KROMANN REUMERT

TILSYNSRAPPORT 2025-2026

Kontaktoplysninger på leverandør ("databehandleren")	Svar
Navn på databehandlingsvirksomhed:	SYNLAB Medical Digital Services A/S

Navn på system eller tjeneste:	WebReq

Den "**dataansvarlige**" refererer til den praktiserende læge.

1. GENERELLE TILSYNSSPØRGSMÅL:

Konklusion	Kromann Reumert kommentar
Konklusionen på tilsynet er følgende:	Tilsynet vedrørende SYNLAB, baseret på ISAE 3000 Type 2-erklæring fra december 2024, fremsendt af SYNLAB, efterfølgende betegnet "Rapporten", samt "Databehandleraftale vedrørende brug af WebReq", efterfølgende betegnet "DPA". Der er ikke konstateret forhold, der giver anledning til væsentlige bemærkninger. Det bemærkes dog (se afsnit F i dette skema), at det i DPA'ens s. 11 og 12, angives, at det for praktiserende speciallæger gælder, at PRO-data videregives til kliniske kvalitetsdatabaser, der er godkendt af Sundhedsdatastyrelsen, hvor det er relevant. PLO har angivet, at videregivelsen til sundhed.dk følger af PLO´s instruks, og at alle klinikker under PLO´s overenskomst er forpligtet til at videregive disse oplysninger til Sundhed.dk. Dette giver derfor ikke anledning til bemærkninger. Endvidere fremgår det af DPA'en med SYNLAB, at der opkræves betaling for audit-relaterede forespørgsler. Det må derfor forventes, at dette også vil være gældende ved eventuel henvendelse angående ovenstående.

Afsnit A Databehandlerens lokationer samt typen af personoplysninger	Kromann Reumert kommentar Grøn: Tilfredsstillende Gul: Kravet efterleves i et vist omfang Rød: Utilfredsstillende
Oplys venligst adresse(r), herunder fysiske beliggenheder, hvor databehandleren modtager, lagrer, tilgår og/eller på anden måde behandler personoplysninger på vegne af den dataansvarlige.	**Delkonklusion: OK.** **DPA:** Odeons Kvarter 19, 2. tv, 5000 Odense, s. 1

Vejledning: Denne liste skal indeholde en beskrivelse af, hvilken type databehandling, der foregår på hver adresse. *Hvis databehandleren behandler personoplysninger uden for EU/EØS, skal listen også indeholde overførselsgrundlag, overførselshyppighed og varighed af overførslen.*	**Rapport:** Odeons Kvarter 19, 2. tv, 5000 Odense, Danmark, jf. rapportens side 4, Ledelseserklæring, midt på siden og side 8, Kapitel 3, indledning.
Beskrivelse af de kategorier af personoplysninger, der behandles på lokationen.	**Delkonklusion: OK.** **DPA:** s. 11, Bilag A.3: "Behandling af personoplysninger sker i forbindelse med laboratorieundersøgelser, PRO-skemaer, mv. Kategorier: navn, adresse, telefonnummer, mail, helbredsoplysninger, CPR-nr., sundhedspersoners oplysninger mv." **Rapport:** s. 9, kapitel 3: "Omfatter bl.a. navn, adresse, telefonnummer, mail, helbredsoplysninger og CPR-nr." **Rapport**: s. 15, kontrolmål A: "Vi har ikke ved vores test konstateret væsentlige afvigelser."

Afsnit B **Underdatabehandlere/underleverandørers lokationer**	**Kromann Reumert kommentar** **Grøn: Tilfredsstillende** **Gul: Kravet efterleves i et vist omfang** **Rød: Utilfredsstillende**
Bruger I underdatabehandlere (underleverandører til at behandle data f.eks. via fjernadgang, mirroring, back-up eller anden type af behandling)?	**Delkonklusion: OK.** **DPA:** Ja, kun for godkendte underdatabehandlere, jf. DPA s. 6, pkt. 7 og s. 12, Bilag B.

	Rapport: s. 26, kontrolmål F: "Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed"
Hvis dette er tilfældet, angiv venligst: (i) navn og adresse for hver underdatabehandler (og deres eventuelle underdatabehandlere) og deres behandling (ii) typen af personoplysninger, som de behandler, og til hvilke formål (iii) hvis underdatabehandleren behandler den dataansvarliges personoplysninger i lande uden for EU/EØS, hvad er så retsgrundlaget for overførslen? *Vejledning: Datatilsynet kræver, at den dataansvarlige kan levere en fuld liste over underdatabehandlere (i hele databehandlerkæden), og dette er også et indirekte krav i henhold til artikel 30 i GDPR.*	**Delkonklusion: OK.** **DPA:** DataGruppen MultiMed A/S, Storhaven 12, 7100 Vejle (hosting, videregivelse, transmission). Region Nordjylland, Niels Bohrs Vej 30, 9220 Aalborg Øst (videregivelse af PRO-data til KIH-databasen), s. 12, Bilag B (tabel).
Har I tredjepartsleverandører involveret i databehandlingen, der ikke er nævnt ovenfor? Hvis ja, angiv dem venligst her. Hvis ja, bedes I angive, hvorvidt databehandleren deler den dataansvarliges personoplysninger med (f.eks. via "kigge-adgang") databehandlerens associerede selskaber, dattervirksomheder eller andre lignende enheder, som ikke er identificeret/opført som underdatabehandler? Hvis ja, angiv venligst, hvilke personoplysninger der deles, og hvorfor enheden ikke er opført som underdatabehandler.	**Delkonklusion: OK.** **DPA:** s. 7, pkt. 8 og s. 16, Bilag C.6. **Rapport**: s. 27, kontrolmål G: “Vi har bekræftet, at der ikke er sket overførsler til tredjelande i kontrolperioden.”

Vejledning: Der kan være leverandører, som ikke har en databeskyttelsesretlig rolle, men som alligevel vil være underdatabehandlere.	
Har databehandleren en procedure for screening af sine underdatabehandlere med henblik på at sikre, at underdatabehandlerne også vil kunne overholde de stillede databeskyttelseskrav?	**Delkonklusion: OK.** **DPA**: s. 6, pkt. 7: "Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2 og 4 … Databehandleren må således ikke gøre brug af en underdatabehandler … uden forudgående specifik skriftlig godkendelse fra den dataansvarlige." **Rapport:** s. 26, kontrolmål F: "Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere..."
Hvordan sikrer I jer, at de underdatabehandlere, I bruger til at levere services, har tilstrækkelige sikkerhedsforanstaltninger (f.eks. ved egne eller eksterne tilsyn)?	**Delkonklusion: OK.** **Rapport:** s. 25-26, kontrolmål F: "Inspiceret ved en stikprøve på underdatabehandleraftaler, at disse indeholder samme krav..."
Hvordan og hvor ofte føres der tilsyn med underdatabehandlere? (beskriv metode for tilsyn samt hyppighed)	**Delkonklusion: OK.** **DPA:** s. 16, Bilag C.7: "Forpligtet til årligt at følge op på eventuelle underdatabehandlere." **Rapport:** s. 26, kontrolmål F: "Inspiceret dokumentation for, at der er foretaget behørig opfølgning..."

Afsnit C Politikker og procedurer	Kromann Reumert kommentar Grøn: Tilfredsstillende Gul: Kravet efterleves i et vist omfang Rød: Utilfredsstillende
Har I implementeret politik(ker) for behandling af personoplysninger? Hvis ja, er alle medarbejdere, der behandler den dataansvarliges personoplysninger, bekendt med disse?	**Delkonklusion: OK.** **DPA:** s. 14, Bilag C.2.2. **Rapport:** s. 21-22, kontrolmål C: “Inspiceret, at der foreligger en informationssikkerhedspolitik...”
Har I procedurer og tekniske foranstaltninger på plads, der gør det muligt for databehandleren at hjælpe den dataansvarlige med at besvare anmodninger fra registrerede om brug af registreredes rettigheder?	**Delkonklusion: OK.** **DPA:** s. 7, pkt. 9 og s. 15, Bilag C.3. **Rapport:** s. 13, s. 28, kontrolmål H: “Vi har ikke ved vores test konstateret væsentlige afvigelser.”

Afsnit D Personer	Kromann Reumert kommentar Grøn: Tilfredsstillende Gul: Kravet efterleves i et vist omfang Rød: Utilfredsstillende
Får medarbejdere, der håndterer den dataansvarliges personoplysninger, løbende træning i håndtering af personoplysninger (f.eks. gennem kurser eller e-learning om GDPR)?	**Delkonklusion: OK.** **DPA:** s. 14, Bilag C.2.2: "Alle ansatte hos databehandleren modtager den tilstrækkelige uddannelse og instruktioner..." **Rapport:** s. 22, kontrolmål C:

	"Inspiceret dokumentation for, at alle medarbejdere... har gennemført den udbudte awareness-træning."
Er medarbejdere, der håndterer den dataansvarliges personoplysninger, bekendt med de sikkerhedskrav, der er aftalt i databehandleraftalen?	**Delkonklusion: OK.** **DPA:** s. 14, Bilag C.2.2. **Rapport:** s. 21-22, kontrolmål C.
Er medarbejderne uddannet i at håndtere sikkerhedsrisici og reagere på dem, f.eks. risici ved phishing-angreb?	**Delkonklusion: OK.** **DPA**: s. 14, Bilag C.2.2. **Rapport:** s. 22, kontrolmål C: "Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til IT-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger. Inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel IT-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning. Vi har ikke ved vores test konstateret væsentlige afvigelser."
Har de medarbejdere, der behandler personoplysninger, underskrevet en fortrolighedsaftale (f.eks. via en klausul i ansættelseskontrakten) eller er de underlagt en lovbestemt tavshedspligt?	**Delkonklusion: OK.** **DPA:** s. 4, pkt. 5: "Alle med adgang er underlagt tavshedspligt." **Rapport:** s. 22, kontrolmål C: "...at de pågældende medarbejdere har underskrevet en fortrolighedsaftale."

Afsnit E **Sikkerhedsbrud**	**Kromann Reumert kommentar** **Grøn: Tilfredsstillende**

	Gul: Kravet efterleves i et vist omfang Rød: Utilfredsstillende
Fører I en log over sikkerhedsbrud? *Vejledning: Den dataansvarlige er forpligtet til at føre log over sikkerhedsbrud for at kunne opfylde sin forpligtelse. Derfor skal databehandleren tilsvarende føre en sådan log.*	**Delkonklusion: OK.** **DPA:** s. 15, Bilag C.2.8. **Rapport:** s. 18, kontrolmål B: "Inspiceret, at logning af brugeraktiviteter... er konfigureret og aktiveret."
Har I som databehandler inden for de seneste 24 måneder været forpligtet til at bistå en dataansvarlig med at anmelde brud på persondatasikkerheden til en tilsynsmyndighed eller til de registrerede? (Hvis ja, uddyb venligst: 1) antallet af anmeldte sikkerhedsbrud, 2) om de pågældende sikkerhedsbrud er anmeldt til Datatilsynet *og* til de registrerede, 3) årsagen til og karakteren af de pågældende sikkerhedsbrud, og 4) hvad der er gjort for at forhindre, at lignende sikkerhedsbrud sker igen)	**Delkonklusion: OK.** **DPA:** s. 8, pkt. 10 og s. 15, Bilag C.3. **Rapport:** s. 28, kontrolmål H: "Vi har fået bekræftet, at der ikke er sket bistand i kontrolperioden."
Har I processer på plads til at opdage sikkerhedsbrud og overvåge unormal netværksaktivitet?	**Delkonklusion: OK.** **DPA:** s. 15, Bilag C.2.8. **Rapport:** s. 29, kontrolmål I: "Inspiceret dokumentation for, at netværkstrafik overvåges, samt at der sker opfølgning på anormaliteter..."
Har I processer på plads til at sikre, at medarbejderne er opmærksomme på, hvad der udgør et sikkerhedsbrud, og hvordan det skal håndteres?	**Delkonklusion: OK.** **DPA:** s. 15, Bilag C.2.2. **Rapport:** s. 29, kontrolmål I.

Har I en procedure, der sikrer, at den dataansvarlige underrettes uden unødig forsinkelse i tilfælde af brud på persondatasikkerheden?	**Delkonklusion: OK.** **DPA:** s. 8, pkt. 10. **Rapport** s. 29-30, kontrolmål I: "Vi har ikke ved vores test konstateret væsentlige afvigelser."

Afsnit F **Brug af personoplysninger til egne formål**	**Kromann Reumert kommentar** **Grøn: Tilfredsstillende** **Gul: Kravet efterleves i et vist omfang** **Rød: Utilfredsstillende**
Kan I bekræfte, at databehandleren (eller dennes underdatabehandlere) ikke behandler den dataansvarliges personoplysninger til egne formål (f.eks. forretningsmæssige formål som udvikling og forbedring af produkter, markedsføringsformål mv.) Hvis databehandleren (eller en af dennes underdatabehandlere) behandler den dataansvarliges personoplysninger til egne formål, bedes du angive formålene, og hvilke personoplysninger der behandles for at opnå formålet. *Vejledning: For at undgå tvivl henviser den dataansvarliges personoplysninger til alle personoplysninger, der behandles af databehandleren i henhold til databeskyttelsesforordningen. Det inkluderer f.eks. journaloplysninger, der opbevares af databehandleren, men også data, der er afledt af den dataansvarliges behandlingsaktiviteter (metadata) osv.*	**Delkonklusion**: **OK.** **DPA:** s. 4, pkt. 4**:** Nej, "Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige..." På s. 11 og 12 Bilag A og B, angives det, at for praktiserende speciallæger gælder, at PRO-data videregives til kliniske kvalitetsdatabaser, der er godkendt af Sundhedsdatastyrelsen, hvor det er relevant. PLO har bekræftet, at videregivelsen til sundhed.dk følger af PLO´s instruks, og alle klinikker under PLO's overenskomst er forpligtede til at videregive disse oplysninger til Sundhed.dk. **Rapport:** s. 15, kontrolmål A: "Vi har ikke ved vores test konstateret væsentlige afvigelser."

Afsnit G Øvrig bistand til den dataansvarlige	Kromann Reumert kommentar Grøn: Tilfredsstillende Gul: Kravet efterleves i et vist omfang Rød: Utilfredsstillende
Har databehandleren etableret procedurer for eventuel bistand til den dataansvarlige til håndtering af anmodninger om registreredes rettigheder i henhold til databeskyttelsesforordningens kapitel III?	**Delkonklusion: OK.** **DPA:** s. 7, pkt. 9 og s. 15, Bilag C.3. **Rapport:** s. 13, s. 28, kontrolmål H.

2. SIKKERHEDSSPØRGSMÅL:

Afsnit 1 **Certificeringer**	**Kromann Reumert kommentar** **Grøn: Tilfredsstillende** **Gul: Kravet efterleves i et vist omfang** **Rød: Utilfredsstillende**
Efterlever databehandleren principperne i ISO 27001 eller en anden i øvrigt anerkendt standard indenfor IT-drift? (uddyb). Hvis ja, vedhæft venligst seneste certificering ved fremsendelse af udfyldt spørgeskema.	**Delkonklusion: OK.** **DPA:** s. 16, Bilag C.7. **Rapport:** s. 10, kontrolmål B: "SYNLAB anvender frameworket for informationssikkerhed ISO27001+2 samt ISO 27701 og er certificeret efter begge standarder."
Får I udarbejdet revisorerklæringer, der dokumenterer jeres efterlevelse af GDPR og/eller databehandleraftalen? Hvis ja, vedhæft venligst seneste erklæring ved fremsendelse af udfyldt spørgeskema.	**Delkonklusion: OK.** **DPA:** s. 16, Bilag C.7: Ja, "Databehandleren skal årligt for egen regning indhente en revisionsrapport fra en uafhængig tredjepart ... ISAE 3000-revisionserklæring." **Rapport:** Det er denne rapport.

Afsnit 2 Netværkssikkerhed og operationel sikkerhed	Kromann Reumert kommentar Grøn: Tilfredsstillende Gul: Kravet efterleves i et vist omfang Rød: Utilfredsstillende
Har I en proces, der sikrer, at alle ændringer og opdateringer af hardware og/eller software testes og godkendes, inden de implementeres?	**Delkonklusion: OK.** **DPA:** s. 14, Bilag C.2.5: **"**Databehandleren skal have formelle procedurer til sikring af, at opdateringer til operativsystemer, databaser, applikationer og anden software bliver vurderet og implementeret inden for rimelig tid. ... enhver ændring er behørigt autoriseret, testet og godkendt inden implementering." **Rapport:** s. 19, kontrolmål B: "Inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Inspiceret ved stikprøve ... at systemer, databaser og netværk er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches. Vi har ikke ved vores test konstateret væsentlige afvigelser."
Har I sikkerhedsforanstaltninger til at forhindre uautoriseret adgang (f.eks. netværksfirewalls)?	**Delkonklusion: OK.** **DPA:** s. 13-14, Bilag C.2.3: "Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. ... Der skal gøres brug af sikre adgangskoder/passwords og autentifikation – samt multifaktorautentifikation ved adgang fra det åbne internet." **Rapport:** s. 16, kontrolmål B: "Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Inspiceret, at firewall er konfigureret i henhold til intern politik herfor. Vi har ikke ved vores test konstateret væsentlige afvigelser."

Har I sikkerhedsforanstaltninger til at forhindre ondsindet kode (f.eks. antivirussoftware)?	**Delkonklusion: OK.** **DPA:** s. 13, Bilag C.2.1: “Der er installeret CrowdStrike Endpoint Detection og Response (EDR) software på alle vores maskiner.” **Rapport:** s. 16, kontrolmål B: "Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus software, og denne er opdateret. Inspiceret, at antivirus software er opdateret. Vi har ikke ved vores test konstateret væsentlige afvigelser.”
Har I implementeret andre sikkerhedsforanstaltninger til at begrænse risikoen for hacking og uautoriseret adgang?	**Delkonklusion: OK.** **DPA:** s. 13-14, Bilag C.2.3 og C.2.8. **Rapport:** s. 17-20, kontrolmål B.
Genererer jeres IT-systemer logfiler i det omfang, det er nødvendigt for at overvåge, analysere, efterforske og rapportere ulovlige, uautoriserede eller upassende aktiviteter?	**Delkonklusion: OK.** **DPA:** s. 15, Bilag C.2.8: "Foretages maskinel logning af alle relevante aktiviteter." **Rapport:** s. 18, kontrolmål B: "Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter ... Inspiceret, at logning af brugeraktiviteter ... er konfigureret og aktiveret. Vi har ikke ved vores test konstateret væsentlige afvigelser."
Transmitteres datakommunikation mellem brugere og systemet, samt mellem forskellige systemer via offentlige netværk? Hvis ja, beskyttes kommunikationen mod uautoriseret aflytning eller manipulation, f.eks. gennem kryptering?	**Delkonklusion: OK.** **DPA:** s. 13, Bilag C.2.1:

	"Der må kun etableres eksterne kommunikationsforbindelser, hvis forbindelsen er krypteret ... HTTPS og nyeste eller næstnyeste version af TLS er et krav. E-mails indeholdende fortrolige og følsomme personoplysninger skal også være beskyttet af kryptering." **Rapport:** s. 18, kontrolmål B: "Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering ... Vi har ikke ved vores test konstateret væsentlige afvigelser."
Hvis der sker ændring af de anvendte sikkerhedsforanstaltninger, der er relevante for behandlingen af den dataansvarliges personoplysninger, vil disse ændringer i så fald blive logget og dokumenteret?	**Delkonklusion: OK.** **DPA:** s. 14, Bilag C.2.5. **Rapport:** s. 19, kontrolmål B.
Anvender databehandleren testmiljøer? Hvis ja; hvordan sikres det, at disse miljøer er tilstrækkeligt afgrænset og sikret mod uautoriseret adgang?	**Delkonklusion: OK.** **DPA:** s. 13, Bilag C.2.1: "SYNLAB anvender ikke personoplysninger i test og udvikling. Der gøres udelukkende brug af Nationale Test CPR-nr. fra MedCom." **Rapport:** s. 19, kontrolmål B: "Vi har fået bekræftet, at der ikke har været anvendt persondata i forbindelse med test og udvikling, og at testdata udelukkende er fiktive data baseret på Nationale Test CPR-nr. Vi har ikke ved vores test konstateret væsentlige afvigelser."

Afsnit 3 Fysisk sikkerhed	Kromann Reumert kommentar Grøn: Tilfredsstillende Gul: Kravet efterleves i et vist omfang Rød: Utilfredsstillende
Hvordan sikrer I jeres fysiske lokaliteter, servere mv. mod uautoriseret fysisk adgang? (f.eks. låse eller andre fysiske sikkerhedskontroller til døre og vinduer)?	**Delkonklusion: OK.** **DPA:** s. 14, Bilag C.2.6: "Fysisk sikring." **Rapport:** s. 15, Bilag C.2.6 og C.2.5.
Har I interne sikkerhedsprocedurer, der ved fjernelse, afhændelse eller genbrug af hardware sikrer, at den dataansvarliges personoplysninger ikke kompromitteres?	**Delkonklusion: OK.** **DPA:** s. 15, Bilag C.2.6. **Rapport:** Rapporten bekræfter, at der er procedurer for fysisk adgang og sikring, men nævner ikke eksplicit procedurer for kassation/genbrug af hardware. s. 20, kontrolmål B “Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Inspiceret dokumentation for, at kun autoriserede personer har haft fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger, i erklæringsperioden. Vi har ikke ved vores test konstateret væsentlige afvigelser.”

Afsnit 4 Backup og gendannelse	Kromann Reumert kommentar Grøn: Tilfredsstillende Gul: Kravet efterleves i et vist omfang Rød: Utilfredsstillende

Foretages der backup af personoplysninger?	**Delkonklusion: OK.** **DPA:** s. 14, Bilag C.2.4. **Rapport:** Rapporten nævner ikke eksplicit backup.
Foretages der tekniske tests af backup?	**Delkonklusion: OK.** **DPA:** s. 14, Bilag C.2.4: Backup læsbart. **Rapport:** N/A.
Hvor ofte foretages backup?	**Delkonklusion: OK.** **DPA**: s. 14, Bilag C.2.4: Aftalen angiver ikke en specifik frekvens, men kræver “regelmæssig backup”. **Rapport:** N/A.
Er backup krypteret? (hvis ja, uddyb krypteringen)	**Delkonklusion: OK.** **DPA:** Aftalen nævner ikke eksplicit kryptering af backup, men stiller generelle krav om kryptering af følsomme data. s. 13, Bilag C.2.1: “Der må kun etableres eksterne kommunikationsforbindelser, hvis forbindelsen er krypteret ... Ved fortrolige og følsomme personoplysninger forventes der en stærk kryptering.” **Rapport:** N/A.
Opbevares sikkerhedskopien fysisk et andet sted end produktionsserveren?	**Delkonklusion: OK.** **DPA:** s. 14, Bilag C.2.4:

	"Backup skal opbevares adskilt fra serveren i et ikke-tilstødende rum for at sikre, at denne ikke går tabt. Backup skal beskyttes, og opbevaring af backup skal altid ske på betryggende vis, så denne ikke fortabes.**"** **Rapport:** N/A.
Har I systemer og procedurer til minimering af afbrydelser som følge af tab eller systemfejl (f.eks. backup på et sikkert sted og gendannelsessystemer)?	**Delkonklusion: OK.** **DPA:** s. 14, Bilag C.2.4: "Databehandleren skal have dokumenterede it-beredskabsprocedurer, der sikrer genetablering af services inden for rimelig tid i tilfælde af driftsafbrydelser. Databehandleren skal regelmæssigt afprøve og evaluere effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed gennem afholdelse af it-beredskabsøvelser." **Rapport:** N/A.
Har I en plan for driftskontinuitet og systemgendannelse i tilfælde af en større katastrofe? Har planen været afprøvet og evalueret inden for de seneste 12 måneder?	**Delkonklusion: OK.** **DPA:** s. 14, Bilag C.2.4: "Databehandleren skal have dokumenterede it-beredskabsprocedurer, der sikrer genetablering af services inden for rimelig tid i tilfælde af driftsafbrydelser. Databehandleren skal regelmæssigt afprøve og evaluere effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed gennem afholdelse af it-beredskabsøvelser. Den dataansvarlige kan anmode om at få dokumentation for dette stillet til rådighed." **Rapport:** N/A.

Afsnit 5 **Adgangskontrol**	**Kromann Reumert kommentar** **Grøn: Tilfredsstillende** **Gul: Kravet efterleves i et vist omfang** **Rød: Utilfredsstillende**
Bruger I adgangskontrol til at sikre, at kun relevante medarbejdere har adgang til de behandlede personoplysninger?	**Delkonklusion: OK.** **DPA:** s. 13-14, Bilag C.2.3.

	Rapport: s. 17-18 og 20, kontrolmål B.
Er adgang (fysisk og enhver anden slags) til personoplysninger og systemer, hvori der behandles personoplysninger, begrænset til medarbejdere, der har et arbejdsrelateret behov for at få adgang til personoplysningerne og systemerne?	**Delkonklusion: OK.** **DPA:** s. 13-14, Bilag C.2.3. **Rapport:** s. 20, kontrolmål B.
Logger I adgang til systemer, hvor personoplysninger behandles, således at I (efter anmodning herom) kan afgive erklæring til den dataansvarlige om, hvilke personer der har haft adgang til personoplysningerne på vegne af databehandleren?	**Delkonklusion: OK.** **DPA:** s. 15, Bilag C.2.8. **Rapport:** s. 18, kontrolmål B.
Har medarbejdere personlige adgangskoder til brug af udstyr, hvorfra der kan opnås adgang til personoplysninger (herunder fysiske medier som f.eks. computer og USB-stik)? Hvis ja, uddyb venligst følgende: 1) Ændres adgangskoderne løbende? 2) Er adgangskoderne unikke og er genbrug af dem ikke muligt inden for en foruddefineret periode? 3) Instrueres medarbejderne i at holde adgangskoder sikre?	**Delkonklusion: OK.** **DPA:** s. 14, Bilag C.2.3. **Rapport:** s. 17, kontrolmål B: "Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysninger, er etableret adgangskontrol, herunder brug af adgangskoder og to-faktor autentifikation."
Hvis der anvendes hjemmekontorer, er der passende foranstaltninger til at beskytte oplysningerne, f.eks. VPN-adgang og multifaktor-godkendelse?	**Delkonklusion: OK.** **DPA:** s. 14, Bilag C.2.7. **Rapport:** s. 17, kontrolmål B: "Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysninger, er etableret adgangskontrol, herunder brug af adgangskoder og to-faktor-autentifikation."
Logges afviste adgangsforsøg? Hvis ja: Hvis der inden for en periode på 24 timer er registreret højst 3 på-hinanden-følgende afviste adgangsforsøg fra	**Delkonklusion: OK.** **DPA:** s. 15, Bilag C.2.8.

samme bruger, sker der så blokering for yderligere forsøg indtil årsagen er klarlagt og dokumenteret?	**Rapport:** s. 18, kontrolmål B: "Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter, og at logning af brugeraktiviteter på systemer og databaser, der anvendes til behandling af personoplysninger, er konfigureret og aktiveret."
Har I procedurer til at sikre fjernelse af adgang til personoplysninger, når arbejdsopgaverne for en medarbejder eller en underdatabehandler ændrer sig, eller når de fratræder?	**Delkonklusion: OK.** **DPA:** s. 14, Bilag C.2.3: "Databehandleren skal uden unødig forsinkelse inddrage autorisationer og adgange for brugere, der efter en konkret vurdering ikke længere bør have disse." **Rapport:** s. 20, kontrolmål B: "Inspiceret, at der sker opfølgning på brugeres adgange, og at adgange fjernes, når arbejdsopgaver ændres eller ophører. Vi har ikke ved vores test konstateret væsentlige afvigelser."

Afsnit 6 **Logning**	**Kromann Reumert kommentar** **Grøn: Tilfredsstillende** **Gul: Kravet efterleves i et vist omfang** **Rød: Utilfredsstillende**
Foretages der maskinel logning af alle anvendelser af personoplysninger? Hvis ja: hvilke oplysninger logges?	**Delkonklusion: OK.** **DPA**: s. 15, Bilag C.2.8. **Rapport:** s. 18, kontrolmål B: "Inspiceret, at logning af brugeraktiviteter på systemer og databaser, der anvendes til behandling af personoplysninger, er konfigureret og aktiveret. Vi har ikke ved vores test konstateret væsentlige afvigelser."
Hvor længe opbevares logs?	**Delkonklusion: OK.**

	DPA: s. 15, Bilag C.2.8: "Loggen opbevares i seks måneder, hvorefter den slettes, medmindre der fastsættes en længere opbevarings-periode af hensyn til efterforskning." **Rapport:** N/A.

Afsnit 7 **Kryptering**	**Kromann Reumert kommentar** **Grøn: Tilfredsstillende** **Gul: Kravet efterleves i et vist omfang** **Rød: Utilfredsstillende**
Er enheder (f.eks. PC, USB-drev, telefoner, tablets), der bruges til at behandle personoplysninger, krypterede?	**Delkonklusion: OK.** **DPA:** s. 13, Bilag C.2.1: Aftalen stiller krav om kryptering af eksterne forbindelser og e-mails, men nævner ikke eksplicit kryptering af alle enheder. **Rapport:** N/A.
Er data i systemet krypteret i hvile? (både backups og live data)	**Delkonklusion: OK.** **DPA:** s. 13, Bilag C.2.1: "Der stilles krav om kryptering af data i transit og e-mails, men ikke eksplicit om data i hvile." **Rapport:** N/A.
Er data i systemet end-to-end krypteret i transit?	**Delkonklusion: OK.** **DPA:** s. 13, Bilag C.2.1:

	"Der må kun etableres eksterne kommunikationsforbindelser, hvis forbindelsen er krypteret ... HTTPS og nyeste eller nyeste version af TLS er et krav." **Rapport:** s. 18, kontrolmål B: "Inspiceret, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering. Vi har ikke ved vores test konstateret væsentlige afvigelser."

Afsnit 8 **Sletning**	**Kromann Reumert kommentar** **Grøn: Tilfredsstillende** **Gul: Kravet efterleves i et vist omfang** **Rød: Utilfredsstillende**
Understøttes sletning i systemet? Hvis ja, uddyb venligst om der f.eks. kan opsættes automatisk sletning, og om den dataansvarlige selv kan foretage sletning i systemet?	**Delkonklusion: OK.** **DPA**: s. 15, Bilag C.4: "Oplysningerne i Webreq lagres i 200 dage inden prøvetagning. Hvis der ikke er sket en prøvetagning, slettes oplysningerne. Hvis der er sket en prøvetagning, lagres oplysningerne i 80 dage herefter inden oplysningerne slettes. PRO-skemaer opbevares i op til 2 år, herefter slettes skemaerne." **Rapport:** s. 23, kontrolmål D: "Vi har ikke ved vores test konstateret væsentlige afvigelser. Webreq 200 og 80 dage • Blanketserver 180 dage • Webpatient 2 år."
Ved et eventuelt ophør af databehandlerrelationen, vil I så teknisk være i stand til at slette eller tilbagelevere de behandlede personoplysninger?	**Delkonklusion: OK.** **DPA:** s. 9, pkt. 11 og s. 15, Bilag C.4. **Rapport:** s. 23, kontrolmål D: "Vi har ikke ved vores test konstateret væsentlige afvigelser."

3. OVERFØRSEL AF PERSONOPLYSNINGER TIL TREDJELANDE (LANDE UDEN FOR EU/EØS)

Afsnit (i) **Tredjelandsoverførsler**	**Kromann Reumert kommentar** **Grøn: Tilfredsstillende** **Gul: Kravet efterleves i et vist omfang** **Rød: Utilfredsstillende**
Overfører I (enten direkte eller via en underdatabehandler) den dataansvarliges personoplysninger til et land uden for EU/EØS? *Vejledning: Overførsel skal forstås bredt, og omfatter f.eks. også tilfælde, hvor oplysningerne opbevares i EU, men kan tilgås af f.eks. en supportmedarbejder i et tredjeland.*	**Delkonklusion: OK.** **DPA:** Der er ingen overførsler til tredjelande, jf. s. 16, Bilag C.6. **Rapport:** s. 27, kontrolmål G.