KROMANN REUMERT

TILSYNSRAPPORT 2026

Kontaktoplysninger på leverandør ("databehandleren")	Svar
Navn på databehandlingsvirksomhed:	Trifork Digital Health A/S (Trifork)
Adresse og land for leverandøren:	Aaboulevarden 13. 8000 Aarhus C
Navn på den person hos databehandleren, der udfylder denne formular:	Anders Bay-Smidt
Stillingsbetegnelse:	Co-Business Unit Lead
E-mailadresse:	Aby@trifork.com
Dato for udfyldelse af dette skema:	18/06-2025
Navn på system eller tjeneste:	Min Læge App, Kontakt Læge app og Virtuelle Venteværelse. *Bemærk, at vi ved dette tilsyn kun har fokuseret på ydelserne ” Min Læge App” og ”Virtuelt venteværelse Web-App” samt den tilhørende underdatabehandleraftale (se nedenfor).*

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

1. KONKLUSION

Konklusion	Kromann Reumert kommentar
Konklusionen på tilsynet er følgende:	Tilsynet vedrørende Trifork tager udgangspunkt i den tilsendte aftale *"Underdatabehandleraftale"* af PLO den 15. april 2026 (herefter benævnt DPA'en) mellem PLSP og Trifork (herefter benævnt *databehandleren*), samt de besvarelser, som databehandleren har fremsendt til Kromann Reumert den 23. juni 2025 (se under *Svar* nedenfor). Dataansvarsforholdet er efter vores forståelse som følger: Klinikkerne (dataansvarlig) → Systemhusene (databehandler)→ PLSP (underdatabehandler) → Trifork (underdatabehandler) for tjenesterne *"Min Læge App"* og *"Virtuelt venteværelse Web-app"*, som er de ydelser, vi har valgt at fokusere på. Bemærk, at databehandleren har oplyst flere ydelser, men tilsynet omfatter udelukkende disse to og dertilhørende DPA. Der er ikke konstateret forhold, der giver anledning til væsentlige bemærkninger.

2. GENERELLE TILSYNSSPØRGSMÅL:

Afsnit A Databehandlerens 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.*	Vi behandler data hos Trifork Digital Health A/S – Aaboulevarden 13, 8000 Aarhus C. Data hostes hos underdatabehandlere jf. næste punkt	**Delkonklusion:** OK. Fremgår af side 1 i DPA'en. I DPA'en står angivet "Trifork Public A/S", mens Trifork har angivet navnet "Trifork Digital Health A/S". Det tyder på, at der er tale om en navneændring og ikke et skift af juridisk enhed. Vi anbefaler, at I følger op over for Trifork og eventuelt får opdateret DPA'en, så det korrekte enhedsnavn/CVR fremgår.

Hvis databehandleren behandler personoplysninger uden for EU/EØS, skal listen også indeholde overførselsgrundlag, overførselshyppighed og varighed af overførslen.			

Afsnit B **Underdatabehandlere/underleverandørers lokationer**	**Svar**	**Yderligere oplysninger (Uddyb venligst)**	**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)?	Data hostes hos underdatabehandlere.		**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens Bilag A, pkt. 3.2, der angiver Netic A/S som godkendt underdatabehandler til drift og hosting.
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.*	**Min Læge** • Netic A/S Alfred Nobels Vej 27 9220 Aalborg Ø **Kontakt Læge** • Netic A/S Alfred Nobels Vej 27 9220 Aalborg Ø • Datagruppen Multimed A/S Storhaven 12 7100 Vejle	For alle 3 løsninger: • Almindelige personoplysninger ○ Borgerens navn ○ Kommunale medarbejderes AD • Følsomme personoplysninger, jf. Databeskyttelsesforordningens artikel 9: ○ Racemæssig eller etnisk oprindelse ○ Politisk overbevisning ○ Religiøs overbevisning	**Delkonklusion:** For de to ydelser omfattet af tilsynet ("Min Læge App" og "Virtuelt venteværelse Web-App") er der overensstemmelse mellem DPA'ens Bilag A, pkt. 3 og Triforks svar vedrørende underdatabehandlere. Netic A/S er den eneste underdatabehandler for begge ydelser, hvilket stemmer overens med det aftalte i DPA'en.

	Virtuelle Venteværelse • Netic A/S Alfred Nobels Vej 27 9220 Aalborg Ø	○ Filosofisk overbevisning ○ Fagforeningsmæssige tilhørsforhold ○ Helbredsoplysninger, herunder misbrug af medicin, narkotika, alkohol m.v. ○ En fysisk persons seksuelle forhold eller seksuelle orientering • Oplysninger om cpr-nummer, jf. Databeskyttelseslovens § 11: ○ CPR-numre	
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.*	Ifbm. Pilot for Autonotar afprøves AI generering af journalnotater. Her er Corti en tredjepartsleverandør, hvor der er en behandling i Microsoft Azure. Denne Pilot er ikke en del af indeværende besvarelse, da aftalegrundlaget for den er udarbejdet i et selvstændig forløb.		**Delkonklusion:** OK. Pilot for Autonotar er ikke en del af dette tilsyn.

Har databehandleren en procedure for screening af sine underdatabehandlere med henblik på at sikre, at underdatabehandlerne også vil kunne overholde de stillede databeskyttelseskrav?	Ja, vi har faste procedure for risikovurderinger og revisioner af vores underdatabehandlere.		**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens pkt. 10.3-10.4, der foreskriver, at databehandleren kun må gøre brug af underdatabehandlere, der gennem en skriftlig aftale er pålagt de samme databeskyttelsesforpligtelser som i DPA'en, herunder at gennemføre passende tekniske og organisatoriske foranstaltninger.
Hvordan sikrer I jer, at de underdatabehandlere, I bruger til at levere services, har tilstrækkelige sikkerhedsforanstaltninger (f.eks. ved egne eller eksterne tilsyn)?	Ved revision og eftersyn - Eftersynet foretages ud fra relevans og risiko. Det betyder, at den pågældende behandlings art, omfang, sammenhæng og formål samt risikoen for enkeltpersoners rettigheder og friheder tages i betragtning. Jo større risiko, jo større krav til sikkerhed. Eftersynet kan f.eks. ske ved evaluering af erklæringer, indsamling af skriftlig information eller fysisk kontrol.		**Delkonklusion:** OK. Fremgår af DPA'ens pkt. 10.3-10.4, der foreskriver, at Trifork skal sikre, at underdatabehandlere gennem en skriftlig aftale er pålagt de samme databeskyttelsesforpligtelser som i DPA'en, og at Trifork er ansvarlig for underdatabehandleres handlinger som for sine egne.
Hvordan og hvor ofte føres der tilsyn med underdatabehandlere? (beskriv metode for tilsyn samt hyppighed)	Som minimum 1 gang årligt eller ved ændringer i aftalegrundlagene eller typen af behandling eller risiko		**Delkonklusion:** OK. DPA'en foreskriver ikke en specifik frekvens for tilsyn med underdatabehandlere, men pkt. 10.3-10.4 kræver løbende sikring af, at

			underdatabehandlere overholder de samme forpligtelser som i DPA'en. Triforks praksis med minimum årligt tilsyn samt ved ændringer i aftalegrundlag, behandlingstype eller risiko vurderes som tilfredsstillende.
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?	Det bekræfter vi		**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens pkt. 10.3, der foreskriver, at Trifork skal indgå skriftlig aftale med underdatabehandlere, der pålægger dem de samme databeskyttelsesforpligtelser som i DPA'en.

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, og som en del var vores årshjul gennemgår vores medarbejdere løbende vores politikker	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 4.4, der kræver, at medarbejdere har tilstrækkeligt kendskab til korrekt håndtering af personoplysninger.
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	**Delkonklusion:** OK. Fremgår af DPA'ens pkt. 5.1-5.2, at Trifork skal have procedurer og tekniske foranstaltninger, der gør det muligt at bistå den dataansvarlige med at besvare anmodninger fra registrerede i henhold til Databeskyttelsesforordningens kapitel III.

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, ifølge vores årshjul så gennemgår vores medarbejder løbende politikker og træning via E-Learning.	**Delkonklusion:** OK. Det er i overensstemmelse med DPA'ens Bilag B, pkt. 4.4, der kræver, at medarbejdere har tilstrækkeligt kendskab til korrekt håndtering af personoplysninger.
Er medarbejdere, der håndterer den dataansvarliges personoplysninger, bekendt med de sikkerhedskrav, der er aftalt i databehandleraftalen?	Ja	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 4.4, der kræver, at medarbejdere har tilstrækkeligt kendskab til korrekt håndtering af personoplysninger.
Er medarbejderne uddannet i at håndtere sikkerhedsrisici og reagere på dem, f.eks. risici ved phishing-angreb?	Ja	**Delkonklusion:** OK. Dette understøtter DPA'ens Bilag B, pkt. 1.1(E), der kræver kontroller for at opdage og forhindre svindel og ondsindet aktivitet, samt Bilag B, pkt. 4.4, der kræver tilstrækkeligt kendskab til korrekt håndtering af personoplysninger.
Har de medarbejdere, der behandler personoplysninger, underskrevet en fortrolighedsaftale (f.eks. via en klausul i ansættelseskontrakten) eller er de underlagt en lovbestemt tavshedspligt?	Ja, ifbm. ansættelseskontrakt	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens pkt. 4.4, der foreskriver, at medarbejdere autoriseret til at behandle personoplysninger skal have påtaget sig en kontraktuel fortrolighedsforpligtelse eller være underlagt lovbestemt tavshedspligt.

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, vi har interne procedure omkring sikkerhedsbrud som håndteres i Jira og Confluence.	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens pkt. 7.2.1, der foreskriver, at Trifork til enhver tid skal føre et register over sikkerhedsbrud med detaljer om bruddene, og efter anmodning give PLSP 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. DPA'ens pkt. 7.3.1-7.3.3 foreskriver procedurerne for underretning ved sikkerhedsbrud, herunder krav om underretning uden unødig forsinkelse med detaljerede oplysninger om bruddets art, omfang og afhjælpende foranstaltninger.
Har I processer på plads til at opdage sikkerhedsbrud og overvåge unormal netværksaktivitet?	Ja, vi har overvågning af vores løsninger og vores driftsleverandør har overvågning.	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 1.1(D)-(E), der kræver, at IT-systemer og netværk skal være sikret mod hacking og uautoriseret adgang, samt at der gennemføres kontroller for at opdage og forhindre svindel, malware og ondsindet aktivitet.
Har I processer på plads til at sikre, at medarbejderne er opmærksomme på, hvad der udgør et sikkerhedsbrud, og hvordan det skal håndteres?	Ja, som en del af deres løbende træning qua vores årshjul	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 4.4, der kræver tilstrækkeligt kendskab til korrekt håndtering af personoplysninger, samt pkt. 7.3.1, der forudsætter, at sikkerhedsbrud kan identificeres og eskaleres med henblik på underretning uden unødig forsinkelse.

Har I en procedure, der sikrer, at den dataansvarlige underrettes uden unødig forsinkelse i tilfælde af brud på persondatasikkerheden?	Ja, det har vi procedurer på	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens pkt. 7.3.1, der foreskriver underretning uden unødig forsinkelse, samt pkt. 7.3.2-7.3.3, der indeholder detaljerede krav til underretningens indhold.

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.*	Vi bekræfter at vi ikke behandler dataansvarliges personoplysninger til egne formål	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens pkt. 3.1-3.2, der foreskriver, at Trifork alene må behandle personoplysninger efter dokumenteret instruks fra PLSP og ikke må behandle personoplysningerne til sine 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. Dette er i overensstemmelse med DPA'ens pkt. 5.1-5.2, der foreskriver, at Trifork skal gennemføre passende tekniske og organisatoriske foranstaltninger til at bistå med opfyldelsen af registreredes rettigheder i henhold til Databeskyttelsesforordningens kapitel III, herunder ret til adgang, berigtigelse, sletning, begrænsning, dataportabilitet og indsigelse mod automatiske individuelle afgørelser.

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.	Vi er inspireret af principperne for ISO27001 og er ved at blive certificeret. Vi forventer en certificering ved udgangen af 2025	**Delkonklusion:** OK. DPA'en henviser ikke til ISO 27001 eller anden øvrig anerkendt standard inden for IT-drift.
Får I udarbejder revisorerklæringer, der dokumenterer jeres efterlevelse af GDPR og/eller databehandleraftalen? Hvis ja, vedhæft venligst seneste erklæring ved fremsendelse af udfyldt spørgeskema.	Ja, vi får årligt udarbejdet en ISAE3000 erklæring. Den er sendt til dataansvarlige	**Delkonklusion:** OK, det er dog ikke et krav efter DPA'en. Det følger af DPA'ens pkt. 12.2, at Trifork én gang årligt, inden juni måned, skal stille en rapport til rådighed for PLSP med oplysninger, der påviser overholdelse af aftalen.
Overholder databehandleren andre certificeringer der er relevant ift. behandlingen af personoplysninger?	N/A	**Delkonklusion:** OK, det er heller ikke et krav efter DPA'en.

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. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 1.1(A)-(C), der foreskriver, at ændringer i sikkerhedsforanstaltninger skal logges og

		dokumenteres, så vidt muligt ikke påvirke driften negativt, samt at testmiljøer skal være tilstrækkeligt afgrænset og sikret mod uautoriseret adgang.
Har I sikkerhedsforanstaltninger til at forhindre uautoriseret adgang (f.eks. netværksfirewalls)?	Ja	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 1.1(E), der foreskriver, at Trifork skal gennemføre kontroller for at opdage og forhindre svindel, malware og anden ondsindet aktivitet.
Har I sikkerhedsforanstaltninger til at forhindre ondsindet kode (f.eks. antivirussoftware)?	Ja	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 1.1(E), der foreskriver, at Trifork skal gennemføre kontroller for at opdage og forhindre svindel, malware og anden ondsindet aktivitet.
Har I implementeret andre sikkerhedsforanstaltninger til at begrænse risikoen for hacking og uautoriseret adgang?	Ja	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 1.1(D) og pkt. 6.2, der foreskriver, at IT-systemer og netværk skal være tilstrækkeligt sikret, og at der skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til risikoen.
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. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 5.1-5.3, der foreskriver maskinel logning af alle anvendelser af personoplysninger, registrering af afviste adgangsforsøg med notifikation ved gentagne forsøg.
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?	De transmitteres krypteret	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens pkt. 6.2(a), der foreskriver kryptering af personoplysninger, samt Bilag B, pkt. 1.1(D), der kræver tilstrækkelig sikring af IT-systemer og netværk mod uautoriseret adgang.
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, der vil blive gennemgået en risikovurdering på ny herunder	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 1.1(A), der foreskriver, at ændringer i sikkerhedsforanstaltninger relevante for behandlingen af personoplysninger skal logges og dokumenteres.

	tjek af krav op imod aftalegrundlagene	
Anvender databehandleren testmiljøer? Hvis ja; hvordan sikres det, at disse miljøer er tilstrækkelig afgrænset og sikret mod uautoriseret adgang?	Ja, databehandleren anvender testmiljøer. Disse er beskyttet via Triforks VPN med to-faktorgodkendelse (OTP til mobil). Testservere kræver både whitelisting af IP og SSH-adgang, som kun gives efter manuel oprettelse. Adgang til testapps sker via invitation og testbrugere. Miljøerne er dermed afgrænset og sikret mod uautoriseret adgang.	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 1.1(C), der foreskriver, at testmiljøer skal være tilstrækkeligt afgrænset og 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)?	Håndteres af vores driftsleverandør Netic som har Fysiske sikkerhedskontroller	**Delkonklusion:** OK. Det er i overensstemmelse med DPA'ens Bilag B, pkt. 2.1, der foreskriver sikring af fysiske lokaliteter og servere mod uautoriseret adgang. Trifork er jf. pkt. 10.4 ansvarlig for Netics handlinger som for sine egne.
Har I en nødstrømsforsyning, og har I varme, ventilation og aircondition i datacenteret/centrene, hvor oplysningerne hostes?	Håndteres af driftsleverandør Netic og ja	**Delkonklusion:** OK. Trifork bekræfter, at nødstrømsforsyning, varme, ventilation og aircondition er på plads i datacenteret og håndteres af driftsleverandøren Netic. Da

		data hostes hos Netic, er dette en naturlig ansvarsfordeling i overensstemmelse med DPA'ens Bilag B, pkt. 2.1 og pkt. 10.4.
Har I brandforebyggende foranstaltninger i datacenteret/centrene, hvor oplysningerne hostes?	Håndteres af driftsleverandør Netic og ja	**Delkonklusion:** OK. Trifork bekræfter, at brandforebyggende foranstaltninger er på plads i datacenteret og håndteres af driftsleverandøren Netic. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 2.1 og pkt. 10.4.
Har I interne sikkerhedsprocedurer der ved fjernelse, afhændelse eller genbrug af hardware sikrer, at den dataansvarliges personoplysninger ikke kompromitteres?	Ja, det er også instrueret i instrukserne.	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 2.2, der foreskriver interne sikkerhedsprocedurer til at sikre, at personoplysninger ikke kompromitteres ved fjernelse, afhændelse eller genbrug af hardware.

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. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 3.1, der foreskriver, at Trifork skal foretage backup.
Foretages der tekniske tests af backup?	Ja	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 3.1, der foreskriver, at Trifork skal foretage teknisk test af backup, samt pkt. 3.2, der kræver, at Trifork stiller en erklæring om backup og teknisk test til rådighed for PLSP.
Hvor ofte foretages backup?	Der tages backup 1 gang i døgnet. Alle daglige backups gemmes i 30 dage. En	**Delkonklusion:** OK. DPA'ens Bilag B, pkt. 3.1 foreskriver, at Trifork skal foretage backup, men angiver ikke en specifik frekvens. Triforks praksis med daglig backup vurderes som tilfredsstillende.

	månedlig backup gemmes i 185 dage.	
Er backup krypteret? (hvis ja, uddyb krypteringen)	Ja, der gælder samme instruks for backup som al anden behandling jf. Databehandleraftalen	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens pkt. 6.2(a), der foreskriver kryptering af personoplysninger.
Opbevares sikkerhedskopien fysisk et andet sted end produktionsserveren?	Ja	**Delkonklusion:** OK. DPA'en kræver ikke eksplicit fysisk adskillelse, men det understøtter kravet i pkt. 6.2(c) om evne til rettidig genoprettelse af tilgængelighed ved fysiske eller tekniske hændelser.
Har I systemer og procedurer til minimering af afbrydelser som følge af tab eller systemfejl (f.eks. backup på et sikkert sted og gendannelsessystemer)?	Backup data gemmes i et fysisk andet datacenter ned der hvor Produktions data befinder sig	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens pkt. 6.2(c), der foreskriver evne til rettidig genoprettelse ved fysiske eller tekniske hændelser, samt pkt. 6.2(d), der kræver procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger. Månedlige restore-test vurderes som tilfredsstillende.
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, der er en beredskabsplan og der er periodiske restore test af backup systemet generelt hver måned.	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens pkt. 6.2(c)-(d), der foreskriver evne til rettidig genoprettelse ved fysiske eller tekniske hændelser samt procedure for regelmæssig afprøvning, vurdering og evaluering af foranstaltningernes effektivitet.

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. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 4.1, der foreskriver, at kun relevante medarbejdere skal have adgang, samt aftalens pkt. 4.2-4.3, der kræver, at kun nødvendige personer autoriseres, og at behandling kun sker efter instruks fra PLSP.
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. Dette er i overensstemmelse med DPA'ens pkt. 4.2 og Bilag B, pkt. 4.1, der foreskriver, at kun nødvendige og relevante medarbejdere skal have adgang til personoplysningerne.
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. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 4.2, der foreskriver, at Trifork efter anmodning skal kunne afgive erklæring herom, samt Bilag B, pkt. 5.1, der kræver maskinel logning af alle anvendelser af 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, og ja til alle 3 punkter	**Delkonklusion:** OK DPA'en foreskriver ikke eksplicit krav til adgangskodepolitik, men dette understøtter de overordnede krav i DPA'ens pkt. 6.2 om passende tekniske og organisatoriske foranstaltninger samt Bilag B, pkt. 4.1 om adgangskontrol.
Hvis der anvendes hjemmekontorer, er der passende foranstaltninger til at beskytte oplysningerne, f.eks. VPN-adgang og multifaktor-godkendelse?	Ja, der er VPN-adgang med to faktor	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens pkt. 6.2 om passende tekniske og organisatoriske foranstaltninger samt Bilag B, pkt. 1.1(D), der kræver tilstrækkelig sikring af IT-systemer og netværk mod uautoriseret adgang.
Logges afviste adgangsforsøg?	Der føres log over adgangsforsøg som	**Delkonklusion:**

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?	løbende overvåges/gennemgås.	OK. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 5.2, der foreskriver registrering af alle afviste adgangsforsøg med notifikation ved gentagne forsøg.
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. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 4.1 og aftalens pkt. 4.2, der foreskriver, at kun relevante og nødvendige medarbejdere skal have adgang til personoplysningerne.

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, der foretages maskinel logning af alle anvendelser af personoplysninger. Der logges oplysninger om adgang, ændringer og søgninger, herunder tidspunkt, bruger, type af anvendelse samt identifikation af den person, oplysningerne vedrører – eller det anvendte søgekriterium.	**Delkonklusion:** OK. Dette er i fuld overensstemmelse med DPA'ens Bilag B, pkt. 5.1, der foreskriver disse logningskrav.
Hvor længe opbevares logs?	6 måneder	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens Bilag B, pkt. 5.3, der foreskriver opbevaring af log 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. Dette er i overensstemmelse med DPA'ens pkt. 6.2(a), der foreskriver kryptering af personoplysninger.
Er data i systemet krypteret i hvile? (både backups og live data)	Ja	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens pkt. 6.2(a), der foreskriver kryptering af personoplysninger.
Er data i systemet end-to-end krypteret i transit?	Ja	**Delkonklusion:** OK. Samme som ovenfor.
Bliver dekrypteringsnøglen/adgangskoden delt med nogen uden for databehandleren, f.eks. andre enheder i koncernen eller offentlige myndigheder?	Data krypteringsnøglerne håndteres af backup systemet, og deles ikke med andre	**Delkonklusion:** OK. Krypteringsnøglerne håndteres af backupsystemet og deles ikke med andre. I overensstemmelse med DPA'ens pkt. 6.2.

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, det understøttes. Der kan opsættes automatisk sletning. Som	**Delkonklusion:**

	det er sat op i dag har dataansvarlige ikke mulighed for selv at slette. Det skal der instrurere/anmodes om	OK. Dette er i overensstemmelse med DPA'ens pkt. 3.1 og 3.4, der foreskriver, at behandling herunder sletning alene sker efter dokumenteret instruks fra PLSP.
Ved et eventuelt ophør af databehandlerrelationen, vil I så teknisk være i stand til at slette eller tilbagelevere de behandlede personoplysninger?	Ja	**Delkonklusion:** OK. Dette er i overensstemmelse med DPA'ens pkt. 14.2, der foreskriver, at Trifork ved ophør skal slette eller tilbagelevere alle personoplysninger til PLSP og slette eksisterende kopier, medmindre EU-retten eller national ret foreskriver opbevaring.

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.