



Databehandleravtale

inngås mellom

Folkehelseinstituttet
Org. Nr. 983 744 516
Lovisenberggata 8
0456 OSLO
Norge

(behandlingsansvarlig)

og

[NAVN]
ORG. NR. [ORG. NR.]
[ADRESSE]
[POST NR. OG STED]
[LAND]

(databehandler)

hver for seg omtalt som en «Part» eller sammen som «Partene».

Partene har avtalt følgende avtalevilkår (Avtalevilkårene) for å oppfylle kravene i forordning 2016/679 (GDPR) og for vern av den registrertes rettigheter. Tre Vedlegg er inntatt i Avtalevilkårene og anses som omfattet av Databehandleravtalen.

1 Innledning

1. Disse Avtalevilkårene regulerer rettigheter og plikter for behandlingsansvarlig og databehandler, når det behandles personopplysninger på vegne av den behandlingsansvarlige.
2. Avtalevilkårene er utformet for å sikre Partenes overholdelse av artikkel 28 nr. 3 i Europaparlaments- og rådsforordning (EU) 2016/679 vedtatt 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (GDPR) og Lov om behandling av personopplysninger av 15. juni 2018 nr.38 og tilhørende forskrifter (heretter Personvernregelverket).
3. Der Avtalevilkårene inneholder ord og begreper som er definert i GDPR, har de samme betydning som i forordningen.
4. I forbindelse med aktivitet som beskrevet i Vedlegg A vil databehandleren behandle personopplysninger på vegne av den behandlingsansvarlige i henhold til Avtalevilkårene.
5. Ved motstrid skal Avtalevilkårene ha forrang over andre bestemmelser i andre avtaler når det gjelder forhold spesifikt knyttet til behandling av personopplysninger som beskrevet i Vedlegg A.
6. Vedlegg A inneholder den behandlingsansvarliges instruks for behandlingen av personopplysninger, detaljer om behandlingen av personopplysninger, herunder behandlingens formål og art, typen personopplysninger, kategorier av registrerte og varigheten av behandlingen.
7. Vedlegg B inneholder den behandlingsansvarliges vilkår for databehandlerens bruk av underdatabehandlere og en liste over underdatabehandlere godkjent av den behandlingsansvarlige.
8. Vedlegg C inneholder en beskrivelse av databehandlerens minimum sikkerhetstiltak ved behandling av personopplysninger og hvordan revisjoner av databehandleren og eventuelle underdatabehandlere skal gjennomføres.
9. Ved motstrid mellom Avtalevilkårene og de rammer som følger av Personvernregelverket eller annen relevant lovgivning, viker Avtalevilkårene.

2 Behandlingsansvarliges rettigheter og plikter

1. Den behandlingsansvarlige er ansvarlig for å sikre at behandlingen av personopplysninger utføres i samsvar med Personvernregelverket, relevant helselovgivning og Avtalevilkårene.
2. Den behandlingsansvarlige bestemmer formålet med og rammene for behandlingen av personopplysningene.
3. Den behandlingsansvarlige er ansvarlig for at det foreligger lovlig behandlingsgrunnlag for personopplysningene som databehandler behandler på vegne av behandlingsansvarlig. Behandlingsgrunnlaget er beskrevet i Vedlegg A.

3 Databehandleren skal følge behandlingsansvarliges instruks

1. Databehandleren skal kun behandle personopplysninger på instruks fra den behandlingsansvarlige. Hvis annen behandling er nødvendig for å oppfylle forpliktelser som databehandler er underlagt i henhold til gjeldende rett, skal databehandleren underrette den behandlingsansvarlige før slik behandling, med mindre loven forbyr dette av hensyn til viktige samfunnsinteresser.

Behandlingsansvarliges instruks er spesifisert i Vedlegg A. Databehandleren skal omgående underrette den behandlingsansvarlige dersom vedkommende mener at instruksen gitt av den behandlingsansvarlige er i strid med Personvernregelverket.

2. Dersom databehandler går utover instruksen ved selv å fastsette formålene med og midlene for behandlingen, skal databehandleren anses for å være behandlingsansvarlig med hensyn til nevnte behandling i henhold til GDPR artikkel 28 nr. 10.

4 Konfidensialitet

1. Databehandleren skal kun gi tilgang til personopplysninger som behandles på vegne av den behandlingsansvarlige til personer som er under databehandlerens instruksjonsmyndighet, som er forpliktet til konfidensialitet eller er underlagt lovfestet taushetsplikt, og som har nødvendig behov for tilgang.
2. Databehandleren skal på anmodning fra den behandlingsansvarlige dokumentere at de involverte personene under databehandlerens myndighet er omfattet av ovennevnte forpliktelser.

5 Sikkerhet ved behandlingen

1. Den behandlingsansvarlige skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til vurdert risiko i henhold til GDPR artikkel 32.
2. I henhold til GDPR artikkel 32, skal databehandleren – uavhengig av den behandlingsansvarlige – vurdere risikoen til rettigheter og friheter for fysiske personer som omfattes av behandlingen og implementere tiltak for å redusere risikoen. For dette formål skal den behandlingsansvarlige på forespørsel gi databehandleren all informasjon som er nødvendig for å identifisere og vurdere slik risiko.
3. Databehandleren skal bistå den behandlingsansvarlige i å sikre overholdelse av den behandlingsansvarliges plikter etter GDPR artikkel 32-36, ved å bl.a. å sørge for at den behandlingsansvarlige får informasjon om tekniske og organisatoriske tiltak som er implementert av databehandleren i henhold til GDPR artikkel 32-36 sammen med all annen informasjon som er nødvendig for etterlevelse av GDPR artikkel 32-36.
4. Databehandler skal dokumentere egen sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, risikovurderinger og etablerte tekniske, fysiske eller organisatoriske sikringstiltak. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

5. Spesifikke sikkerhetskrav som gjelder ved behandlingen av personopplysninger i tillegg til Avtalevilkårene og krav til dokumentasjon fremgår av Vedlegg C.

6 Bruk av underdatabehandlere

1. Databehandleren skal overholde kravene inntatt i artikkel 28 nr. 2 og nr. 4 i GDPR når databehandler engasjerer en annen databehandler for å utføre spesifikke behandlingsaktiviteter på vegne av behandlingsansvarlig (en underdatabehandler).
2. Databehandleren skal kun engasjere underdatabehandlere dersom det foreligger særlig skriftlig tillatelse fra den behandlingsansvarlige. Slik tillatelse må foreligge før den aktuelle underdatabehandler engasjeres og får tilgang til personopplysninger. Liste over underdatabehandlere som allerede er godkjent av den behandlingsansvarlige skal inntas i Vedlegg B.
3. Dersom databehandleren engasjerer en underdatabehandler skal de samme forpliktelsene som er fastsatt i denne Databehandleravtalen bli pålagt underdatabehandleren ved avtale. I denne avtalen skal det gis tilstrekkelige garantier for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne Databehandleravtalen og GDPR.
4. En kopi av slik underdatabehandleravtale og etterfølgende endringer skal – på den behandlingsansvarliges forespørsel – oversendes den behandlingsansvarlige, og dermed gi den behandlingsansvarlige muligheten til å sikre at de samme plikter for behandling av personopplysninger pålegges underdatabehandleren.
5. Dersom underdatabehandleren ikke oppfyller sine forpliktelser skal databehandleren overfor den behandlingsansvarlige ha fullt ansvar for at underdatabehandler oppfyller sine forpliktelser. Databehandleren har også plikt til å underrette den behandlingsansvarlige om enhver manglende oppfyllelse fra underdatabehandlerens side av dennes kontraktsrettslige forpliktelser.

7 Overføring av personopplysninger til tredjestater eller internasjonale organisasjoner

1. Enhver overføring av personopplysninger til land utenfor EØS-området (tredjestat) eller til internasjonale organisasjoner av databehandleren skal kun finne sted på grunnlag av dokumenterte instruksjoner fra den behandlingsansvarlige. Behandlingsansvarliges instruks for overføring skal fremgå av Vedlegg A.

Hvis annen overføring er nødvendig for å oppfylle forpliktelser som databehandler er underlagt i henhold til gjeldende rett, skal databehandleren underrette den behandlingsansvarlige før overføringen, med mindre loven forbyr dette av hensyn til viktige samfunnsinteresser.

2. Overføring til tredjestater eller internasjonale organisasjoner skal kun finne sted dersom det foreligger nødvendige garantier for tilstrekkelig beskyttelsesnivå for personvern i henhold til Personvernregelverket og i overensstemmelse med GDPR kapittel V.

8 Bistand til den behandlingsansvarlige

1. Databehandleren skal, i den grad det er mulig, bistå den behandlingsansvarlige med å oppfylle den behandlingsansvarliges plikt til å svare på anmodninger fra den registrerte med henblikk på å utøve sine rettigheter fastsatt i GDPR kapittel III. Databehandleren underretter straks den behandlingsansvarlige om enhver anmodning fra de registrerte. Databehandleren skal ikke selv besvare anmodninger, med mindre den behandlingsansvarlige har gitt tillatelse til dette.
2. Databehandleren skal bistå den behandlingsansvarlige med overholdelse av:
 - a. Den behandlingsansvarliges plikt til å uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde brudd på personopplysnings-sikkerheten til Datatilsynet, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter,
 - b. den behandlingsansvarliges plikt til å underrette om brudd på personopplysnings-sikkerheten til den registrerte, dersom det er sannsynlig at bruddet på personopplysnings-sikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter,
 - c. den behandlingsansvarliges plikt til å foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personvernet (en vurdering av personvernkonsekvenser - DPIA) i henhold til GDPR artikkel 35,
 - d. den behandlingsansvarliges plikt til å rådføre seg med Datatilsynet (forhåndsdrøftinger) i henhold til GDPR artikkel 36,
 - e. forpliktelsen til å sikre at personopplysningene er korrekte og oppdaterte, ved straks å underrette behandlingsansvarlig dersom databehandleren blir oppmerksom på at personopplysningene som behandles er ukorrekte eller er blitt foreldet.

9 Melding om brudd på personopplysnings-sikkerheten

1. I tilfelle brudd på personopplysnings-sikkerheten, skal databehandleren underrette den behandlingsansvarlige uten ubegrunnet opphold.
2. Brudd på personopplysnings-sikkerheten vil si et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller til personopplysninger som er overført, lagret eller på annen måte behandlet, jf. GDPR artikkel 4 nr. 12. Dette kan for eksempel være datainnbrudd og omfattende forsøk på datainnbrudd, distribusjon av personopplysninger til uautoriserte mottakere, tyveri og annet tap av lagringsmedier (uavhengig av om disse er kryptert eller ikke), eller manglende etterlevelse av tiltak i vedlegg C.

3. Underretning om brudd på personopplysningssikkerheten etter punkt 9.1 skal;
 - a. beskrive arten av bruddet på personopplysningssikkerheten, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt,
 - b. inneholde navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes,
 - c. beskrive de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten, og
 - d. beskrive de tiltak som databehandleren har truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.

Informasjonen kan i den grad det det er nødvendig gis trinnvis uten ytterligere ugrunnet opphold.

Brudd på personopplysningssikkerheten skal varsles til kontaktperson som angitt i Vedlegg A, både per e-post og telefon, med kopi til; folkehelseinstituttet@fhi.no. Behandlingsansvarliges personvernombud skal også varsles; <mailto:personvernombud@fhi.no>.

4. I henhold til punkt 8(2)(a), skal databehandleren bistå den behandlingsansvarlige i å melde brudd på personopplysningssikkerheten til Datatilsynet, hvilket omfatter at databehandleren skal bistå i å innhente informasjon i henhold til GDPR artikkel 33 nr. 3.

10 Sletting og tilbakelevering av personopplysninger

Ved opphør av aktivitetene vedrørende behandling av personopplysninger, er databehandleren forpliktet til å tilbakelevere eller slette alle personopplysninger som er behandlet på vegne av den behandlingsansvarlige under Avtalevilkårene i samsvar med bestemmelsene i Vedlegg A. Anonymisering er ikke likestilt med sletting.

11 Sikkerhetsrevisjon og inspeksjoner

1. Databehandleren skal på forespørsel gjøre tilgjengelig for den behandlingsansvarlige all informasjon som er nødvendig for å påvise overholdelse av pliktene som følger av GDPR artikkel 28 og Avtalevilkårene. Databehandler skal tillate og bidra til sikkerhetsrevisjoner, inkludert inspeksjoner, utført av den behandlingsansvarlige eller annen uavhengig tredjepart bemyndiget av den behandlingsansvarlige. Sikkerhetsrevisjonen kan omfatte gjennomgang av rutiner, stikkprøver, mer omfattende stedlige kontroller og andre egnede kontrolltiltak.
2. Databehandler plikter selv å gjennomføre sikkerhetsrevisjoner jevnlig. Databehandler skal dokumentere at de har gjennomført sikkerhetsrevisjoner og slik dokumentasjon skal være tilgjengelig for den behandlingsansvarlige på forespørsel.
3. Etter relevant lovgivning kan et tilsynsorgan pålegge både behandlingsansvarlig og databehandler å fremlegge informasjon og gi tilgang som er nødvendig for at tilsynet skal

kunne utføre sine oppgaver. Datatilsynets tilgang til lokaler og utstyr er hjemlet i GDPR artikkel 58 nr. 1 bokstav f.

12 Erstatning

1. Partene er ansvarlige overfor hverandre for eventuelle tap, kostnader og skader som oppstår på grunn av Partens unnlattelse av å overholde sine forpliktelser i henhold til denne Databehandleravtalen.
2. Ingen av Partene er ansvarlig for indirekte skade, følgeskade eller lignende skade som en annen Part pådrar seg.
3. Eventuell erstatningsbegrensning avtalt i tilknyttede avtaler gjelder ikke erstatning etter denne Databehandleravtalen.

13 Lovvalg og verneting

Databehandleravtalen er underlagt norsk rett og Partene velger Oslo tingrett som verneting. Dette gjelder også etter opphør av Databehandleravtalen.

14 Avtalens varighet

1. Denne Databehandleravtalen trer i kraft når den er signert av begge Parter.
2. Denne Databehandleravtalen skal gjelde så lenge databehandler behandler personopplysninger på vegne av den behandlingsansvarlige.

15 Signatur

For den behandlingsansvarlige:

[sted], den [dato]

For databehandleren:

[sted], den [dato]

.....
[Navn]
[Tittel]
[Avdeling]
Folkehelseinstituttet

.....
[Navn]
[Tittel]
[Avdeling]
[Virksomhet]

Vedlegg A Instruks vedrørende behandling av personopplysninger

A.1. Bakgrunn og formål med behandlingen

Partene har inngått avtale om levering av tjenester («Hovedavtalen») som innebærer at databehandler behandler personopplysninger på vegne av behandlingsansvarlig.

Behandlingen av personopplysninger er knyttet til leveranse, konfigurasjon, support, vedlikehold og videreutvikling av nytt system for adgangskontroll. Systemet skal benyttes til å administrere fysisk adgang til behandlingsansvarliges lokaler og områder, herunder utstedelse og administrasjon av adgangskort, tilganger og tilhørende brukerprofiler.

For å sikre korrekt og effektiv tilgangsstyring skal adgangskontrollsystemet integreres med behandlingsansvarliges personalsystem og besøkssystem. Integrasjonene er nødvendige for at relevante og oppdaterte personopplysninger kan overføres til adgangskontrollsystemet, slik at adganger kan opprettes, endres og avsluttes i samsvar med den enkeltes tilknytning, rolle og adgangsbehov.

Formålet med behandlingen er å ivareta behandlingsansvarliges behov for sikker, sporbar og administrerbar fysisk adgangskontroll, samt å sikre at personopplysninger i adgangskontrollen til enhver tid er tilstrekkelige, korrekte og oppdaterte. Behandlingen av personopplysninger er nødvendig fordi databehandleren skal levere og konfigurere løsningen på vegne av behandlingsansvarlig, herunder håndtere teknisk konfigurasjon, integrasjoner, feilretting, vedlikehold, support og eventuelle oppgraderinger.

A.2. Behandlingsaktiviteter

Databehandleren skal utføre følgende behandlingsaktiviteter på vegne av den behandlingsansvarlige:

Tilgjengeliggjøring, lagring og sammenstilling av personopplysninger.

A.3. Type personopplysninger

Databehandlerens behandling av personopplysninger på vegne av behandlingsansvarlige omfatter følgende personopplysninger om de registrerte:

Personopplysninger som skal behandles er hentet fra behandlingsansvarliges personalsystem, besøkssystem og system for adgangskontroll.

Personopplysninger som skal behandles er foto, fullt navn, telefonnummer, e-post, arbeidsgiver, personellkategori, organisasjonstilhørighet hos behandlingsansvarlig og adgangsløgg. Følgelig skal det behandles både direkte og indirekte identifiserbare opplysninger.

A.4. Behandlingen omfatter følgende kategorier av registrerte

Databehandlerens behandling av personopplysninger på vegne av behandlingsansvarlig omfatter følgende kategorier av registrerte:

Kategorier personopplysningene omfatter er ansatte, eksterne betalte/ ubetalte, gjester og tjenesteleverandører hos behandlingsansvarlig.

A.5. Behandlingen har følgende varighet

Databehandlerens behandling av personopplysninger på vegne av behandlingsansvarlig har følgende varighet:

Databehandlerens behandling av personopplysninger på vegne av Behandlingsansvarlig er ikke tidsbegrenset, og varer frem til opphør av Hovedavtalen mellom Partene.

A.6. Rutiner for tilbakelevering og sletting av personopplysninger

Ved opphør av Databehandleravtalen eller av databehandlers behandling av personopplysninger på behandlingsansvarliges vegne, skal personopplysninger tilbakeleveres og slettes i samsvar med Databehandleravtalen punkt 10. Databehandler skal bekrefte skriftlig overfor behandlingsansvarlig at sletting eller tilbakelevering av personopplysninger er foretatt, og skal på forespørsel dokumentere hvordan det er gjennomført.

Partene har avtalt følgende om sletting/tilbakelevering av personopplysninger:

Databehandler skal ikke lagre eller på annen måte oppbevare personopplysninger i egne systemer. Behandling av personopplysninger skal skje i behandlingsansvarliges systemer.

Dersom databehandler besitter personopplysninger i egne systemer, skal disse slettes uten ugrunnet opphold og senest 90 kalenderdager etter opphør av Hovedavtalen.

A.7. Behandlingssted

Behandling av personopplysninger etter databehandleravtalen skal ikke utføres på andre lokasjoner enn de følgende uten at det foreligger skriftlig forhåndssamtykke fra den behandlingsansvarlige:

Behandling av personopplysninger etter databehandleravtalen skal kun finne sted på behandlingsansvarlig sine lokasjoner i Norge, herunder i behandlingsansvarlig sine egne servermiljøer og IKT-nett. Det skal ikke utføres behandling på andre lokasjoner uten at det foreligger skriftlig forhåndssamtykke fra den behandlingsansvarlige, og da utelukkende på autorisert maskinvare via sikre kommunikasjonsløsninger inn til behandlingsansvarlig sitt IKT-nett av personell med tjenstlig behov og nødvendige tilgangsrettigheter.

A.8. Instruks for overføring av personopplysninger til tredjestat eller internasjonal organisasjon

Behandlingen av personopplysninger som databehandleravtalen omfatter medfører ikke overføring av personopplysninger til tredjestat eller internasjonal organisasjon.

A.9. Den behandlingsansvarliges og databehandlers kontaktopplysninger

Partene kan kontakte hverandre ved følgende kontakter/kontaktpunkter:

Administrativt ansvarlig:

Hos behandlingsansvarlig:

[Navn]

[Adresse]

[E-postadresse]

[Telefon]

Hos databehandler:

[Navn]

[Adresse]

[E-postadresse]

[Telefon]

Personvernombud:

Hos behandlingsansvarlig:

[Navn]

[E-postadresse]

[Telefon]

Hos databehandler (hvis aktuelt):

[Navn]

[E-postadresse]

[Telefon]

Informasjonssikkerhetsansvarlig:

Hos behandlingsansvarlig:

[Navn]

[E-postadresse]

[Telefon]

Hos databehandler (hvis aktuelt):

[Navn]

[E-postadresse]

[Telefon]

Partene skal være forpliktet til å fortløpende informere hverandre om endringer i kontakter/kontaktpunkter.

Vedlegg B Godkjente underdatabehandlere

B.1. Godkjente underdatabehandlere

Ved inngåelse av denne Databehandleravtalen gir den behandlingsansvarlige databehandler tillatelse til engasjement av følgende underdatabehandlere:

NAVN	ORG. NR.	ADRESSE	BEHANDLINGSSTED	BESKRIVELSE AV BEHANDLINGEN
[Navn]	[org.nr.]	[Adresse]	[Oppgi land hvor opplysningene lagres, oppnås tilgang fra eller på andre måter behandles]	[Overordnet beskrivelse av behandlingen hos underdatabehandleren]

Den behandlingsansvarlige skal ved inngåelse av denne Databehandleravtalen gi tillatelse til bruk av de ovennevnte underdatabehandlere for behandlingen beskrevet for denne. Databehandleren skal ikke ha rett til – uten den behandlingsansvarliges eksplisitte skriftlige tillatelse – å engasjere en underdatabehandler for annen behandling enn den som er blitt avtalt eller benytte en annen underdatabehandler til å foreta den beskrevne behandlingen.

B.2. Tidsperiode for forutgående varsel og aksept av nye underdatabehandlere

Databehandler skal varsle behandlingsansvarlige ved endring av underdatabehandlere **minimum 1 måned** før disse får tilgang til personopplysninger som behandles på vegne av behandlingsansvarlige. Databehandler må motta skriftlig tillatelse fra behandlingsansvarlig før endringen kan foretas.

Vedlegg C Krav til tekniske og organisatoriske tiltak

Databehandleren skal etablere og etterkomme nødvendige tekniske og organisatoriske tiltak med hensyn til vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet ved behandling av personopplysninger for å sikre tilfredsstillende informasjonssikkerhet i henhold til personvernregelverket, herunder kravene etter personvernforordningen artikkel 32, og gjeldende helselovgivning.

Sikkerhetsnivået skal ta hensyn til art, omfang, sammenheng og formål av behandlingsaktivitetene, samt risiko av varierende sannsynlighets- og alvorlighetsgrad for personvernet. Når særlige kategorier av personopplysninger behandles, som f.eks. helseopplysninger, stilles høyere krav til sikkerhetstiltakene. Prinsippene for innebygd personvern skal følges.

Skjemaet fylles ut av databehandler. Sikkerhetstiltakene skal være dokumentert, og utfyllende dokumentasjon vedlagt/henvist ved lenke.

Sikkerhetstiltakene skal være egnet og tilstrekkelig i forhold til hva som er mulig, tilgjengelig og generelt anbefalt, og skal vurderes ut fra personopplysningenes sensitivitet.

Område	Ja/Nei	Henvisning til dokument/ utfyllende informasjon
Sikkerhetsstrategi og organisering		
Databehandler har en sikkerhetsstrategi og en informasjonssikkerhetspolicy som er vedtatt av ledelsen.		[Bør legges ved.]
Databehandler har en sikkerhetsorganisasjon med klare ansvarsområder.		
Databehandler har et personvernombud.		[Hvis nei: Er det vurdert om det er pålagt?]
Ansatte gis systematisk opplæring i relevante sikkerhetskrav og krav til håndtering av personopplysninger.		
Ansatte og oppdragstakere har signert taushetserklæring.		
Databehandler er underlagt sertifiseringsordninger for sikkerhet.		[Hvis ja: Hvilke? Eventuelle sertifikater/resultater fra revisjon legges ved avtalen]
Databehandler er underlagt Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten.		[Et krav hvis virksomheten er tilknyttet Norsk helsenett]
Databehandler gjennomfører revisjon av IT-systemene minst årlig og ved større endringer.		[Relevante revisjonsdokumenter bør kunne fremlegges for Behandlingsansvarlig]
Databehandler gjennomfører risiko- og sårbarhetsanalyser av sikkerhetstiltakene jevnlig og ved større endringer		[Relevante ROS-analyser bør kunne fremlegges for Behandlingsansvarlig]
Databehandler følger opp underleverandører, og at: <ul style="list-style-type: none"> de etterlever Databehandleravtalen og Personvernregelverket, og oppfyller sikkerhetstiltakene i dette bilaget på samme måte som Databehandleren, der det er relevant. 		

Område	Ja/Nei	Henvvisning til dokument/ utfyllende informasjon
Forvaltning av systemer som inngår i leveransen		
Databehandler har rutiner for å ivareta prinsipper for innebygd personvern.		[Se f.eks.: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/]
Databehandler har oversikt over utstyr, programvare og tjenester som benyttes i leveransen.		
Databehandler har prosesser som sikrer at sikkerhet er en integrert del av informasjonssystemene i hele livssyklusen, fra anskaffelse, utvikling, vedlikehold, til avhending (innebygd personvern).		

Område	Ja/Nei	Henvvisning til dokument/ utfyllende informasjon
Tekniske sikkerhetstiltak		
Det er etablert adgangskontroll til lokaler og utstyr.		
Det er etablert tilgangsstyring- og kontroll av alle systemer. Kun ansatte med tjenstlig behov har tilgang til systemer som inneholder personopplysninger databehandler behandler på vegne av behandlingsansvarlig. All autorisert og uautorisert tilgang til personopplysninger skal registreres.		
Databehandler har kontroll over alt utstyr og programvare som brukes til behandling av personopplysningene. For eksempel oversikt over godkjent programvare, fjernstenging- og styring.		
Det gjennomføres inntrengningstester for kritiske eller spesielt utsatte systemer.		
Det brukes kryptering i tråd med god praksis for å sikre informasjon ved lagring.		
Metoder for sikker kommunikasjon, som autentisering og kryptering, sikrer informasjonen ved overføring mellom parter eller systemer.		
Det er etablert systemer for å ivareta driftssikkerheten, som omfatter <ul style="list-style-type: none"> • kontinuerlig oppdatering av all programvare • systemplanlegging • kapasitetsplanlegging • egne miljøer for utvikling og test • systemer for endringskontroll. 		
Det er etablert systemer for håndtering av tekniske sårbarheter, som automatisk sårbarhetsscanning, sikkerhetskopiering, logging og overvåking, og tiltak for beskyttelse mot ødeleggende programvare.		

Område	Ja/Nei	Henvisning til dokument/ utfyllende informasjon
Kritiske driftsprosesser er beskyttet mot uønskede hendelser og katastrofer, og driftsprosessene kan gjenopptas på kort tid.		
Databehandler har prosesser for å håndtere flytting, gjenbruk, fjerning, avhending og destruksjon av utstyr og informasjon.		

Område	Ja/Nei	Henvisning til dokument/ utfyllende informasjon
Hendelsehåndtering		
Databehandler har tiltak for å oppdage feil, sikkerhetshendelser og sikkerhetsbrudd så raskt som mulig. Avvik logges.		
Databehandler har skriftlige rutiner for å håndtere alvorlige sikkerhetshendelser		
Alvorlige hendelser blir evaluert og gjennomgått for å unngå gjentagelser.		
Sikkerhetshendelser som påvirker leveransen, blir varslet til Behandlingsansvarlige så snart som mulig og uten unødvendige forsinkelser.		[Viktig for å ivareta Behandlingsansvarliges forpliktelser om varsling innen 72 timer for brudd på personopplysningssikkerheten, jf. Databehandleravtalen punkt 9.]