KROMANN REUMERT

TILSYNSRAPPORT - 2023-2024

Tilsyn med databehandleren CompuGroup Medical Denmark A/S

Udarbejdet / senest opdateret: 22. august 2024

1. INDLEDENDE BEMÆRKNINGER

Praktiserende Lægers Organisation (”**PLO**”) fører tilsyn med de systemhuse, der leverer journalsystemer til de praktiserende læger i Danmark. Tilsynet føres af PLO, med bistand fra Kromann Reumert, på vegne af de praktiserende læger, der – efter endt tilsyn – får adgang til denne tilsynsrapport.

Nærværende tilsynsrapport skal anses som dokumentation for det tilsyn, der er ført med CompuGroup Medical Denmark A/S (”**Databehandleren**”) overholdelse af den databehandleraftale (”**Databehandleraftalen**”), der er indgået mellem Databehandleren og de enkelte dataansvarlige praktiserende læger.

De praktiserende læger er selvstændigt dataansvarlige for den behandling af personoplysninger, der sker hos Databehandleren. Den enkelte praktiserende læge er derfor ansvarlig for at forholde sig til indholdet i denne tilsynsrapport. Hvis den enkelte praktiserende læge ikke finder tilsynsrapporten tilstrækkelig eller finder, at der er behov for udbedring af visse forhold, er den praktiserende læge ansvarlig for at sikre dette – eventuelt via orientering til PLO, der i så fald kan bistå den dataansvarlige praktiserende læge.

2. SAMLET KONKLUSION OM DATABEHANDLERENS EFTERLEVELSE AF DATABEHANDLERAFTALEN

Databehandlerens efterlevelse af kravene i Databehandleraftalen vurderes samlet set at være tilfredsstillende.

3. MATERIALE

Tilsynet, der danner udgangspunktet for denne tilsynsrapport, er baseret på følgende materiale (”Materialet”), som PLO har modtaget fra Databehandleren:

- Udfyldt spørgeskema af 11. april 2024. Spørgeskemaet er udfyldt af Kjeld Gandrup, Country Data Protection Officer i CompuGroup Medical Denmark A/S.
- Oversigt over underdatabehandlere (udklip fra databehandleraftale).
- ISO 27001:2022 certifikat, gyldigt fra 12. juli 2023 til 11. juli 2026.
- Mail fra Kjeld Gandrup af 7. august 2024
- Telefonsamtale med Kjeld Gandrup den 8. august 2024, inkl. opfølgende mail derpå.

Tilsynsrapporten skal ses i sammenhæng med det bagvedliggende materiale.

4. DATABEHANDLERENS EFTERLEVELSE AF KRAV I DATABEHANDLERAFTALEN

Krav	Bemærkninger baseret på materialet *OBS: Der er kun indsat bemærkninger, hvis der er anledning hertil. Et tomt felt er derfor udtryk for, at det ikke er anledning til bemærkninger (f.eks. hvis databehandleren blot har svaret "Ja", og der ikke derudover er anledning til at bemærke noget særligt)*	Vurdering af niveau af efterlevelse **Grøn**: Tilfredsstillende **Gul**: Kravet efterleves i et vist omfang **Rød**: Utilfredsstillende	Eventuelt behov for opfølgning
FORTROLIGHED			
Databehandlerens medarbejdere, der behandler personoplysninger, har underskrevet en fortrolighedsaftale eller er underlagt en lovbestemt tavshedspligt			
POLITIK(KER) FOR BEHANDLING AF PERSONOPLYSNINGER			
Databehandleren har implementeret politik(ker) for behandlingen af personoplysninger			
Alle databehandlerens medarbejdere, der behandler den dataansvarliges personoplysninger, er bekendt med databehandlerens politik(ker) for behandling af personoplysninger			

Databehandleren har implementeret procedurer og tekniske foranstaltninger, så databehandleren kan hjælpe den dataansvarlige med at besvare anmodninger fra registrerede, der gør brug af de registreredes rettigheder			
OVERFØRSEL AF OPLYSNINGER TIL TREDJELANDE			
Databehandleren behandler kun personoplysninger i EU, og hvis ikke, sker behandling uden for EU efter instruks fra den dataansvarlige	Databehandleren overfører ikke personoplysninger til tredjelande.		
Hvis der sker behandling af personoplysninger uden for EU, sikrer Databehandleren et fornødent overførselsgrundlag og eventuelt supplerende foranstaltninger	Databehandleren overfører ikke personoplysninger til tredjelande.		
SIKKERHEDSBRUD			
Databehandleren har processer på plads til at opdage sikkerhedsbrud og overvåge unormal netværksaktivitet			
Databehandleren sikrer, at medarbejderne har kendskab til, hvad der udgør et			

sikkerhedsbrud, og hvordan et sikkerheds-brud håndteres			
Databehandleren fører en log over sikkerheds-brud			
Databehandleren bistår i forhold til den dataan-svarliges forpligtelse til at anmelde brud på per-sondatasikkerheden til Datatilsynet, herunder ved underretning af den dataansvarlige uden unødig forsinkelse om brud på persondatasik-keheden			
STANDARDER OG REVISORERKLÆRINGER			
Databehandleren efter-lever kravene i ISO 27001 eller kravene i en i øvrigt anerkendt stan-dard inden for IT-drift			
Databehandleren får udarbejdet revisorer-klæringer, der doku-menterer databehandle-rens efterlevelse af GDPR og/eller databe-handleraftalen	Databehandleren laver in-tern audit fra Group DPO i stedet. OK, når der er ISO-certificering.		
OPERATIONEL SIKKERHED OG NETVÆRKSSIKKERHED			
Databehandleren sikrer, at eventuelle underda-tabehandlere har til-strækkelige sikkerheds-foranstaltninger i			

overensstemmelse med databehandleraftalen			
Ændringer i Databehandlerens sikkerhedsforanstaltninger, der er relevante for behandlingen af den dataansvarliges personoplysninger, logges og dokumenteres			
Alle ændringer og opdateringer af hardware og/eller software testes og godkendes, inden de implementeres			
Databehandlerens eventuelle testmiljøer er tilstrækkelig afgrænset og i øvrigt sikret mod uautoriseret adgang	CGM har ved e-mail af 7. august 2024 supplerende oplyst, at patientdata aldrig benyttes til test, idet kun syntetiske data benyttes, jf. CGM's interne politik.		
Databehandlerens it-systemer og netværk er tilstrækkeligt sikret mod hacking, anden uautoriseret adgang og ondsindet kode			
Databehandleren gennemfører kontroller for at opdage og forhindre svindel, malware mv.			
Databehandlerens enheder, der bruges til at behandle personoplysninger, er krypterede	Data i hvile (backups og live data) er ikke krypteret som standardindstilling. Dette er et tilvalg for kunden, og sker derfor, hvis kunden vælger det.		Det anbefales, at den dataansvarlige vurderer behovet for at aktivere kryptering for data i hvile.

Databehandlerens eventuelle dekrypteringsnøgle/adgangskode deles ikke med eksterne, som ikke er identificeret/anført som underdatabehandlere			
Databehandlerens IT-systemer understøtter sletning	Der er to kørsler, der manuelt igangsættes i systemet af den praktiserende læge (én, hvor den praktiserende læge kan vælge først at sætte en eller flere journaler i karantæne i 3 mdr. og herefter én, hvor lægen efterfølgende selv kan vælge, om journalen/journalerne i karantæne skal slettes permanent efter de 3 mdr.). Systemet foretager dermed alene den sletning af journalerne, som den enkelte praktiserende læge beder om. Hvis en lægeklinik ønsker at straks-slette en journal, kan de gøre dette enkeltvis for hver journal.		
Databehandleren er teknisk i stand til at slette eller tilbagelevere de behandlede personoplysninger, hvis databehandlerrelationen ophører			
FYSISK SIKKERHED			

Databehandleren har sikret sine fysiske lokaliteter, servere mv. mod uautoriseret adgang	Databehandleren har dobbeltdøre, nøglebrik, alarm og brandalarm.		
Databehandleren har tilstrækkelig fysisk sikkerhed i datacentre			
Databehandleren har interne sikkerhedsprocedurer der ved fjernelse, afhændelse eller genbrug af hardware sikrer, at den Dataansvarliges personoplysninger ikke kompromitteres			
BACKUP			
Hvis backup er aftalt: Databehandleren foretager backup af personoplysninger i journalsystemet én gang i døgnet			
Hvis backup er aftalt: Databehandleren sikrer, at backup opbevares i en anden bygning end produktionsserveren			
ADGANG TIL PERSONOPLYSNINGERNE			
Databehandleren sikrer, at kun relevante medarbejdere har adgang til personoplysningerne			
Databehandleren er i stand til – efter			

eventuel anmodning fra den dataansvarlige – at afgive erklæring om, hvilke personer, der har haft adgang til personoplysningerne på vegne af Databehandleren			
Databehandleren sikrer, at medarbejdere hos Databehandleren, der behandler personoplysningerne, har tilstrækkeligt kendskab til korrekt håndtering af personoplysninger, f.eks. gennem undervisning eller e-learning.			
Databehandleren fjerner adgang til personoplysninger, når en medarbejders eller underdatabehandlers arbejdsopgaver ændrer sig, eller når samarbejdet ophører			
BRUG AF OPLYSNINGER TIL DATABEHANDLERENS EGNE FORMÅL			
Databehandleren (eller dennes eventuelle underdatabehandlere) behandler ikke den dataansvarliges personoplysninger til egne formål			
UNDERDATABEHANDLERE			
Databehandleren har indgået underdatabehandleraftaler med alle eventuelle			

underdatabehandlere, som overholder de samme krav, som den dataansvarlige har pålagt databehandleren			
Databehandleren screener/fører tilsyn med eventuelle underdatabehandlere med henblik på at sikre, at de efterlever databeskyttelseskravene			
Databehandleren kan - efter anmodning - fremlægge dokumentation for gennemførte pre-audit og/eller løbende audit af eventuelle underdatabehandlere			
LOGNING			
Databehandleren logger alle afviste adgangsforsøg			
Databehandleren sikrer, at en bruger blokeres, indtil årsagen er klarlagt og dokumenteret, hvis den samme bruger inden for en periode på 24 timer har haft 3 på hinanden følgende afviste adgangsforsøg			
Databehandleren logger al behandling af personoplysninger, herunder tidspunkt, bruger, type af anvendelse og den person, de			

anvendte oplysninger vedrører eller det anvendte søgekriterium			
Databehandlerens IT-systemer generer logfiler, der er nødvendige for at overvåge, analysere, efterforske og rapportere ulovlige, autoriserede eller upassende aktiviteter			

5. EVENTUELLE ØVRIGE OPLYSNINGER AF RELEVANS FOR TILSYNSRAPPORTEN

Den dataansvarlige har den 18. juli 2024 stillet følgende opfølgende spørgsmål:

- I har svaret, at sletning sker ved, at sletning startes manuelt, hvorefter relevante data bliver sat i karantæne i 3 mdr. Næste gang kørslen foretages, slettes data i karantæne og potentiel ny data sættes i karantæne. Kan I uddybe hvad baggrunden er for, at data sættes i karantæne i 3 måneder, og om der er mulighed for at gennemføre sletning straks, hvis den dataansvarlige instruerer om dette?
- I har svaret, at I anvender testmiljøer, der er tilstrækkelig beskyttet. Anvendes personoplysninger om patienter til test, og vil I så fald identificere hvor/hvordan de dataansvarlige klinikker har afgivet instruks herom?