
1.7	Tilgang til lagra personopplysningar for konfigurasjon	1.8	<Særleg relevant – forslag til tekst: Leverandøren har behov for tilgang til lagra personopplysningar for konfigurasjon. Leverandøren kan utføre konfigurasjonsendringar på oppdrag frå databehandlar eller dataansvarlig.>
1.9	Innsamling	1.10	<Fyll ut dersom relevant>
1.11	Registrering	1.12	<Fyll ut dersom relevant>
1.13	Organisering	1.14	<Fyll ut dersom relevant>
1.15	Strukturering	1.16	<Fyll ut dersom relevant>
1.17	Lagring	1.18	<Fyll ut dersom relevant>
1.19	Tilpassing eller endring	1.20	<Fyll ut dersom relevant>
1.21	Gjenfinning	1.22	<Fyll ut dersom relevant>
1.23	Samanstilling	1.24	<Fyll ut dersom relevant>
1.25	Sletting	1.26	<Fyll ut dersom relevant>
1.27	Utlevering/Overføring	1.28	<Fyll ut dersom relevant>
1.29	Andre former for tilgjengeleggjering	1.30	<Fyll ut dersom relevant>
1.31	<Andre relevante behandlingar>	1.32	<Fyll ut>

C. Typar av opplysningar

Følgjande helse- og personopplysningar blir behandla: [her lister ein opp kva helse- og personopplysningar som blir omfatta – sjå dømer nedanfor – fyll ut/stryk det som passar]

Personopplysningar

Namn

Fødselsnummer

Bustad

<Andre opplysningar – fyll ut>

OBS- Fjern denne boksen med rettleiingstekst.

Stikkordet her er «kva er lagra om dei registrerte». Kva opplysningar ligg lagra i løysinga som underleverandøren eventuelt kan få tilgang til/komme i inngrep med.

Helseopplysningar

Legemiddelbruk

Diagnoseopplysningar

Opplysningar frå helseregistre

<Andre opplysningar – fyll ut>

D. Kategoriar av registrerte
1.33

Følgjande kategoriar av personar blir det behandla opplysningar om (registrerte): [her blir det lista opp kva kategoriar av registrerte som blir omhandla – sjå døme nedanfor. Stikkordet her er «om kven». Kva personar ligg det data om i løysinga. Fyll ut/stryk det som ikkje passar.]

Kategoriar av registrerte

Pasientar

Barn

Foreldre

Fullmektigar

Helsepersonell

Tilsette

Tidligare tilsette

Tilsette i samarbeidande firma

Leverandører

Nøkkelpersonar

<Fyll ut>

VEDLEGG 2 – DETALJERTE KRAV TIL INFORMASJONSTRYGGLEIK

[her skal det listast opp detaljerte krav til informasjonstryggleik – sjå døme nedanfor – fyll ut det som er relevant]

[dato/månad/år]

Nr.	Tema	Krav
1.	Norm for informasjonstryggleik i helse- og omsorgssektoren	Databehandlar skal følge relevante krav i Norm for informasjonstryggleik (sjå faktaark 6b, og kva krav som er gitt for databehandlar)
2.	Sikring av data	Databehandlar skal ha mekanismar for data under transport, prosessering og lagring for å ta vare på integritet og konfidensialitet.
3.	Autentisering	Ved tilgang til data ved tenestleg behov skal det brukast personlege brukarnamn med passord. Databehandlar skal ha etablert passordpolicy.
4.	Tenestenektangrep	<Fyll ut dersom relevant>
5.	Logging og sporbarheit	<Fyll ut dersom relevant>
6.	Redundans og skalering	<Fyll ut dersom relevant>
7.	Testdata	<Fyll ut dersom relevant>
8.	Sletting og tilbakelevering	<Fyll ut dersom relevant>
9.	Lagringstid	<Fyll ut dersom relevant>
10.	Backup og restore	<Fyll ut dersom relevant>
11.	Kryptering ved lagring	<Fyll ut dersom relevant>
12.	Kryptering i kommunikasjon	<Fyll ut dersom relevant>
13.	<Anna>	
14.		
15.		

VEDLEGG 3 – UNDERLEVERANDØRER

[her skal det listast opp kva underleverandører som blir brukt av Databehandlar – sjå eksempel nedanfor- blir fylt ut berre når underleverandøren brukar andre underleverandører]

Tabellane skal bli oppdatert fortløpande.

[dato/månad/år]

Navn på underleverandør	Leveranseområde	Stedlig plassering
ABC	Datasenter, hosting	Stockholm, Sverige
DEF	IT-supporttenestar	Oslo, Norge
XYZ	Backup	Paris, Frankrike

Interne referansar

Eksterne referansar

Vedlegg

