KROMANN REUMERT

TILSYNSRAPPORT 2025-2026

Kontaktoplysninger på leverandør ("databehandleren")	Svar
Navn på databehandlingsvirksomhed:	PLSP A/S
Adresse og land for leverandøren:	Krøyer Kielbergs Vej 3, 1, 8660 Skanderborg, DK
Navn på den person hos databehandleren, der udfylder denne formular:	Jesper Sørensen
Stillingsbetegnelse:	CEO
E-mailadresse:	jes@plsp.dk
Dato for udfyldelse af dette skema:	15. maj 2025
Navn på system eller tjeneste:	PLSP har oplyst at den dataansvarlige anvender følgende services: DDS-aftaledeling Aftalevisning Klinikbeskeder Min Læge Videokonsultation Kontakt Læge FLP Kronikerdatabase FLP-deling via DDS FriFerie 2.0 Ydelsesoverblik Klinik+ AIM frontend visning AIM-RKKP Apps i Almen Praksis Digital Svangrejournal Fælles Stamkort

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

Konklusion	Kromann Reumert kommentar
Konklusionen på tilsynet er følgende:	Tilsynet vedrørende PLSP er baseret på den tilsendte aftale "Underdatabehandleraftale" mellem systemhusene og PLSP, herefter også benævnt "databehandleren", samt de besvarelser, som databehandleren har givet (se under "Svar" nedenfor) og fremsendt til Kromann Reumert den 15. maj 2025. Kæden er således: Klinikkerne (Dataansvarlig) → Systemhusene (Databehandler) → PLSP (Underdatabehandler). Tilsynet har givet anledning til følgende bemærkninger, som der bør følges op på: • Underdatabehandleraftalen ("DPA") er modtaget i templateform og er ikke underskrevet, og listen over underdatabehandlere i bilag B er ikke udfyldt. Disse elementer er et krav i henhold til GDPR artikel 28, se bl.a. afsnit B og 3 nedenfor. Vi forstår, at dette er tilsigtet, da tilsynet foretages på vegne af de enkelte klinikker, som selv er ansvarlige for at indgå den endelige aftale med underskrift og udfyldning af bilag m.v., men for den enkelte klinik medfører det visse opmærksomhedspunkter: o Det er vigtigt, at klinikken kan fremlægge en underskrevet version af DPA'en for at kunne dokumentere, at den er indgået. o Vi har ved tilsynet ikke kunnet verificere, hvorvidt den enkelte dataansvarlige anvender samtlige services, som er oplistet af PLSP i besvarelsen. Vi har heller ikke modtaget hovedaftalen ("kontrakten", som der henvises til i DPA'en), og derfor har vi ikke kunnet efterse, hvad der er aftalt i DPA'en mellem den dataansvarlige og systemhusene. o Databehandleren har ved dette tilsyn oplistet en række underdatabehandlere, som anvendes, men vi har ikke kunnet vurdere, om listen med underdatabehandlere stemmer overens med det, som parterne konkret har udfyldt i DPA'en, da den tilsendte DPA's bilag B om underdatabehandlere ikke er udfyldt. Vi har ej heller modtaget oplysninger om, hvem der hoster PLSP's data, da dette ikke fremgår af bilag B, se afsnit 3. • Gennemgang af DPA'en m.v. har givet anledning til følgende sikkerhedsmæssige opmærksomhedspunkter, som der bør følges op på: • Det bør også aftales, at backup krypteres i hvile, se afsnit 4.

	• Uoverensstemmelse mellem det aftalte i DPA'en afsnit bilag C, punkt 2.6 om opbevaring af logs, se afsnit 6. • Endelig anbefaler vi, at data i systemet krypteres i hvile, se afsnit 7.

1. GENERELLE TILSYNSSPØRGSMÅL:

Afsnit A **Underdatabehandlerens lokationer**	**Svar**	**KR kommentarer** **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 *Vejledning: Denne liste skal indeholde en beskrivelse af hvilken type databehandlingen der foregår på hver adresse, samt en beskrivelse af de kategorier af personoplysninger, der behandles på lokationen.* *Hvis databehandleren behandler personoplysninger uden for EU/EØS, skal listen også indeholde overførselsgrundlag, overførselshyppighed og varighed af overførslen.*	Krøyer Kielbergs Vej 3, 1, 8660 Skanderborg, DK	**Delkonklusion:** OK.

Afsnit B Underunderdatabehandlere lokationer	Svar	KR kommentarer 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)?	Ja	**Delkonklusion:** OK.
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.*	A MedCom, Forskerparken 10B, 5230 Odense M, DK Personopl.: Alm. stamdata samt heldredsoplysninger B Datagruppen MultiMed A/S, Storhaven 12, 7100 Vejle, DK Personopl.: Alm. stamdata samt heldredsoplysninger C OVHCLOUD, 2 Rue Kellermann, 59100 Roubaix, Frankrig Personopl.: Alm. stamdata samt heldredsoplysninger D Trifork Public A/S, Europaplads 2,1, 8000 AArhus C, DK Personopl.: Alm. stamdata samt heldredsoplysninger	**Delkonklusion:** Dette tilsynspunkt er ikke omfattet af dette tilsyn, da det forudsætter gennemgang af den enkelte DPA, som den enkelte klinik har indgået med deres databehandler. Se yderligere uddybning ovenfor i opsamlingsafsnittet.

	E Sundhedsdatastyrelsen, Ørestads Boulevard 5, 2300 København S, DK Personopl.: Alm. stamdata samt heldredsoplysninger F KiAP Fonden, Thomas B. Thriges Gade 48, 1., 5000 Odense C, DK Personopl.: Alm. stamdata samt heldredsoplysninger	
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, datterselskaber 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 *Vejledning: Der kan være leverandører, som ikke har en databeskyttelsesretlig rolle, men som alligevel vil være underdatabehandlere.*	Nej	**Delkonklusion:** OK.
Har databehandleren en procedure for screening af sine underdatabehandlere med henblik på at sikre, at underdatabehandlerne også vil kunne overholde de stillede databeskyttelseskrav?	Ja	**Delkonklusion:** OK. Underdatabehandleren må desuden kun anvende underunderdatabehandlere, hvis de opfylder de betingelser der er i GDPR art. 28, stk. 2, jf. DPA'en punkt 6.

Hvordan sikrer I jer, at de underdatabehandlere, I bruger til at levere services, har tilstrækkelige sikkerhedsforanstaltninger (f.eks. ved egne eller eksterne tilsyn)?	Vi har procedure, tjeklister og kontroller.	**Delkonklusion:** OK. DPA'ens punkt 11 og Bilag C, punkt C7, beskriver desuden, at databehandleren har ret til at føre tilsyn og kræve dokumentation for overholdelsen.
Hvordan og hvor ofte føres der tilsyn med underdatabehandlere? (beskriv metode for tilsyn samt hyppighed)	En gang årligt samt efter behov. Kontrollen gennemføres ud fra en kategorisering af underdatabehandlerne og en dertil tilpasset gennemgang af relevante sikkerhedsområder og dokumentation.	**Delkonklusion:** OK. Ifølge Bilag C, punkt C7.2, "*skal Underdatabehandleren én gang årligt stille en rapport til rådighed for Databehandleren, der dokumenterer overholdelse af aftalen*."
Bekræft venligst, at der er indgået underdatabehandleraftaler med alle underdatabehandlere, og at disse aftaler indeholder de samme krav, som I er pålagt via databehandleraftalen med den dataansvarlige?	Ja	**Delkonklusion:** OK. Det følger også af DPA'en punkt. 6.5. og 6.6.

Afsnit C **Politikker og procedurer**	**Svar**	**KR kommentarer** **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?	Ja, vi er ISO27001 og ISO 27701 certificeret og bruger aktivt disse rammeværker i hverdagen. Alle medarbejdere instrueres i dette arbejde og holdes løbende ajour med ændringer.	**Delkonklusion:** OK. ISO27001 (informationssikkerhed). Fremgår af DPA'ens Bilag, C2.1, at det er et krav. Samme følger også af deres hjemmeside her: //www.plsp.dk/iso2700127701. Seneste certifikater er gældende fra perioden 22. oktober 2023 til 21. oktober 2026

		(27001) og 9. februar 2025 til 21 oktober 2026 (ISO27701). Disse vedlægges også denne tilsynsrapport. Certifikaterne er udstedt til PLSP A/S og dækker deres rolle som databehandler.
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?	Ja, det ligger i procedurer i ISO rammeværket.	**Delkonklusion:** OK. DPA'en punkt 8 beskriver desuden bistand til databehandleren.

Afsnit D **Personer**	**Svar**	**KR kommentarer** **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)?	Ja, dels internt i kvartalsmæssige ISO-møder og dels via årligt seminar med tilknyttet Advokat/DPO. Desuden efter behov.	**Delkonklusion:** OK. DPA'en stiller krav om, at medarbejdere, der håndterer den dataansvarliges personoplysninger, skal have tilstrækkeligt kendskab til korrekt håndtering af personoplysninger og være bekendt med de gældende sikkerhedskrav, jf. DPA'ens punkt 4 og bilag C, punkt C2.5.
Er medarbejdere, der håndterer den dataansvarliges personoplysninger, bekendt med de sikkerhedskrav, der er aftalt i databehandleraftalen?	Ja	**Delkonklusion:** OK. Se ovenfor.
Er medarbejderne uddannet i at håndtere sikkerhedsrisici og reagere på dem, f.eks. risici ved phishing-angreb?	Ja	**Delkonklusion:** OK. Se ovenfor.
Har de medarbejdere, der behandler personoplysninger, underskrevet en fortrolighedsaftale (f.eks. via en klausul i ansættelseskontrakten) eller er de underlagt en lovbestemt tavshedspligt?	Ja, i ansættelseskontrakt	**Delkonklusion:** OK. Intet konkret om ansættelseskontrakter, men et afsnit om fortrolighed i DPA'ens punkt. 4 , hvor der kun må gives adgang

		til personoplysninger til personer "*som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt*" jf. også GDPR artikel 28 stk. 3 litra b

Afsnit E **Sikkerhedsbrud**	**Svar**	**KR kommentarer** **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.*	Ja	**Delkonklusion:** OK. Følger af DPA'ens Bilag C, punkt C3.1. "*Underdatabehandleren skal til enhver tid føre et register over Underdatabehandlerens sikkerhedsbrud med detaljer om bruddene i forbindelse med Underdatabehandlerens databehandling af personoplysningerne. Underdatabehandleren skal efter anmodning give Databehandleren en kopi deraf.*"
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)	Nej	**Delkonklusion:** OK.
Har I processer på plads til at opdage sikkerhedsbrud og overvåge unormal netværksaktivitet?	Ja	**Delkonklusion:** OK.
Har I processer på plads til at sikre, at medarbejderne er opmærksomme på, hvad der udgør et sikkerhedsbrud, og hvordan det skal håndteres?	Ja	**Delkonklusion:** OK.

Har I en procedure, der sikrer, at den dataansvarlige underrettes uden unødig forsinkelse i tilfælde af brud på persondatasikkerheden?	Ja	**Delkonklusion:** OK. Følger af DPA'ens Bilag C, punkt C3.2, at "*underdatabehandleren skal uden unødig forsinkelse efter opdagelse af sikkerhedsbruddet eller ved mistanke herom, orientere Databehandleren om sikkerhedsbruddet.*"

Afsnit F **Brug af personoplysninger til egne formål**	**Svar**	**KR kommentarer** **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.*	Ja	**Delkonklusion:** OK. Det fremgår, af DPA'en bilag C at der ikke må behandle personoplysninger til egne formål.

Afsnit G **Øvrig bistand til den dataansvarlige**	**Svar**	**KR kommentarer** **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?	Ja	**Delkonklusion:** OK.

2. SIKKERHEDSSPØRGSMÅL:

Afsnit 1 Certificeringer	Svar	KR kommentarer 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.	Ja, vi er ISO 27001 certificerede.	**Delkonklusion:** OK. Fremgår af DPA'ens Bilag C, punkt C2.1, at de skal være 27001 certificerede. Vi anbefaler, at vi ved næste tilsyn får certificeringen tilsendt.
Får I udarbejder revisorerklæringer, der dokumenterer jeres efterlevelse af GDPR og/eller databehandleraftalen? Hvis ja, vedhæft venligst seneste erklæring ved fremsendelse af udfyldt spørgeskema.	Nej	**Delkonklusion:** OK, da PLSP er ISO-certificerede.
Overholder databehandleren andre certificeringer der er relevant ift. behandlingen af personoplysninger?	Vi er også ISO27701 certificerede.	**Delkonklusion:** OK.

Afsnit 2 Netværkssikkerhed og operationel sikkerhed	Svar	KR kommentarer 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?	Ja	**Delkonklusion:** OK. Se DPA'ens Bilag C, punkt C2.2 (Operationel sikkerhed).
Har I sikkerhedsforanstaltninger til at forhindre uautoriseret adgang (f.eks. netværksfirewalls)?	Ja	**Delkonklusion:**

		OK. Se DPA'ens Bilag C, punkt C2.2 (Operationel sikkerhed) og Bilag C, punkt C2.3 (Fysisk sikkerhed).
Har I sikkerhedsforanstaltninger til at forhindre ondsindet kode (f.eks. antivirussoftware)?	Ja	**Delkonklusion:** OK. Se DPA'ens Bilag C, punkt C2.2 (Operationel sikkerhed) og Bilag C, punkt C2.3 (Fysisk sikkerhed).
Har I implementeret andre sikkerhedsforanstaltninger til at begrænse risikoen for hacking og uautoriseret adgang?	Ja, vi har en lang række overvågningsmekanismer og organisatoriske tiltag.	**Delkonklusion:** OK. Se DPA'ens Bilag C, punkt C2.2 (Operationel sikkerhed) og Bilag C, punkt C2.3 (Fysisk sikkerhed).
Genererer jeres IT-systemer logfiler i det omfang, det er nødvendigt for at overvåge, analysere, efterforske og rapportere ulovlige, uautoriserede eller upassende aktiviteter?	Ja	**Delkonklusion:** OK. Se DPA'ens Bilag C, punkt C2.6 (Logning).
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?	Ja, men beskyttet vha. Sundhedsdatanettet og kryptering.	**Delkonklusion:** OK. PLSP har den 18. februar 2026 bekræftet pr. e-mail til KR, at de anvender TLS 1.2 eller højere.
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?	Ja	**Delkonklusion:** OK. Se DPA'ens Bilag C, punkt C2.2 (Operationel sikkerhed).
Anvender databehandleren testmiljøer? Hvis ja; hvordan sikres det, at disse miljøer er tilstrækkelig afgrænset og sikret mod uautoriseret adgang?	Ja, test- og produktionsmiljøer er separate miljøer der ikke har noget tilfælles.	**Delkonklusion:** OK. Se DPA'ens Bilag C, punkt C2.2 (Operationel sikkerhed). Underdatabehandleren skal sikre" *at Underdatabehandlerens eventuelle testmiljøer er tilstrækkelig afgrænset og i øvrigt sikret mod uautoriseret adgang*".

Afsnit 3 Fysisk sikkerhed	Svar	KR kommentarer 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)?	Vi har ingen fysiske servere, alt hostes hos vores hostingpartnere. Hostingleverandørne lever op til vores krav mht. disse områder.	**Delkonklusion:** Det fremgår ikke af DPA'ens Bilag B, hvem der hoster PLSP's data. PLSP har dog oplyst i en e-mail af 18. februar 2026, at PLSP's data hostes hos Datagruppen MultiMed A/S, Storhaven 12, 7100 Vejle (Backup i Herning).
Har I en nødstrømsforsyning, og har I varme, ventilation og aircondition i datacenteret/centrene, hvor oplysningerne hostes?	Ja hostingpartnerne har.	**Delkonklusion:** OK.
Har I brandforebyggende foranstaltninger i datacenteret/centrene, hvor oplysningerne hostes?	Ja hostingpartnerne har.	**Delkonklusion:** OK.
Har I interne sikkerhedsprocedurer der ved fjernelse, afhændelse eller genbrug af hardware sikrer, at den dataansvarliges personoplysninger ikke kompromitteres?	Ja	**Delkonklusion:** OK. Fremgår af DPA'ens Bilag C, punkt C2.3 (Fysisk sikkerhed)

Afsnit 4 Backup og gendannelse	Svar	KR kommentarer Grøn: Tilfredsstillende Gul: Kravet efterleves i et vist omfang Rød: Utilfredsstillende
Foretages der backup af personoplysninger?	Ja	**Delkonklusion:**

		OK.
Foretages der tekniske tests af backup?	Ja, ugentligt	**Delkonklusion:** OK.
Hvor ofte foretages backup?	Dagligt	**Delkonklusion:** OK.
Er backup krypteret? (hvis ja, uddyb krypteringen)	Nej	**Delkonklusion:** Vi anbefaler, at backup krypteres, da det indeholder følsomme oplysninger. Datatilsynet har angivet, at der eksempelvis ved patientjournaler skal der foretages backup. Se her. Vi anbefaler, at det bliver aftalt i den nye DPA. Der fremgår følgende af DPA'en Bilag C, punkt C2.4 (Backup): *"Såfremt det er en del af Kontrakten, eller hvis det på anden vis er aftalt mellem Parterne, vil Underdatabehandleren herefter én gang i døgnet tage en backup af den dataansvarliges oplysninger i journalsystemet. Backup-overførslen skal være krypteret. Backup skal opbevares i et aflåst område i en anden bygning end hvor produktionsserveren fysisk er placeret."*
Opbevares sikkerhedskopien fysisk et andet sted end produktionsserveren?	Ja	**Delkonklusion:** OK.
Har I systemer og procedurer til minimering af afbrydelser som følge af tab eller systemfejl (f.eks. backup på et sikkert sted og gendannelsessystemer)?	Ja	**Delkonklusion:** OK.
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?	Ja, planerne afprøves delvist hver år.	**Delkonklusion:** OK.

Afsnit 5 **Adgangskontrol**	**Svar**	**KR kommentarer** **Grøn: Tilfredsstillende**

		Gul: Kravet efterleves i et vist omfang **Rød: Utilfredsstillende**
Bruger I adgangskontrol til at sikre, at det kun er relevante medarbejdere har adgang til de behandlede personoplysninger?	Ja	**Delkonklusion:** OK. Fremgår af DPA'ens Bilag C, punkt C2.5 (Adgang til personoplysninger.
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?	Ja	**Delkonklusion:** OK. Fremgår af DPA'ens Bilag C, punkt C2.5 (Adgang til personoplysninger.
Logger I adgang til systemer, hvor personoplysninger behandles, således at I (efter anmodning herom) kan afgive erklæring til den dataansvarlige om hvilke personer, som har haft adgang til personoplysningerne på vegne af databehandleren?	Ja	**Delkonklusion:** OK. Fremgår af DPA'ens Bilag C, punkt C2.5 (Adgang til personoplysninger.
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?	Ja 1. Nej de ændres ikke 2. Ja 3. Ja, alle medarbejdere har en key-vault hertil.	**Delkonklusion:** OK. Vi vurderer dette er acceptabelt, da Center for Cybersikkerhed har angivet, at det ikke er mere sikkert at skifte password regelmæssigt. Se her.
Hvis der anvendes hjemmekontorer, er der passende foranstaltninger til at beskytte oplysningerne, f.eks. VPN-adgang og multifaktor-godkendelse?	Ja	**Delkonklusion:** OK.
Logges afviste adgangsforsøg? Hvis ja; Hvis der inden for en periode på 24 timer er registreret højst 3 på hinanden følgende afviste adgangsforsøg fra samme bruger, sker der så blokering for yderligere forsøg indtil årsagen er klarlagt og dokumenteret?	Ja og ja	**Delkonklusion:** OK. Fremgår af DPA'ens Bilag C, punkt C2.6 (Logning).

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?	Ja	**Delkonklusion:** OK.

Afsnit 6 **Logning**	**Svar**	**KR kommentarer** **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?	Ja	**Delkonklusion:** OK. Fremgår af DPA'ens Bilag C, punkt C2.6 (Logning):
Hvor længe opbevares logs?	30 dage	**Delkonklusion:** Uoverensstemmelse mellem instruks via DPA og det der reelt sker. Vi anbefaler at følge op på denne del. Fremgår af DPA'ens Bilag C, punkt C2.6 (Logning): "*Log opbevares i 6 måneder*".

Afsnit 7 **Kryptering**	**Svar**	**KR kommentarer** **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?	Ja	**Delkonklusion:** OK. Der er ikke et direkte krav i aftalen om, at alle enheder, der bruges til behandling af personoplysninger (f.eks. PC, USB-drev, telefoner, tablets), skal være krypterede, men krav i DPA'ens Bilag C, punkt. C2.3.

Er data i systemet krypteret i hvile? (både backups og live data)	Nej	**Delkonklusion:** Vi anbefaler, at PLSP fremover krypterer data i hvile. Datatilsynet har angivet, at eksempler på foranstaltninger, der kan indbygges og udgøre databeskyttelse gennem design (privacy by design), som er et krav efter GDPR, kan være kryptering af data i transit eller hvile. Se her. Vi anbefaler, at det bliver aftalt i den nye DPA.
Er data i systemet end-to-end krypteret i transit?	Ja	**Delkonklusion:** OK.
Bliver dekrypteringsnøglen/adgangskoden delt med nogen uden for databehandleren, f.eks. andre enheder i koncernen eller offentlige myndigheder?	Nej	**Delkonklusion:** OK.

Afsnit 8 **Sletning**	**Svar**	**KR kommentarer** **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?	Ja, alt efter system findes både manuel og automatisk sletning.	**Delkonklusion:** OK.
Ved et eventuelt ophør af databehandlerrelationen, vil I så teknisk være i stand til at slette eller tilbagelevere de behandlede personoplysninger?	Ja	**Delkonklusion:** OK. Fremgår af DPA'ens punkt 10 og Bilag C, punkt C4 (Sletning og tilbagelevering af oplysninger).

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

Afsnit (i) Tredjelandsoverførsler	Svar	KR kommentarer 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.*	Nej	**Delkonklusion:** OK.