

**DATABEHANDLERAVTALE**

Avtale om behandling av personopplysninger

mellom

**Sykehuset Østfold HF**

Org. no.: 983 971 768

*Dataansvarlig*

og

**[Navn på databehandler]**

Org. no.: 000 000 000

*Databehandler*

Dato: xx.xx.20xx

Innholdsfortegnelse

**1. Om avtalen**

**2. Definisjoner**

**3. Avtalens bakgrunn og formål**

**4.** **Omfang**

**5. Behandlingens formål, opplysninger og behandlinger**

**6. Rammene for behandling av helse- og personopplysninger**

**7. Dataansvarliges plikter**

**8. Databehandlers plikter**

**9.** **Bruk av underleverandør**

**10. Overføring av personopplysninger til utlandet**

**11. Taushetsplikt**

**12. Innsyn, verifikasjon og revisjon**

**13.** **Varighet og opphør**

**14.** **Endring av avtale**

**15.** **Meddelelser**

**16.** **Lovvalg og verneting**

**17.** **Undertegning**

**VEDLEGG 1 – BEHANDLINGENS FORMÅL, OPPLYSNINGER OG BEHANDLINGER**

**VEDLEGG 2a – SIKKERHETSKRAV**

**VEDLEGG 2b – RISIKOVURDERINGER**

**VEDLEGG 3 – UNDERLEVERANDØRER**

**1. Om avtalen**

Denne databehandleravtalen (heretter omtalt som "Avtalen") regulerer rettigheter og plikter mellom Dataansvarlig og Databehandler (heretter omtalt som "partene") etter:

* Lov av 15.juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven);
* EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen");
* Lov om helseregistre og behandling av helseregistre av 20.juni 2014 nr.43 (helseregisterloven);
* Lov om behandling av helseopplysninger ved ytelse av helsehjelp av 20.juni 2014 nr. 42 (pasientjournalloven); og
* Enhver lov, forskrift eller annet regelverk som erstatter disse.

Ved motstrid mellom Avtalens regulering og de rammer som følger av personopplysnings­lovgivningen eller relevant helselovgivning (personvernregelverket), viker Avtalens regulering.

Dataansvarliges navn, organisasjonsnummer og øvrig kontaktinformasjon finnes i Databehandlers kundesystem, basert på dataansvarliges egne opplysninger.

Denne avtalen skal kun benyttes om Sykehuspartner HF ikke er part. Dersom Sykehuspartner HF er involvert, skal regionens standard databehandleravtale benyttes.

**2. Definisjoner**

|  |  |
| --- | --- |
| **Personvernregelverket:** | Med Personvernregelverket menes:   1. Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven) 2. EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen"); 3. Lov 20. juni 2014 nr. 42 om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) 4. Lov 20. juni 2014 nr. 43 om helseregistre og behandling av helseopplysninger (helseregisterloven) 5. All annen gjeldende norsk lov og forskrift som regulerer Databehandlers behandling av helse- og personopplysninger, 6. Enhver lov, forskrift og annet regelverk som erstatter disse.   Med mindre annet er spesifisert gjelder alle referanser til GDPR som en henvisning til norsk implementering av personvernforordningen i nasjonal rett, og tolkning av denne. |
| **Personopplysning:** | Enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»), jf. GDPR art. 4 (1). Personopplysninger i denne avtalen omfatter også helseopplysninger, se definisjon av helseopplysninger nedenfor. |
| **Helseopplysning:** | Enhver personopplysning om en fysisk persons fysiske eller psykiske helse, herunder om ytelse av helsetjenester, som gir informasjon om vedkommendes helsetilstand, jf. GDPR art. 4 (15), samt genetiske og biometriske opplysninger jf. samme bestemmelse (13) og (14). I denne Avtalen omfatter helseopplysninger videre alle opplysninger som er taushetsbelagt etter helsepersonelloven herunder helseopplysninger om avdøde personer, jf. pasientjournalloven § 3 andre ledd. |
| **Behandling:** | Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring, jf. GDPR art. 4 (2) |
| **Dataansvarlig:** | Fysisk eller juridisk person som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes, jf. GDPR art. 4 (7). I denne avtalen benyttes begrepet Dataansvarlig i stedet for behandlingsansvarlig også i de tilfeller det i henhold til personvernregelverket brukes begrepet behandlingsansvarlig. Hvem som er Dataansvarlig i denne avtalen er angitt på første siden av denne avtalen. |
| **Databehandler:** | Fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige/dataansvarlige, jf. GDPR art. 4 (8). Hvem som er Dataabehandler i denne avtalen er angitt på første siden av denne avtalen. |
| **Risikovurdering** | I risikovurderingen fremgår det hvilke personopplysninger som blir behandlet, samt annen relevant informasjon i henhold til GDPR. Risikovurderingen kartlegger informasjonssikkerhetsmessig risiko ved behandlingen, og identifiserer risikoreduserende tiltak. Det er Dataansvarlig som aksepterer risiko. |

"Avvik": brudd på personopplysningssikkerheten, slik det er definert i GDPR art 4 (12) og bruk av informasjonssystemet i strid med fastlagte rutiner.

Bruk av informasjonssystemet som ikke er i samsvar med instrukser fra Dataansvarlig eller gjeldende personvernregelverk skal behandles som avvik.

Når det i Databehandleravtalen vises til dokumentasjon eller informasjon med bruk av fotnoter med elektronisk url må Dataansvarlig, Databehandler, og eventuelle underleverandører sørge for å lese og forstå disse.

**3. Avtalens bakgrunn og formål**

Denne Avtalen beskriver de generelle vilkårene for den behandling av helse- og personopplysninger som Databehandler utfører på vegne av Dataansvarlig.

Formålet med Avtalen er å sikre at behandlingen av helse- og personopplysninger på vegne av Dataansvarlig behandles i samsvar med kravene til personvernregelverket, i henhold til denne Databehandleravtalen og i henhold til instruksjoner fra Dataansvarlig.

**4.** **Omfang**

Denne Avtalen kommer til anvendelse på all behandling av helse- og personopplysninger som Databehandler foretar på grunnlag av [*skriv navn på tjeneste/oppdragsavtale*] (heretter omtalt som "Tjeneste/oppdragsavtalen").

De tjenester som innebærer behandling av helse- og personopplysninger er angitt i Bilag 1 til denne Avtalen. Databehandlers behandling av helse- og personopplysninger skal begrenses til den behandlingen som er nødvendig for at Databehandler skal kunne gjennomføre ytelse av de avtalte tjenester. Før Behandling kan igangsettes skal det gjøres risikovurdering. Risikovurderingen inneholder alle relevante krav og informasjon i henhold til GDPR, og vil bli oppsummert og oppdatert i Databehandlers til enhver tid gjeldende Protokoll over behandlingsaktiviteter.

I tilfelle konflikt mellom denne Avtalen og Tjeneste/oppdragsavtalen, skal denne Avtalen gjelde.

Tjenester som inngår i denne Avtalen er de tjenester som inngår i Tjeneste/oppdragsavtalen og som innebærer behandling av helse- og personopplysninger.

Der Dataansvarlig velger å ta i bruk nye tjenester hos denne databehandler, skal det avklares om behandlingen ligger innenfor samme formål som Avtalen regulerer. Dersom det ligger innenfor samme formål, gjelder denne databehandleravtalen.

Enhver endring av databehandlingen hos Databehandler som har eller kan ha betydning for informasjonssikkerheten skal risikovurderes og godkjennes av Dataansvarlig før endring gjennomføres, eventuelt med slike ytterligere tiltak Dataansvarlig har anvist. Det er kun Dataansvarlig som kan akseptere endring av risiko, og Dataansvarlig må derfor godkjenne bruk av tjenester i henhold til risikovurdering på bakgrunn av utført og behandlet risikovurdering før databehandlingen kan starte. Dette omfatter også endring av eventuelle underleverandører til databehandler.

Denne Avtalen vil i tillegg gjelde for ytterligere behandling av helse- og personopplysninger basert på eventuelle skriftlige avtaler mellom partene som inngås i løpet av denne Avtalens varighet og som innebærer at Databehandler behandler helse- og personopplysninger på vegne av Dataansvarlig (heretter omtalt som "senere skriftlige avtaler mellom partene").

Helse- og personopplysninger skal kun benyttes til de formålene som følger av denne Avtalen, Tjeneste/oppdragsavtalen og senere skriftlige avtaler mellom partene i den utstrekning det er strengt nødvendig for å gjennomføre og imøtekomme kravene i avtalene.

**5. Behandlingens formål, opplysninger og behandlinger**

[Beskrives]

**6. Rammene for behandling av helse- og personopplysninger**

Dataansvarlig har til enhver tid full rådighet over de helse- og personopplysningene som Databehandler har anledning til å behandle etter denne Avtalen. Databehandler har ikke selvstendig råderett over helse- og personopplysningene, og kan ikke behandle disse til egne formål.

Dataansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i helse- og personopplysningene som behandles hos Databehandleren.

**7. Dataansvarliges plikter**

Dataansvarlig skal etterleve de forpliktelser som fremkommer av personvernregelverket, samt denne Avtalen, Norm for informasjonssikkerhet og sykehusets styringssystem for informasjonssikkerhet.

**8. Databehandlers plikter**

**8.1. Generelt**

Databehandler forplikter seg til å behandle helse- og personopplysninger i samsvar med personvernregelverket, denne Avtalen, til enhver tid gjeldende felles regionalt styringssystem for informasjonsikkerhet i HSØ og dataansvarliges styringssystem, Tjeneste/oppdragsavtalen, Dataansvarliges dokumenterte instruksjoner og andre gjeldende avtaler mellom partene, samt "Norm for informasjonssikkerhet i helse- og omsorgstjenesten". Databehandler skal ikke ved noen handling eller unnlatelse, sette Dataansvarlig i en slik situasjon at Dataansvarlig bryter noen bestemmelse i gjeldende lov og regelverk.

Databehandler er ansvarlig for skade forårsaket av Databehandlers behandling, kun dersom forpliktelsene i personvernregelverket som særlig er rettet mot databehandlere ikke er oppfylt, eller dersom Databehandler har opptrådt utenfor eller i strid med instrukser fra Dataansvarlig.

Dersom en underleverandør ikke oppfyller sine forpliktelser med hensyn til Personvernregelverket og denne Databehandleravtalen, skal Databehandler ha fullt ansvar for Underleverandørs oppfyllelse eller manglende oppfyllelse av disse forpliktelsene.

Databehandler skal ikke:

1. behandle helse- og personopplysninger for andre formål eller i større grad enn det som følger av denne Avtalen, Tjeneste/oppdragsavtale og eventuelle senere skriftlige avtaler mellom partene;
2. behandle helse- og personopplysninger utover det som er nødvendig for å oppfylle Databehandlers forpliktelser i henhold til de til enhver tid gjeldende avtaler;
3. utlevere, overlate eller overføre helse- og personopplysninger i noen form på eget initiativ med mindre det er avtalt på forhånd med Dataansvarlig eller Dataansvarlig har godkjent dette skriftlig;
4. samle inn fra, eller overføre helse- og personopplysninger til en tredjepart;
5. behandle helse- og personopplysninger de får tilgang eller adgang til gjennom oppdraget fra Dataansvarlig på annen måte enn hva som er angitt i denne Avtalen, Tjeneste/oppdragsavtale og eventuelle senere skriftlige avtaler mellom partene.

Databehandler skal:

1. ha løpende kontroll på alle kategorier av behandlingsaktiviteter utført på vegne av Dataansvarlig;
2. gi Dataansvarlig tilgang til og innsyn i helse- og personopplysninger som behandles hos Databehandleren;
3. føre og vedlikeholde en oversikt over alle opplysninger og behandlinger eller dersom det er relevant, protokoll over sine egne behandlingsaktiviteter i henhold til personvernforordningen artikkel 30;
4. treffe alle rimelige tiltak for å sikre at helse- og personopplysningene til enhver tid er korrekte og oppdaterte;
5. 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;
6. ha rutiner for, og teknisk mulighet til å begrense behandlingen av den registrertes helse- og personopplysninger dersom den registrerte ønsker det med hjemmel i gjeldende lovgivning;
7. påse at samtlige personer som gis tilgang til personopplysninger som behandles på vegne av Dataansvarlig er kjent med denne Avtalen og gjeldende avtaler mellom partene, og er underlagt disse avtalenes bestemmelser;
8. 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;
9. gi Dataansvarlig nødvendig bistand slik at Dataansvarlig skal kunne oppfylle sine forpliktelser overfor de registrerte;
10. samarbeide med og bistå Datasansvarlig 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;
11. omgående underrette den Dataansvarlige dersom Databehandler mener at en instruks er i strid med personvernforordningen eller andre bestemmelser om vern av personopplysninger;
12. bistå Dataansvarlig for å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 35-36 som omhandler vurdering av personvernkonsekvenser og forhåndsdrøftinger med Datatilsynet.

**8.2. Tekniske, organisatoriske og sikkerhetsmessige tiltak**

Databehandler plikter å treffe og gjennomføre alle nødvendige og adekvate planlagte og systematiske tekniske, organisatoriske og sikkerhetsmessige tiltak slik at det til enhver tid er tilfredsstillende informasjonssikkerhet ved behandling av helse- og personopplysninger. All behandling av Personopplysninger som er omfattet av denne Databehandleravtale skal skje i henhold til det nivå for akseptabel risiko som er fastsatt av Dataansvarlig.

Databehandleren skal:

1. etablere og etterkomme nødvendige tekniske og organisatoriske tiltak med hensyn til vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet ved behandling av helse- og personopplysninger for å sikre tilfredsstillende informasjonssikkerhet i henhold til personopplysningslovgivningens bestemmelser, herunder kravene etter personvernforordningen artikkel 32, og gjeldende helselovgivning (personvernregelverket), felles regionalt styringssystem i HSØ og foretakets interne styringssystem. Dette omfatter blant annet, alt etter hva som er relevant, nødvendige tiltak for å forhindre tilfeldig eller ulovlig ødeleggelse eller tap av data, ikke-autorisert tilgang til eller spredning av data så vel som enhver annen bruk av helse- og personopplysninger som ikke er i overensstemmelse med denne Avtalen, og tiltak for å gjenopprette tilgjengelighet og tilgang til opplysningene ved hendelser;
2. Sikre helseopplysninger mot uaktsom utlevering. Tekniske tiltak skal være på plass for å forhindre at personopplysninger kan flyttes ut av sikker sone eller fra godkjent lagringssted
3. Ivareta sikkerheten ved fjerndrift av Dataansvarliges systemer. Det skal benyttes kryptert VPN-forbindelse med sperring mot samtidig tilgang til internett. Utstyr som benyttes i forbindelse med fjerntilgang skal ikke brukes av uautoriserte personer
4. Benytte 2-nivå-autentisering dersom tilgang til Dataansvarliges systemer skjer via usikre nettverk
5. Sikre kommunikasjon med kryptering dersom den går over usikre nettverk
6. Ha gode og hensiktsmessige internkontrollrutiner;
7. Ha rutiner for autorisasjon og styring som sikrer at bare de av Databehandlers medarbeidere som har reelt behov for tilgang til systemer og opplysningene for å ivareta nødvendige oppgaver for gjennomføring av tjeneste/oppdragsavtalen får slik tilgang. Tilgangsnivået skal være i henhold til reelt behov knyttet til å gjennomføre oppdraget;
8. Benytte adgangskontroll med bruk av adgangskort med personlig kode eller tilsvarende. Tilgang til begrensede områder, eksempelvis drifts- og serverrom, skal være basert på reelt behov. Adgangskontroll med låste dører skal benyttes for følgende typer lokaler: datahall/serverrom, IT lokaler (drift/support), lokaler med IT relatert utstyr (koblingsmatriser, svitsjer/rutere) mv.
9. Etablere nødvendige systemer og rutiner for å ivareta informasjonssikkerheten og følge opp avvik, som skal omfatte blant annet rutiner for avviksmelding, gjenoppretting av normalsituasjonen, fjerne årsaken til avviket og hindre gjentakelse. På forespørsel, skal Databehandler gi Dataansvarlig tilgang til relevant sikkerhetsdokumentasjon og systemene som benyttes for behandling av helse- og personopplysninger;
10. Avdekke, registrere, rapportere og lukke avvik knyttet til informasjonssikkerhet, herunder loggføre og dokumentere ethvert forsøk på ikke-autorisert tilgang og andre brudd på opplysningssikkerheten i datasystemene. Slik dokumentasjon skal oppbevares hos Databehandler;
11. ved mistanke om eller konstatering av avvik, omgående varsle Dataansvarlig og Dataansvarliges personvernombud. I varselet opplyses avviket med forklaring om årsak, tidsrom og tidspunktet avviket ble oppdaget, kategoriene av og omtrentlig antall registrerte som er berørt, kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt, navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes, antatte konsekvenser av avviket og hvilke umiddelbare tiltak som er igangsatt eller vurderes igangsatt for å håndtere avviket. Enhver varsling eller henvendelse til Datatilsynet skal skje gjennom Dataansvarlig;
12. dokumentere ethvert avvik, herunder de faktiske forhold knyttet til avviket, dets virkninger og eventuelle iverksatte utbedringstiltak;
13. omgående varsle Dataansvarlig ved uautorisert utlevering av personopplysninger;
14. registrere all autorisert og uautorisert tilgang til informasjon. Alle oppslag som gjøres skal registreres slik at de kan spores til den enkelte bruker (dvs. ansatte hos Databehandler, underleverandører og Dataansvarlig). Loggene skal oppbevares til det ikke lenger antas å være bruk for dem eller i henhold til det Tjeneste/oppdragsavtalen spesifiserer;
15. bistå Dataansvarlig med å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 32–34, dvs:  
    - sikkerhet ved behandlingen;  
    - melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten;  
    - underretning av den registrerte om brudd på personopplysningssikkerheten;
16. i forbindelse med sikkerhetsrevisjon som utføres av Dataansvarlig eller en tredjepart utpekt av Dataansvarlig, framlegge interne revisjonsrapporter, interne prosedyrer, rutiner, sikkerhetsarkitektur, risiko og sårbarhetsanalyser med tiltak og andre dokumenter av betydning for revisjonen;
17. varsle Dataansvarlig om alle forhold som medfører endring i risikobildet;
18. innhente godkjenning av Dataansvarlig før gjennomføring av enhver endring av databehandlingen hos Databehandler som har eller kan ha betydning for informasjonssikkerheten.

Nærmere krav til Databehandlerens informasjonssikkerhet er angitt i Vedlegg 2a (hvis relevant). Risikovurderinger er i Vedlegg 2b. Ved brudd på denne Avtalen eller på bestemmelsene i personvernregelverket kan Dataansvarlig kreve endringer i behandlingsmåten eller pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Databehandler skal dokumentere sine rutiner og alle tiltak truffet for å oppfylle kravene angitt ovenfor. Denne dokumentasjonen skal på forespørsel gjøres tilgjengelig for Dataansvarlig.

**9.** **Bruk av underleverandør**

Dataansvarlig tillater at Databehandler benytter underleverandører for oppfyllelse av forpliktelsene under Avtalen. Databehandler benytter underleverandører som angitt i Vedlegg 3 for de der angitte tjenester og bekrefter at det er ingen andre underleverandører som benyttes. Databehandler kan ikke benytte andre underleverandører enn de som ved avtaletidspunktet var avtalt mellom dataansvarlig og databehandler uten at aktiviteter i bokstav d og f er gjennomført.

Databehandler skal:

a. sikre at underleverandøren påtar seg tilsvarende forpliktelser som Databehandler under Avtalen og gjeldende lovgivning;

b. sørge for at underleverandører kun behandler personopplysninger i samsvar med denne Avtalen og ikke i større utstrekning enn det som er nødvendig for å oppfylle den aktuelle tjenesten som underleverandøren leverer;

c. holde en oppdatert liste over identiteten og stedlig plassering av underleverandører som angitt i **Vedlegg 3**. Oppdatert liste skal være tilgjengelig for Dataansvarlig;

d. gjennomføre en risikovurdering av bruk av underleverandør og betydningen for tjenesten før det inngås avtale med underleverandør og på Dataansvarliges forespørsel, dele vurderingen med Dataansvarlig;

e. på Dataansvarliges forespørsel, legge frem kopi av avtalen(e) som er inngått med underleverandørene (med unntak av merkantile betingelser). Slike avtaler skal senest være inngått før underleverandørene starter med behandling av helse- og personopplysninger;

f. underrette Dataansvarlig i god tid om eventuelle planer om å benytte andre underleverandører eller skifte ut underleverandører. Slike bytter skal varsles i god tid slik at Dataansvarlig gis mulighet til å motsette seg endringen. Databehandler kan ikke benytte andre underleverandører enn de som ved avtaletidspunktet følger av Vedlegg 3 uten at følgende er gjennomført:1) Dataansvarlig har godkjent risikovurderingen, 2) Dataansvarlig har skriftlig godkjent bruk av aktuelle/nye underleverandør, Ved bytte av underleverandør skal **Vedlegg** 3 oppdateres og oversendes Dataansvarliges kontaktperson skal gjøres oppmerksom på dette;

g. sikre at Behandlingsansvarlig og tilsynsmyndighetene har samme rett til innsyn og kontroll med behandling av personopplysninger hos en underleverandør som Behandlingsansvarlig har overfor Databehandler etter Avtalens punkt 12;

h. ved opphør av Avtalen, sikre at underleverandører oppfyller plikten til å slette og forsvarlig destruere eller på oppfordring tilbakelevere alle helse- og personopplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene som framgår av Avtalens punkt 13 på samme måte som Databehandler så langt det ikke strider mot andre lovbestemmelser.

Databehandler er til enhver tid fullt ut ansvarlig overfor Behandlingsansvarlig for alt arbeid som utføres av underleverandører og for underleverandørenes etterlevelse av bestemmelsene i denne Avtalen.

Tilgang til helse- og personopplysninger for tredjeparter krever konkret avtale utover denne Avtalen mellom partene for alle andre enn Databehandlers underleverandører.

**10. Overføring av personopplysninger til utlandet**

Partene i denne Avtalen er enige om at ingen av helse- og personopplysningene som behandles under denne Avtalen skal føres ut av Norge, med mindre det er særskilt avtalt mellom partene. I tillegg skal helse- og personopplysninger være plassert på servere i Norge (jf. arkivloven § 9 bokstav b). Eventuelle unntak som innebærer overføring til utlandet skal godkjennes eksplisitt av Dataansvarlig før behandlingen starter.

Databehandler bekrefter at ingen av underleverandørene overfører helse- og personopplysninger som omfattes av denne Avtalen til utlandet, med unntak for slike overføringer som er angitt i Vedlegg 3. Dette omfatter også fjerntilgang fra utlandet.

Bruk av underleverandører som overfører helse- og personopplysninger til land utenfor EU/EØS (tredjeland) skal avtales skriftlig med Dataansvarlig på forhånd. Ved overføring av helse- og personopplysninger til land utenfor EU/EØS (tredjeland) skal Databehandler benytte godkjente EU-overføringsmekanismer.

Ved overføring til utlandet, uavhengig av om det er innenfor EU/EØS eller utenfor EU/EØS (tredjeland), skal Databehandler gi nødvendig dokumentasjon om sikkerhet, risiko og etterlevelsesnivå knyttet til aktuelle underleverandører slik at Dataansvarlig får nødvendig informasjon for å kunne gjennomføre en særskilt risikovurdering. Dataansvarlig kan nekte samtykke til den aktuelle overføringen basert på spesifikke risikoer som fremkommer av Dataansvarliges egen risikovurdering.

**11. Taushetsplikt**

Databehandlers ansatte og andre som opptrer på Databehandlers vegne i forbindelse med behandling av personopplysninger i henhold til denne Avtalen, Tjeneste/oppdragsavtale og senere skriftlige avtaler mellom partene (heretter omtalt som «personer som er autorisert til å behandle personopplysningene»), er underlagt taushetsplikt etter denne Avtalen og gjeldende regelverk. Personer som er autorisert til å behandle helse- og personopplysningene forplikter seg til å behandle opplysningene fortrolig. Det samme gjelder eventuelle underleverandører.

Databehandler skal påse at alle som behandler personopplysninger under Avtalen er kjent med taushetsplikten.

Ansatte og andre som opptrer på Databehandlers vegne i forbindelse med behandling av personopplysninger skal ha undertegnet taushetserklæring. Bestemmelsen gjelder tilsvarende for underleverandører.

Partene har i tillegg taushetsplikt om konfidensiell informasjon knyttet til hverandres virksomhet, som er formidlet i forbindelse med oppdraget.

Partene plikter å ta de forholdsregler som er nødvendige for å sikre at materiale eller opplysninger ikke blir gjort kjent for andre i strid med dette punktet.

Taushetsplikten gjelder også etter Avtalens opphør.

**12. Innsyn, verifikasjon og revisjon**

Dataansvarlig kan til enhver tid kreve innsyn i og verifikasjon av Databehandlers behandling av personopplysninger tilhørende Dataansvarlig, herunder innsyn i og verifikasjon av dokumentasjon for oppfyllelse av kravene til informasjonssikkerhet og Databehandlers system for internkontroll.

Retten til innsyn gjelder alle tekniske, organisatoriske og administrative forhold som er relevante for sikkerheten ved behandlingen som utføres av Databehandler på vegne av Dataansvarlig, og øvrige innsynsrettigheter nedfelt i lov. Hvis Dataansvarlig ber om innsyn skal generell informasjon fra revisjonen gjøres tilgjengelig for andre dataansvarlige som benytter samme tjeneste hos Databehandler.

Dataansvarlig skal så vidt mulig gi Databehandler varsel i rimelig tid ved krav om innsyn og kontroll, vanligvis minst 30 dagers varsel. For krav om dokumentinnsyn bør det gis minst 14 dagers varsel. Dataansvarlig skal medvirke til at innsyn og kontroll kan koordineres mellom flere dataansvarlige som får levert tjenester fra Databehandler. Innsyn og kontroll kan gjennomføres av Dataansvarlig eller tredjepart som Dataansvarlig utpeker. Databehandler kan kreve dekket dokumenterte merkostnader som påløper ved slike revisjoner.

Databehandler skal gi Datatilsynet og annen relevant tilsynsmyndighet tilgang og innsyn i behandlingen av helse- og personopplysninger slik det følger av relevant lovgivning.

Databehandler skal uten ugrunnet opphold korrigere eventuelle avvik. Avvik som skyldes Databehandler eller dennes underleverandører skal korrigeres uten kostnad for Dataansvarlig. Databehandler skal skriftlig redegjøre for korrektive tiltak og plan for gjennomføring.

**13.** **Varighet og opphør**

Denne Avtalen gjelder fra den er signert av partene og gjelder til Avtalen og alle gjeldende avtaler mellom partene, som innebærer at Databehandler skal behandle helse- og personopplysninger på vegne av Dataansvarlig, er opphørt.

Ved opphør av Avtalen skal Databehandler tilrettelegge for og medvirke til tilbakeføring av alle opplysninger som Databehandler har mottatt og behandlet på vegne av Dataansvarlig. Partene avtaler nærmere hvordan overføring konkret skal skje.

Etter at alle opplysningene er overført til Dataansvarlig og bekreftet mottatt av denne, skal Databehandler irreversibelt slette eller forsvarlig destruere alle opplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene i sine systemer, med mindre ufravikelige rettsregler krever at helse- og personopplysningene fortsatt lagres.

Benyttes delt infrastruktur der direkte sletting ikke er teknisk mulig skal Databehandler sørge for at data gjøres utilgjengelig inntil disse dataene er overskrevet av systemet.

Databehandler skal gi Dataansvarlig skriftlig bekreftelse på at opplysningene er overført og slettet som angitt over.

**14.** **Endring av avtale**

I tilfelle endringer i gjeldende lovverk, endelig dom som gir en annen tolkning av gjeldende lov, eller endringer i tjenester i Tjeneste/oppdragsavtalen som krever endringer av denne Avtalen, skal partene samarbeide for å oppdatere Avtalen tilsvarende.

**15.** **Meddelelser**

Meddelelser, underretting, varsel eller annen kommunikasjon mellom Dataansvarlig og Databehandler skal gis skriftlig, eller bekreftes skriftlig til:

|  |  |
| --- | --- |
| Dataansvarlig | Databehandler |
| [Virksomhetens navn]  [Adresse] | **[Virksomhetens navn]**  [Adresse] |
| Navn:  Rolle:  E-post:  Mobilnr.: | Navn:  Rolle:  E-post:  Mobilnr.: |

**16.** **Lovvalg og verneting**

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

**17.** **Undertegning**

Denne Avtalen foreligger i to originaler, hvorav partene beholder et eksemplar hver.

Sted og dato:

[*skriv sted*], xx.xx.20xx

|  |  |
| --- | --- |
| Dataansvarlig | Databehandler |
|  |  |
| Navn: | Navn: |

**VEDLEGG 1 – BEHANDLINGENS FORMÅL, OPPLYSNINGER OG BEHANDLINGER**

Tabellene oppdateres fortløpende.

[*dato/måned/år*]

1. **Formålet med og varigheten av behandlingen**

Formålet med og varigheten av behandling av helse- og personopplysninger er: [*husk at hver behandling må være knyttet til spesifikke og uttrykkelig angitt formål – se eksempel nedenfor*]

|  |  |  |
| --- | --- | --- |
| Navn på tjeneste | Formålet med behandlingen | Varigheten av behandlingen |
|  |  |  |
|  |  |  |
|  |  |  |

**B. Behandling av helse- og personopplysninger**

Følgende behandlinger omfattes av Avtalen: *[her listes opp hvilke behandlinger av helse- og personopplysninger som omfattes – se eksempler nedenfor]*

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

**C. Typer av opplysninger**

Følgende helse- og personopplysninger behandles: *[her listes opp hvilke helse- og personopplysninger som omfattes – se eksempler nedenfor]*

|  |  |
| --- | --- |
| Personopplysninger | Helseopplysninger |
| navn  Brukernavn  Stilling  Telefonnummer  E-postadresse  Kommunikasjonsdata  Fødselsnummer  Bosted |  |

**D. Kategorier av registrerte**

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

|  |  |  |
| --- | --- | --- |
| Kategorier av registrerte | | |
|  |  |  |

**VEDLEGG 2a – Sikkerhetskrav**

*[her listes opp detaljerte krav til informasjonssikkerhet ved behov]*

**VEDLEGG 2b – Risikovurderinger**

*[her legges ved aktuelle risikovurdering av tjenesten/løsningen som databehandleravtalen omfatter]*

**VEDLEGG 3 – UNDERLEVERANDØRER**

*[her listes opp hvilke underleverandører som benyttes av Databehandler – se eksempler nedenfor]*

Tabellene oppdateres fortløpende.

[*dato/måned/år*]

|  |  |  |
| --- | --- | --- |
| Navn på underleverandør | Leveranseområde | Stedlig plassering |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |