KROMANN REUMERT

TILSYNSRAPPORT - 2023-2024

Tilsyn med databehandleren EG Danmark A/S

Udarbejdet / senest opdateret: 12. september 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 EG Danmark 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 2. september 2024. Spørgeskemaet er udfyldt af Christian Nyholm Jensen, Legal Counsel i EG Danmark A/S.
- ISAE3000-erklæring af maj 2024.
- ISAE3402-erklæring af maj 2024.
- Bemærkning til tilsynsrapport fra EG Danmark A/S ved e-mail af 10. september 2024.

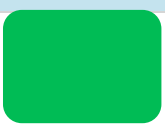
Tilsynsrapporten skal ses i sammenhæng med det bagvedliggende materiale.

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	Fra ISAE3000-erklæringen: "Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang af og opfølgning på logge. Inspiceret, at logning af		Der bør på baggrund af den beskrevne stikprøve følges op på, om databehandleren fremadrettet foretager logning på alle servere i overensstemmelse med databehandlerens politikker herfor.

	brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret. Inspiceret, at opsamlede oplysninger om brugeraktivitet i logge er beskyttet mod manipulation og sletning. Inspiceret ved en stikprøve på logning, at logfilerne har det forventede indhold i forhold til opsætning, og at der er dokumentation for den foretagne opfølgning og håndtering af eventuelle sikkerhedshændelser. Inspiceret ved en stikprøve på logning, at der er dokumentation for den foretagne opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder." Resultat af test: "Vi har ved vores test konstateret, at der for udvalgte windows servere ikke var opsat audit logs i overensstemmelse med EG's politik. Ingen yderligere afvigelser noteret." "Inspiceret, at databehandleren udbyder awarenesstræning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Inspiceret dokumentation for, at netværkstrafikken overvåges, samt at der sker opfølgning		

	på anormaliteter, overvågningsalarmer, overførsel af store filer mv. Inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang."		
Databehandleren sikrer, at medarbejderne har kendskab til, hvad der udgør et sikkerhedsbrud, og hvordan et sikkerhedsbrud håndteres			
Databehandleren fører en log over sikkerhedsbrud	Databehandleren har ved e-mail af 10. september 2024 oplyst, at databehandleren fører log over samtlige sikkerhedsbrud, hvilket også gælder for databehandlerens lægesystemer, EG WinPLC og EG Clinea.		
Databehandleren bistår i forhold til den dataansvarliges forpligtelse til at anmelde brud på persondatasikkerheden til Datatilsynet, herunder ved underretning af den dataansvarlige uden unødig forsinkelse om brud på persondatasikkeheden			
STANDARDER OG REVISORERKLÆRINGER			
Databehandleren efterlever kravene i ISO 27001 eller kravene i en			

i øvrigt anerkendt standard inden for IT-drift			
Databehandleren får udarbejdet revisorerklæringer, der dokumenterer databehandlerens efterlevelse af GDPR og/eller databehandleraftalen			
OPERATIONEL SIKKERHED OG NETVÆRKSSIKKERHED			
Databehandleren sikrer, at eventuelle underdatabehandlere har tilstrækkelige sikkerhedsforanstaltninger 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			
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			
Databehandlerens eventuelle dekrypteringsnøgle/adgangskode deles ikke med eksterne, som ikke er identificeret/anført som underdatabehandlere			
Databehandlerens IT-systemer understøtter sletning			
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 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	Fra ISAE3402-erklæring: "Vi har ved vores test konstateret, at der for en specifik AS/40 server ikke var opsat password policy i overensstemmelse med EG's politik." "Vi har ved vores test konstateret, at der for udvalgte windows servere ikke var opsat lockout settings i		Der bør på baggrund af den beskrevne stikprøve følges op på, om databehandleren fremadrettet opsætter lockout settings i overensstemmelse med databehandlerens politikker herfor.

	overensstemmelse med EG's politik,"		
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	Fra ISAE3402-erklæringen: ”Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, gennemgået systemopsætningen på servere og væsentlige netværksenheder samt inspiceret, at parametrene for logning er opsat, således at handlinger udført af brugere med udvidede rettigheder bliver logget. Vi har endvidere ved stikprøvevis inspektion kontrolleret, at der foretages tilstrækkelig opfølgning på logs fra kritiske systemer.” Fra ISAE3000-erklæringen: "Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang af og opfølgning på logge. Inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret. Inspiceret, at opsamlede oplysninger om brugeraktivitet i logge er beskyttet mod manipulation og		Der synes generelt at foretages logning i fornødent omfang. Dog bør der på baggrund af den beskrevne stikprøve følges op på, om databehandleren fremadrettet foretager logning på alle servere i overensstemmelse med databehandlerens politikker herfor.

	sletning. Inspiceret ved en stikprøve på logning, at logfilerne har det forventede indhold i forhold til opsætning, og at der er dokumentation for den foretagne opfølgning og håndtering af eventuelle sikkerhedshændelser. Inspiceret ved en stikprøve på logning, at der er dokumentation for den foretagne opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder." "Vi har ved vores test konstateret, at der for udvalgte windows servere ikke var opsat audit logs i overensstemmelse med EG's politik."		
Databehandlerens IT-systemer generer logfiler, der er nødvendige for at overvåge, analysere, efterforske og rapportere ulovlige, autoriserede eller upassende aktiviteter