DATABEHANDLERAVTALE – BILAG 1a

Krav til leverandør ved kjøp av tjenester.

Nr.	Krav	Ivaretatt	Kommentar
Generelle krav			
1.	Leverandøren plikter å følge Normen og oppfylle kravene i denne		
2.	Leverandøren skal til enhver tid oppfylle de krav til informasjonssikkerhet som følger av databehandleravtalen og databehandlingsansvarliges sikkerhetsstrategi. Resultat fra gjennomført risikovurdering skal fremlegges av databehandler som dokumentasjon av egen og eventuelle underleverandørers sikkerhet		
3.	Leverandøren skal vedlegge sikkerhetsmål, sikkerhetsstrategi og ansvar for informasjonssikkerheten		
4.	Leverandøren plikter å behandle all informasjon i henhold til databehandleravtalen		
5.	Leverandøren kan ikke benytte underleverandører i forbindelse med velferdsteknologien uten at det er skriftlig avtalt med virksomheten		
6.	Leverandøren skal sikre at informasjon som behandles på vegne av virksomheten holdes adskilt fra egne og andre virksomheters informasjon og tjenester		
7.	Leverandøren plikter å dokumentere sitt system for behandling av helse- og personopplysninger i forbindelse med databehandleravtalen. Med dokumentasjon menes bl.a. beskrivelse av prosedyrer for autorisasjon, autentisering og bruk, samt tekniske og organisatoriske sikkerhetstiltak. Dokumentasjon skal være tilgjengelig for virksomheten, Datatilsynet og Helsetilsynet.		
Krav til logging			
8.	Leverandøren skal sikre at all tilgang og bruk av velferdsteknologien logges		
9.	Loggene skal samles inn og tilgjengeliggjøres for virksomheten		
10.	Loggene skal oppbevares så lenge avtalen med kunder spesifiserer det		
11.	Følgende skal som minimum registreres i loggene: • entydig identifikator for den autoriserte brukeren • rollen den autoriserte brukeren har ved tilgangen • virksomhetstilhørighet • organisatorisk tilhørighet til den som er autorisert • hvilke type opplysninger det er gitt tilgang til • grunnlaget for tilgangen • tidspunkt og varighet for tilgangen		
Leverandøren skal sikre at følgende minimumskrav til teknisk sikkerhet er oppfylt			
12.	Tilgang til tjenester og opplysninger i nettverket og IKT-systemet skal være basert på individuelle brukernavn og passord		
13.	Opplysninger overlevert av virksomheten skal sikres, slik		

	at kun autoriserte medarbeidere har tilgang		
14.	Tilgang til eksterne nett/Internett/helsenett, inkludert leverandørens åpne nettverk, skal sikres med sikkerhetstiltak som ikke kan påvirkes eller omgås av eksterne og egne ansatte, og som forhindrer uforvarende eksponering av sensitive personopplysninger til nettverk med lavere sikkerhet		
15.	Ved bruk av fjernaksess skal alle sikkerhetstiltak og avtale innføres iht. til dokumentet "Veileder for fjernaksess"		
16.	Hvis leverandøren behandler helse- og personopplysninger for flere virksomheter skal leverandøren ved hjelp av tekniske tiltak som ikke kan overstyres av brukerne ivareta at det er etablert skiller mellom virksomhetene i henhold til gjennomført risikovurdering. Dette gjelder både hvor data er lagret og i kommunikasjon		
Krav til tilgangsstyring			
17.	Leverandøren skal ha prosedyrer for å autorisere kun de av leverandørens medarbeidere som har et reelt behov for tilgang til velferdsteknologien og opplysninger for å gjennomføre leveransen/tjenesten		
18.	Leverandøren skal til enhver tid ha oversikt over eget personell som er autorisert for tilgang til velferdsteknologien og informasjon. På forespørsel skal slik oversikt forelegges virksomheten		
19.	Det skal benyttes personlig brukerkonto for all tilgang knyttet til gjennomføring av leveransen		
20.	Dersom leverandøren benytter mobilt utstyr til drift, skal leverandøren ha prosedyrer som sikrer at disse bare benyttes av driftspersonell og til driftsrelaterte oppgaver		
21.	Dersom tredjepart eller underleverandør, i forbindelse med support eller tilsvarende, skal ha tilgang til velferdsteknologien, skal alle sikkerhetstiltak iht. til dokumentet "Veileder for fjernaksess" ivaretas		
Taushetsplikt			
22.	Leverandørens ansatte og andre som opptrer på leverandørens vegne i forbindelse med velferdsteknologien er underlagt taushetsplikt, jf. pasientjournalloven § 15, helsepersonelloven og forvaltningsloven. Det samme gjelder eventuelle underleverandører. Leverandøren skal påse at alle som behandler helse- og personopplysninger er kjent med taushetsplikten		
23.	Alle ansatte og andre som opptrer på leverandørens vegne i forbindelse med velferdsteknologien skal ha undertegnet taushetserklæring. Bestemmelsen gjelder tilsvarende for eventuelle underleverandører		
24.	Taushetsplikten gjelder også etter databehandleravtalens opphør		
Tilbakerapportering			
25.	Leverandøren skal jevnlig gi statusrapporter om resultater fra sine ansvarsområder. Eksempler på hva som skal inngå i rapportering fra databehandler: • Driftsstatus på kritiske systemer • Oppetid på systemer		

	• Planlagte avbrudd og tidslengde på avbrudd • Planlagte endringer, forventet effekt og tidspunkt de skal utføres • Forsøk på uautorisert bruk • Sikkerhetsoppdateringer • Feilsituasjoner/ -rettinger • Manglende oppfyllelse av tjenesteavtale og mulige årsaker		
Avvikshåndtering			
26.	Leverandøren skal gjennomføre avvikshåndtering på informasjonssikkerhet (se personopplysningsforskriften) etter en fastlagt rutine. Ved alvorlige hendelser skal leverandøren melde avviket til virksomheten uten opphold		