

DATABEHANDLERAVTALE

I henhold til personopplysningsloven og
EUs Personvernforordning 2016/679

mellom

[Virksomhetens navn]

Org.nr.: 000 000 000

Dataansvarlig

og

[Virksomhetens navn]

Org.nr.: 000 000 000

Databehandler

Datert: xx.xx.20xx

1. Om avtalen

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

- Lov om behandling av personopplysninger av 15.juni 2018 nr. 38 (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 endrer eller erstatter disse.

Ved motstrid mellom Avtalens regulering og de rammer som følger av personopplysningslovgivningen eller relevant helselovgivingen, viker Avtalens regulering.

2. Definisjoner

Begrepene "personopplysninger", "behandling", "dataansvarlig", "databehandler", "brudd på opplysningssikkerhet" og "helseopplysninger" skal forstås slik de er definert i personvernforordningen § 4, helseregisterloven § 2 og pasientjournalloven § 2 som gjeldende.

"Avvik": brudd på opplysningssikkerhet og bruk av informasjonssystemet i strid med fastlagte rutiner.

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

3. Avtalens bakgrunn og formål

Denne Avtalen er inngått mellom partene og skisserer de generelle vilkårene for den behandling av helse- og personopplysninger som Databehandler utfører på vegne av Dataansvarlig.

Formålet med Avtalen er å sikre behandlingen av helse- og personopplysninger på vegne av Dataansvarlig slik at helse- og personopplysningene ikke brukes urettmessig eller kommer uberettigede i hende.

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"). 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.

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 virksomhetsperiode og som innebærer at Databehandler behandler helse- og personopplysninger på vegne av Dataansvarlig (heretter omtalt som "senere skriftlige avtaler mellom partene").

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

Formålet med og varigheten av behandling av helse- og personopplysninger, hvilke helse- og personopplysninger som behandles, kategorier av de registrerte og behandlingens art er angitt i **Vedlegg 1**.

Nærmere beskrivelse av behandlingen, behandlingens formål og hvilke helse- og personopplysninger som omfattes fremgår av Tjeneste/oppdragsavtalen og senere skriftlige avtaler mellom partene [*hvis relevant*].

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 personopplysningsloven, personvernforordningen, relevant helselovgivning og annen særlovgivning, samt denne Avtalen.

8. Databehandlers plikter

8.1. Generelt

Databehandler forplikter seg til å behandle helse- og personopplysninger kun i samsvar med all relevant lov og regelverk, denne Avtalen, 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 unnlattelse, sette Dataansvarlig i en slik situasjon at Dataansvarlig bryter noen bestemmelse i gjeldende lov og regelverk.

Databehandler skal ikke:

- a. 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;
- b. behandle helse- og personopplysninger utover det som er nødvendig for å oppfylle Databehandlers forpliktelser i henhold til de til enhver tid gjeldende avtaler;
- c. utlevere, overlate eller overføre helse- og personopplysninger i noen form på eget initiativ med mindre det er avtalt på forhånd med Dataansvarlig eller Dataansvarlig har godkjent dette skriftlig;
- d. samle inn fra eller overføre helse- og personopplysninger til en tredjepart;
- e. 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:

- a. ha løpende kontroll på alle kategorier av behandlingsaktiviteter utført på vegne av Dataansvarlig;
- b. gi Dataansvarlig tilgang til og innsyn i helse- og personopplysninger som behandles hos Databehandleren;
- c. føre og vedlikehold en oversikt over alle opplysninger og behandlinger eller dersom det er relevant, protokoll over sine egne behandlingsaktiviteter i henhold til personvernforordningen artikkel 30;
- d. treffe alle rimelige tiltak for å sikre at helse- og personopplysningene til enhver tid er korrekte og oppdaterte;
- e. etablere rutiner for å slette informasjon når den ikke lenger er nødvendig ut fra formålet med behandlingen og slette informasjon i henhold til fastsatte rutiner og retningslinjer;
- f. ha rutiner for og teknisk mulighet til å begrense behandlingen av den registrertes helse- og personopplysninger dersom den registrerte ønsker det med hjemmel i gjeldende lovgivning;

- g. påse at samtlige personer som gis tilgang til personopplysninger som behandles på vegne av Dataansvarlig er kjent med denne Avtalen og gjeldende avtaler mellom partene, og er underlagt disse avtalenes bestemmelser;
- h. sikre at krav til innebygd personvern og personvern som standardinnstilling innfris i Databehandlers løsninger. Dette inkluderer å bygge inn funksjonalitet for å oppfylle personvernprinsipper samt funksjonalitet for å sikre den registrertes rettigheter;
- i. gi Dataansvarlig nødvendig bistand slik at Dataansvarlig skal kunne oppfylle sine forpliktelser overfor de registrerte;
- j. samarbeide med og bistå Dataansvarlig ved oppfyllelse av de registrertes rettigheter knyttet til tilgang til opplysninger, herunder å svare på anmodninger fra den registrerte med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III;
- k. omgående underrette den Dataansvarlige dersom Databehandler mener at en instruks er i strid med personvernforordningen eller andre bestemmelser om vern av personopplysninger;
- l. 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.

Databehandleren skal:

- a. 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. 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;
- b. ha gode og hensiktsmessige internkontrollrutiner;
- c. 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;
- d. 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;

- e. 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;
- f. ved mistanke om eller konstatering av avvik, omgående varsle Dataansvarlig. 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;
- g. dokumentere ethvert avvik, herunder de faktiske forhold knyttet til avviket, dets virkninger og eventuelle iverksatte utbedringstiltak;
- h. omgående varsle Dataansvarlig ved uautorisert utlevering av personopplysninger;
- i. 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;
- j. 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;
- k. 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;
- l. varsle Dataansvarlig om alle forhold som medfører endring i risikobildet;
- m. 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 2** (hvis relevant).

Ved brudd på denne Avtalen eller på bestemmelsene i personopplysningslovgivningen, helselovgivningen eller annen relevant lovgivning 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 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 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. Ved bytte av underleverandør skal **Vedlegg 3** oppdateres og oversendes Dataansvarliges kontaktperson;
- g. sikre at Dataansvarlig og tilsynsmyndighetene har samme rett til innsyn og kontroll med behandling av personopplysninger hos en underleverandør som Dataansvarlig har overfor Databehandler etter Avtalens punkt 12;
- h. ved opphør av Avtalen, sikre at underleverandører oppfyller plikten til å slette eller forsvarlig destruere 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 Dataansvarlig 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.

9.1 Standardiserte tredjepartstjenester

Redigert av Oppdragsgiver HIKT: satt inn dette kapittel hentet fra Digitaliseringsdirektoratets mal, punkt 9.7

I den utstrekning Databehandleren benytter underleverandør som leverer standardiserte tredjepartstjenester som Dataansvarlig uttrykkelig har akseptert at leveres på underleverandørens standardvilkår i henhold til Hovedavtalen, og som Databehandleren følger opp på Dataansvarliges vegne, kan partene bli enige om at underleverandørens standard databehandleravtale legges til grunn og gjøres gjeldende direkte overfor Dataansvarlig som et direkte databehandlerforhold (altså ikke som Underdatabehandler) forutsatt at den oppfyller kravene i Gjeldende personvernregler. Databehandleren skal følge opp databehandleravtalen med underleverandøren på vegne av Dataansvarlig med mindre annet er avtalt i det enkelte tilfellet.

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 arkiververdige dokumenter med helse- og personopplysninger være plassert på servere i Norge (jf. arkivloven § 9 bokstav b), og eventuelle unntak fra dette skal godkjennes eksplisitt av Dataansvarlig før denne 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 etterlevelsensnivå 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 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]	[Virksomhetens navn]
[Adresse]	[Adresse]
Navn:	Navn:
Rolle:	Rolle:
E-post:	E-post:
Mobilnr.:	Mobilnr.:

16. Lovvalg og verneeting

Avtalen er underlagt norsk rett og partene vedtar Oslo tingrett som verneeting. 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]

A. 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
Filoverføringstjenesten	Overføre større datamengder	Til formålet er oppnådd

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	Legemiddelbruk
Fødselsnummer	Diagnoseopplysninger
Bosted	Opplysninger fra helseregistre

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		
Pasienter	Helsepersonell	Leverandører
Barn	Ansatte	Nøkkelpersoner
Foreldre	Tidligere ansatte	
Fullmektiger	Ansatte i samarbeidende firma	

VEDLEGG 2 – DETALJERTE KRAV TIL INFORMASJONSSIKKERHET

[her listes opp detaljerte krav til informasjonssikkerhet – se eksempler nedenfor]

Nr.	Tema	Krav
1.	Norm for informasjonssikkerhet i helse- og omsorgssektoren	Databehandler skal følge relevante krav i Norm for informasjonssikkerhet (se faktaark 6b, og hvilke krav som er angitt for databehandler)
2.	Sikring av data	Databehandler skal ha mekanismer for data under transport, prosessering og lagring for å ivareta integritet og konfidensialitet.
3.	Autentisering	Ved tilgang til data ved tjenstlig behov skal det benyttes personlige brukernavn med passord. Databehandler skal ha etablert passordpolicy.
4.	Tjenestenektangrep	
5.	Logging og sporbarhet	
6.	Redundans og skalering	
7.	Testdata	
8.	Sletting og tilbakelevering	
9.	Lagringstid	
10.	Backup og restore	
11.	Kryptering ved lagring	
12.	Kryptering i kommunikasjon	
13.		
14.		
15.		

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
ABC	Datasenter, hosting	Stockholm, Sverige
DEF	IT-supporttjenester	Oslo, Norge
XYZ	Backup	Paris, Frankrike